Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC

Bundesamt für Strassen
Office fédéral des routes
Ufficio federale delle Strade

IT-Security im Bereich Verkehrstelematik

IT-Security pour la télématique des transports

IT-Security for Transport and Telematics

Rosenthaler + Partner AG

Claude Marschal

Lukas Schildknecht

Zürcher Hochschule für Angewandte Wissenschaften

Marc Rennhard

Marco Koster

Forschungsauftrag VSS 2007/904 auf Antrag des

Verbandes Schweizer Strassen- und Verkehrsfachleute

Mai 2011 **1350**

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK
Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC
Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni DATEC

Bundesamt für Strassen
Office fédéral des routes
Ufficio federale delle Strade

IT-Security im Bereich Verkehrstelematik

IT-Security pour la télématique des transports

IT-Security for Transport and Telematics

Rosenthaler + Partner AG

Claude Marschal

Lukas Schildknecht

Zürcher Hochschule für Angewandte Wissenschaften

Marc Rennhard

Marco Koster

Forschungsauftrag VSS 2007/904 auf Antrag der

Verbandes Schweizer Strassen- und Verkehrsfachleute

Mai 2011 **1350**

Impressum

Forschungsstelle und Projektteam

Projektleitung
Claude Marschal

Mitglieder
Marc Rennhard
Lukas Schildknecht
Marco Koster

Federführende Fachkommission

Fachkommission 9: Verkehrstelematik

Begleitkommission

Präsident
Beat Zumsteg

Mitglieder
Roland Aellen
Kurt Amstad
Simon Benz
Rudolf Blessing
Robert Hämmerli
Beat Hiller
Bruno Hofstetter
Rolf Münger
Ferdinand Prisi
Markus Schlup
Nikolaus Seifert
Jürg Uhlmann

Antragsteller

Schweizerischer Verband der Strassen- und Verkehrsfachleute

Bezugsquelle

Das Dokument kann kostenlos von http://partnershop.vss.ch herunter geladen werden.

Inhaltsverzeichnis

Zusammenfassung

Ausgangslage

Die Bedrohung von IT-Systemen durch Attacken aus dem Internet wie die Verbreitung von Malware, Trojanern oder Phishing-Seiten sowie von Sabotageakten durch professionelle Hacker nimmt laufend zu. Gleichzeitig werden in der Verkehrstelematik die Systeme vermehrt zwischen Bund, Kantonen und Agglomerationen vernetzt, um die Fachprozesse des Verkehrsmanagements noch effizienter und durchgängiger zu unterstützten. Dadurch steigt auch das Risiko von bösartigen Zugriffen auf die vernetzten Systeme. Bisher wurden diese Gefahren von den Verantwortlichen unterschiedlich beurteilt, was eine Verbesserung der Sicherheit der Systeme und des Betriebs erschwert.

Ziele

Das Ziel der Forschungsarbeit ist es, praxisorientierte Massnahmenkataloge für die Minderung des Gefahrenpotentials beim Aufbau zukünftiger VT-Systeme und der Verbesserung bereits operativer VT-Systeme bereit zu stellen.

Auf der Grundlage von bekannten Methoden für die Analyse der IT-Sicherheit sollen die Verkehrstelematik-Anwendungen, elektromechanische Anlagen für Strassen und Tunnels, Verkehrs- und Betriebsleitsysteme sowie zugehörige Netzwerk- und Kommunikationskomponenten auf Sicherheitslücken untersucht werden. Aus der Untersuchung sollen mögliche technische und organisatorische Massnahmen abgestimmt auf das spezifische Verkehrsumfeld (Bund, Gebietseinheiten, Kantone und Städte) definiert werden.

Methodik und Vorgehen

Die Forschungsarbeit orientiert sich am vierstufigen Verfahren des BSI mit einer "Ist-Analyse und Ermittlung der Schutzbedürftigkeit", einer "Bedrohungsanalyse", einer "Risikoanalyse" und einem "Sicherheitskonzept". Auf Grund der ständigen Weiterentwicklungen der Angriffstechniken sowie evtl. erweiterten Sicherheitsanforderungen neuer Systemkomponenten ist es notwendig, das Sicherheitskonzept regelmässig zu überprüfen und ggfs. anzupassen. Aus diesem Grund wird, zusätzlich zu den vier Stufen des BSI-Verfahrens, eine weitere Stufe "Empfehlung" eingeführt.

Ist-Analyse und Schutzbedürftigkeit

Bei der Ermittlung der Schutzbedürftigkeit wird festgelegt, welche IT-Anwendungen aufgrund ihres Wertes schutzbedürftig sind. Die Abgrenzung der Anwendungen erfolgt über die Auswertung der Interviews, die mit Gebietseinheiten der Verkehrsmanagementzentrale Schweiz und dem ASTRA geführt wurden. Dabei wurden betreffend IT-Sicherheit zum Teil unterschiedliche Verfahren sowie heterogene Umsetzungen identifiziert. Aus der Ist-Analyse geht hervor, dass die Anwendungen des Verkehrsmanagements und der Ereignisbewältigung im Zentrum der Betrachtung stehen.

Die klassischen Schutzziele der IT-Sicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Aus den Interviews und auch anhand der durchgeführten Literaturstudie wird eindeutig die Verfügbarkeit als höchstes Schutzziel identifiziert. Entsprechend richten sich realistische Bedrohungen auch direkt gegen die Verfügbarkeit der VT-Systeme. Die Integrität von Systemen und Daten und die Vertraulichkeit gewisser Daten sind bedeutend, damit das primäre Ziel der Verfügbarkeit erreicht werden kann.

Bedrohungsanalyse

Unter der Betrachtung des gesamten Spektrums von Angreifern (Hacker, interne Mitarbeiter, Lieferanten, …) werden realistische Bedrohungsszenarien für die VT-Systeme definiert. Dies erfolgt an Hand eines "Attack-Tree", wo systematisch die verschiedenen Angriffsmöglichkeiten auf ein System in einer Hierarchie strukturiert werden. Dabei werden als oberstes Angriffsziel "Betrieb stören" und darunter dann die Systemebenen der Verkehrstelematik sowie generelle Angriffsziele aufgeführt. Auf der untersten Ebene der Hie-

rarchie befinden sich konkrete Angriffsvektoren (Portscan, Sniffing, Social Engineering, …). Die Angriffsvektoren werden in 10 Angriffsgruppen, die jeweils ein Angriffsziel beschreiben, zusammengefasst.

Bereits umgesetzte Sicherheitsmassnahmen

Für die in der Bedrohungsanalyse identifizierten 10 Angriffsgruppen wird untersucht, wie gut die aktuell umgesetzten Sicherheitsmassnahmen sind. Als Grundlagen werden die Resultate aus den Interviews sowie Resultate aus Penetrations-Tests von Systemen und eines Servicelaptops sowie auf der AGK-Anlage im Arisdorftunnel verwendet. Es können daraus einige technische (nicht sichere Protokolle, veraltete Software-Versionen, keine Verschlüsselung, …), organisatorische (Prozesse und Dokumentation) und physische (unterschiedlicher Zugangsschutz) Schwachstellen hervorgehoben werden, die in der Risikoanalyse weiter betrachtet werden.

Risikoanalyse

Die Risikoanalyse betrachtet die Eintrittswahrscheinlichkeit und die Auswirkung der einzelnen Risiken aus einem qualitativen Blickwinkel.

Die Resultate der Risikoanalyse zeigen, dass keine Angriffsvektoren mit katastrophalen Konsequenzen und hohen Eintrittswahrscheinlichkeiten vorhanden sind. Allerdings sind doch einige Angriffsvektoren vorhanden, die kritische Konsequenzen haben und gelegentlich eintreten könnten. In diese Gruppe gehören das Installieren von Patches/OS-Updates/Malwareupdates, das Einstecken eines mit Malware verseuchten Geräts, die allgemeinen Wartungsarbeiten sowie das Bedienen von Betriebs- und Sicherheitsausrüstungen mit dem Ziel das Verkehrsystem zu stören. DoS Attacken haben zwar nur geringe Konsequenzen, könnten grundsätzlich aber häufig auftreten.

Sicherheitskonzept

Das Sicherheitskonzept umfasst eine sinnvolle Menge von Massnahmen, die für die Reduktion der in der Risikoanalyse erkannten Risiken für Betriebs- und Sicherheitsausrüstungen (BSA) relevant sind. Das Ziel ist, einer Gebietseinheit oder einer VM-Zentrale eine Checkliste zur Verfügung zu stellen, wo die Massnahmen und eine kurze Erläuterung verständlich aufgeführt sind. Dabei wird nicht unterschieden, ob eine Massnahme bereits in einzelnen Gebietseinheiten oder VM-Zentralen umgesetzt ist oder nicht.

Die Massnahmen gliedern sich in die Bereiche organisatorische Sicherheitsmassnahmen, technische Sicherheitsmassnahmen und physische Sicherheitsmassnahmen.

Folgerungen und Empfehlungen

Das Forschungsprojekt liefert folgende Folgerungen:

- In IT-Netzwerken mit BSA-Anlagen werden die IT-Schutzziele grundsätzlich anders bewertet als in herkömmlichen Netzwerken, wie zum Beispiel der Büroautomation. Das oberste Schutzziel ist eindeutig die Verfügbarkeit gefolgt von der Integrität der Daten.
- VT-Systeme können nur durch einen Mix aus technischen, organisatorischen und physischen Massnahmen effizient gesichert werden.
- Die IT-Security ist ein kontinuierlicher Prozess, wo die Gefahrenlage sich stetig aufgrund neuer und sich ändernder Bedrohungen verändert. Die Sicherheitsmassnahmen müssen deshalb laufend hinterfragt und bei Bedarf überarbeitet werden.

Aus diesen Folgerungen wird die Erarbeitung einer Richtlinie vorgeschlagen, die im Wesentlichen den Massnahmenkatalog aus dem Kapitel 9 als Grundlage verwendet.

Résumé

Situation initiale

Les menaces de systèmes informatiques par des attaques du net telles que la dispersion de malware, chevaux de Troie ou du Phishing ainsi que des actes de sabotage par des hackers professionnels augmentent constamment. En même temps les systèmes de la télématique routière de la confédération, des cantons et des agglomérations sont mis en réseau pour supporter de façon plus efficace et intégrée les processus métier de la gestion du trafic. De ce fait le risque d'accès malveillants sur les systèmes en réseau augmente. Jusqu'à présent ces dangers ont été appréciés de différentes façon par les responsables ce qui rend une augmentation de la sécurité des systèmes et de leur exploitation difficile.

Objectifs

L'objectif du projet de recherche est de fournir des catalogues de mesures orientés à la pratique pour diminuer le potentiel de dangers lors de la mise en œuvre de futurs systèmes de la télématique routière et d'améliorer celui des systèmes déjà en exploitation. A l'aide de méthodes existantes pour l'analyse de la sécurité de systèmes informatiques les applications de la télématique routière, les installations électromécaniques pour les routes et les tunnels, les systèmes de gestion du trafic ainsi que les composants des réseaux de communications doivent être analysés sur les lacunes de sécurité. A partir des résultats de l'analyse des mesures techniques et organisationnelles possibles en tenant compte de l'environnement spécifique du trafic et des transports (confédération, unités territoriales, cantons et agglomérations) seront définis.

Méthode et démarche

La recherche s'oriente au processus en quatre étapes du BSI qui prévoit une "analyse de la situation avec détermination du degré de protection", une "analyse des menaces", une "analyse des risques" et un "concept de sécurité". Du fait du développement permanent des techniques d'attaque ainsi que de l'extension éventuelle des exigences de sécurité liée à de nouvelles composantes du système, il est nécessaire de vérifier et d'adapter régulièrement le concept de sécurité. La démarche prévoit ainsi une étape supplémentaire "Recommandation" pour prendre en compte cet aspect.

Analyse de la situation avec détermination du degré de protection

Lors de la détermination du degré de protection on définit les systèmes informatiques à protéger en fonction de leur valeur. La délimitation des applications s'effectue sur la base des résultats des interviews avec des unités territoriales, la centrale Suisse de gestion de trafic et l'OFROU. Au niveau de la sécurité informatique ces interviews ont identifiés des différences dans les processus ainsi que des réalisations très hétérogènes. L'analyse montre que les applications de la gestion du trafic et de la résolution des évènements sont à considérer en priorité.

Les objectifs classiques de protection des systèmes informatique sont la confidentialité, l'intégrité et la disponibilité. A la suite des interviews et de l'étude de la littérature il résulte que l'objectif premier de la protection est la disponibilité du système. En conséquence les menaces réalistes se dirigent directement contre la disponibilité des systèmes de la télématique routière. L'intégrité des systèmes et des données ainsi que la confidentialité sont importantes pour pouvoir atteindre l'objectif premier de la disponibilité.

Analyse des menaces

Pour les systèmes de la TR des scénarii réalistes de menaces sont définis en considérant la totalité du spectre des attaques (hacker, collaborateurs internes, fournisseurs, …). Ceux-ci sont documentés à l'aide d'un "Attack-Tree" qui représente de façon hiérarchique les différentes possibilités d'attaques. L'objectif principal de l'attaque "Perturber l'exploitation" est placé au plus haut niveau de l'arbre suivis des niveaux standards de l'architec-

ture du système et des objectifs d'attaques plus généraux. Au niveau le plus bas de la se retrouvent les vecteurs d'attaques concrets (Portscan, Sniffing, Social Engineering, …). Les vecteurs d'attaques sont regroupés en 10 groupes qui décrivent chacun un objectif d'attaque.

Mesures de sécurité déjà mises en œuvre

Pour les 10 groupes d'attaques identifiés lors de l'analyse des menaces la qualité de la mise en œuvre des mesures de sécurité est examinée. L'analyse se base sur les résultats des interviews ainsi que sur des tests de pénétration sur divers systèmes, sur un portable utilisé pour la maintenance ainsi que sur le système de contrôle de vitesse par section dans le tunnel d'Arisdorf. Ces analyses permettent de mettre en évidence certaines lacunes techniques (protocoles non sécurisés, anciennes versions de logiciels, pas de cryptage, …), organisationnelles (processus et documentation) et physiques (différences dans la protection des accès) qui seront considérées plus en détail dans l'analyse des risques.

Analyse des risques

L'analyse des risques considère la probabilité d'apparition et la conséquence des risques d'un point de vue qualitatif. Les résultats de l'analyse de risques montrent qu'il n'existe pas de vecteur d'attaque avec des conséquences catastrophales et une probabilité d'apparition élevée. Cependant il existe quelques vecteurs d'attaques avec des conséquences critiques pouvant apparaître occasionnellement. Appartiennent à cette catégorie l'installation de patch/mise à jour de systèmes d'exploitation/mise à jour de protection malware, la connexion d'un appareil souillé d'un malware, les opérations de maintenance générales ainsi que la commande malveillante des équipements d'exploitation et de sécurité. Les attaques DoS n'ont que des conséquences faibles mais peuvent apparaître en principe fréquemment.

Concept de sécurité

Le concept de sécurité comporte un ensemble raisonnable de mesures nécessaires à la réduction des risques identifiés pour les EES dans l'analyse des risques. L'objectif est de mettre à disposition d'une unité territoriale ou d'une centrale de gestion de trafic une checkliste décrivant les mesures avec une explication de façon compréhensible. Le concept ne tient pas compte si une mesure est déjà mise en œuvre ou non des les unités territoriales ou des centrales de gestion du trafic. Les mesures sont classées en mesures de sécurité organisationnelles, techniques et physiques.

Conclusions et recommandations

Le projet de recherche livre les conclusions suivantes:

- Dans les réseaux informatiques des systèmes EES, les objectifs de protection informatique sont généralement évalués différemment de ceux des réseaux traditionnels, tels que la bureautique. L'objectif principal de la protection est la disponibilité du système suivi de l'intégrité des données.
- Les systèmes de la TR ne peuvent être protégés efficacement que par une combinaison de mesures techniques, organisationnelles et physiques.
- La sécurité informatique est un processus continu, où la situation des risques se modifie en permanence à cause de nouvelles menaces. Les mesures de sécurité doivent de ce fait être examinées et au besoin adaptés de façon continue.

Suite à ces conclusions, le projet de recherche propose le développement d'une directive basée essentiellement sur le catalogue de mesures du chapitre 9.

Summary

Initial situation

The threats of computing systems by attacks of the Net such as the dispersion of malware, Trojan horses or Phishing as of the acts of sabotage by professional hackers increase constantly. At the same time the traffic telematics systems of the confederation, cantons and agglomerations are networked to support in a more effective and integrated way the business processes of traffic management. Thus the risk of malicious access on networked systems increases. So far, these risks have been assessed differently by the authorities, which make an increase of the systems security and their operation difficult.

Objectives

The objective of the research project is to provide catalogs of measures directed to the practice to decrease the potential of dangers during the implementation of future traffic telematics systems and to improve the security of the systems already in operation.

On the basis of known methods for the analysis of IT security, the transport telematics applications, electro-mechanical equipment for roads and tunnels, traffic management systems and related network and communication components are examined for security vulnerabilities. From the results of the analysis, possible technical and organizational measures, taking into account the specific environment of traffic and transport (confederation, territorial units, cantons and agglomerations) will be defined.

Method and Approach

The research is based on the four steps of the BSI process which provides a "situation analysis with determination of the degree of protection, a "threat analysis", a "risk analysis" and a "security concept". Due to the continual development of techniques of attack as well as the possible extension of the safety requirements related to new system components, it is necessary to review regularly and adapt the security concept. The approach thus provides an additional step "Recommendation" to take into account this aspect.

Analysis of the situation with determination of the degree of protection

When determining the degree of protection the IT systems to be considered are defined based on their value. The delimitation of the applications is made on the basis of the results of interviews with the territorial units, the Swiss traffic management centre and FEDRO. Related to IT security these interviews have identified differences in the processes as well as very heterogeneous implementations. The analysis shows that the applications for traffic management and event management should be considered in priority.

The traditional objectives of protection of IT systems are confidentiality, integrity and availability. The outcome from the interviews and the study of literature is that the primary objective of protection is the availability of the system. Therefore the realistic threats are directed directly against the availability of traffic telematics systems. The integrity of systems and data as well as privacy is important to achieve the primary objective of availability.

Threat Analysis

For ITS systems realistic scenarios of threats are defined by considering the full spectrum of attacks (hacker, internal employees, suppliers ...). These are documented using an "Attack Tree" which represents the different possibilities of attacks in a hierarchy. The main objective of the attack "Disrupting the operation" is placed at the top level of the tree followed by the levels of the IT system architecture and more general attack targets. At the lowest level are placed the concrete attack vectors (Portscan, Sniffing, Social Engineering ...). The attack vectors are grouped into 10 groups each describing an attack target.

Already implemented security measures

For the 10 groups of attacks identified during the analysis of threats the quality of the implementation of safety measures is examined. The analysis is based on the results of the interviews, penetration tests on various systems, tests on a laptop used for maintenance as well as tests on section control in the tunnel of Arisdorf. Such analysis can highlight some technical (nonsecure protocols, old software version, no encryption ...), organizational (process and documentation) and physical (differences in access protection) gaps to be considered in more detail in the risk analysis.

Risk analysis

The risk analysis considers the likelihood and consequence of the risks on a qualitative point of view. The results of the risk analysis show that there is no attack vector with very high consequences and a high probability of occurrence. However there are a few attack vectors with critical impact that may arise occasionally. To this category belong the install of patches, OS updates, update of malware protection, the maintenance activities of the equipments as well as malicious operating of systems. DoS attacks have only small consequences but can appear frequently.

Security concept

The security concept has a reasonable set of measures needed to reduce risks identified in the risk analysis. The goal is to provide a territorial unit or a traffic management centre a checklist of measures with an understandable explanation. The concept does not take into account whether a measure is already implemented or not at the territorial units or the Swiss traffic management centre. The measures are divided into organizational, technical and physical security measures.

Conclusions and recommendations

The research project provides the following conclusions:

- In IT networks with ITS systems, the objectives of the IT-protection are generally valued differently than in traditional networks, such as office automation. The ultimate aim of protection is clearly the system availability followed by the data integrity.
- The security of ITS systems can only be assured efficiently through a mix of technical, organizational and physical measures.
- The IT security is an ongoing process, where the risk situation is continiously changing due to new and changing threats. The security measures must therefore be permanently verified and revised as needed.

From these conclusions, the research project proposes the development of a policy based essentially on the catalog of measures from Chapter 9.

1 Einleitung

1.1 Ausgangslage und Auftrag

1.1.1 IT-Sicherheit

Bei der **IT-Sicherheit** geht es um den Schutz der Informatikanwendungen vor möglichen Bedrohungen, welche die Verfügbarkeit der IT-Systeme, die Integrität und die Vertraulichkeit der verarbeiteten Informationen gefährden. Um die **Schutzbedürftigkeit** zu ermitteln, muss der Wert der Anwendungen und Informationen festgestellt werden.

Die vielfältigen **Bedrohungen**, die in der Einsatzumgebung und im IT-System eintreten können, wie beispielsweise Spannungsschwankungen, fehlerhafte Eingaben, Computer-Malware oder Hackerangriffe, müssen erkannt und erfasst werden. Dazu gehören Bedrohungen, deren Ursachen in den Schwachstellen der Informationstechnik, in menschlichem Versagen und im Missbrauch der Informationstechnik bis hin zur Computerkriminalität liegen können. Auch die Folgen von Ereignissen höherer Gewalt müssen bedacht werden. Das **Risiko** ist ein Mass für die Gefährdung, die von einer Bedrohung ausgeht. Es setzt sich aus der Wahrscheinlichkeit, mit der das Ereignis eintritt und der Höhe des Schadens, der als Folge des Ereignisses auftritt, zusammen.

Zum Schutz der IT-Anwendungen müssen **Massnahmen** in verschiedenen Bereichen ergriffen werden. Die Vorkehrungen können im baulichen, technischen, organisatorischen, personellen und politischen Bereich liegen. Massnahmen reduzieren entweder die Wahrscheinlichkeit oder die Höhe des Schadens beim Ereignisfall.

Die **Bewertung** der Schutzbedürftigkeit und der Bedrohungen ist vom Einsatzzweck, von den Eigenschaften des IT-Systems und von der Einsatzumgebung abhängig. Sie ist deshalb nicht pauschal möglich, sondern muss für jeden Einzelfall gesondert vorgenommen werden.

1.1.2 IT-Sicherheit und Verkehrstelematik

Gemäss SN 671'951 umfasst die Verkehrstelematik eine Vielzahl von Systemen mit Funktionen, die über Schnittstellen kommunizieren. Es bestehen daher grosse Abhängigkeiten zwischen den Funktionen, z.B. Verkehrsdatenerfassung → Verkehrsdatenvalidierung → Verkehrsdatenaufbereitung → Verkehrszustandsbestimmung → Verkehrsbeeinflussung. Fällt eine Funktion in der Kette aus, ist das gesamte System in Gefahr.

Die Systeme der Verkehrstelematik werden von verschiedenen Organisationseinheiten (Bund, Kantone, Städte, Dritte) betrieben. Jeder Beteiligte hat seine eigenen Anforderungen an die IT-Sicherheit aufgrund seiner technischen, betrieblichen und organisatorischen Umgebung. Durch die Notwendigkeit, die Systeme untereinander vermehrt zu vernetzen (z.B. Vernetzung von kantonalen Verkehrsleitzentralen mit der nationalen Verkehrsmanagementzentrale oder der Kantonspolizeien mit der nationalen Verkehrsinformationszentrale), entstehen neue Herausforderungen an die IT-Sicherheit.

1.1.3 Ziele

Die Ziele des Forschungsprojekts sind wie folgt formuliert:

- Festlegen der IT-Security-Regeln für die Untersuchung: z.B. IT-Security-Regeln für Datennetze des Bundes.
- Untersuchen der Verkehrstelematik-Anwendungen, elektromechanische Anlagen für Strassen und Tunnels, Verkehrs- und Betriebsleitsysteme sowie zugehörige Netzwerk- und Kommunikationskomponenten auf Sicherheitslücken.
- Beschreiben von möglichen technischen und organisatorischen Massnahmen abgestimmt auf das spezifische Verkehrsumfeld (Bund, Gebietseinheiten, Kantone und Städte).

1.1.4 Zweck

Der Zweck der Forschungsarbeit ist die Entwicklung eines IT-Sicherheitskonzepts für die Verkehrstelematik-Anwendungen. Es soll ein standardisiertes Regelwerk entstehen, das für typische Anwendungen die notwendigen IT-Sicherheitsmassnahmen definiert. Diese sollen den Verkehrstelematik-Anwendern und -Betreibern als Hilfsmittel für die Erhöhung der Datensicherheit bei der Vernetzung, innerhalb des Netzwerks und beim Zugriff von Dritten zum Beispiel für Supportzwecke dienen, und die Grundlagen für eine anwenderorientierte Normierung bieten.

1.1.5 Notwendigkeit

Der Aufbau der Verkehrstelematiksysteme ist bisher mehrheitlich aus den Bedürfnissen einzelner Betreiber aufgekommen. Diese haben ihre Systeme, optimiert auf das Anwendungsgebiet, spezifiziert und umgesetzt. Sowohl für die Erfassung des Verkehrsaufkommens als auch für die Überwachung der Verkehrssicherheit oder in der Gebührenabgabe sind somit "Insellösungen" entstanden, die in sich homogen und sicher funktionieren. Die IT-Security-Aspekte sind in diesen Systemen jeweils in Abhängigkeit der spezifischen Anforderungen berücksichtigt worden.

Durch Veränderungen in der Aufgabenverteilung der VT-Funktionen und VT-Dienste oder durch neue Anforderungen (z.B. VM-CH) entsteht das Bedürfnis die bestehenden VT-Systeme vermehrt zu vernetzen mit der Möglichkeit auf verschiedene VT-Syteme zuzugreifen oder zwischen diesen Daten auszutauschen.

Aus der Sicht der IT-Sicherheit fehlt bisher die systematische Ermittlung der Schutzbedürftigkeit und daher auch die systematische Darstellung der Anforderungen an die IT-Sicherheit. Die heterogene Landschaft einerseits und die unterschiedlichen Ziele andererseits konnten bisher nicht analysiert und in ein homogenes Sicherheitskonzept integriert werden. Darüber hinaus fehlen jegliche Grundlagen für die Erarbeitung von praxisorientierten Normen.

1.2 Abgrenzung

Das Forschungsprojekt legt den Fokus auf das Thema der Datensicherheit. Es werden dazu die Aspekte der Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität betrachtet. Einige dieser Aspekte werden in HERMES unter dem Thema "ISDS" Informationssicherheit und Datenschutz behandelt. Diese werden als Grundlage in der Untersuchung berücksichtigt.

Die Funktionale Systemarchitektur der Verkehrstelematik, gemäss SN 671'951, bildet eine sinnvolle Checkliste für die Festlegung des Untersuchungsumfangs aus der Sicht der darin definierten Funktionsblöcke. Soll eine umfassende Untersuchung der IT-Security für die Verkehrstelematik durchgeführt werden, so stehen die Struktur der Teilsysteme und die Schnittstellen im Zentrum des Verfahrens.

Die Untersuchung der IT-Security beinhaltet sowohl eine technische Komponente als auch eine organisatorische Komponente. In der Verkehrstelematik sind die Systeme in Abhängigkeit ihrer Rolle (Verkehrsdatenerfassung, Verkehrsanalyse, Verkehrssteuerung, Dienste, …) organisatorisch auf verschiedene Beteiligte verteilt. In der Forschungsarbeit werden deshalb die öffentlichen Organisationen auf Ebene Bund, Kantone, Städte sowie private Organisationen berücksichtigt. Zwingend bei der Untersuchung ist auch die Berücksichtigung sämtlicher Benutzerschnittstellen nach "Innen" (Schadenspotential - mutwillig oder fahrlässig - durch interne Mitarbeiter wie Betreiber und Systemadministratoren) und Schnittstellen nach "Aussen", insbesondere zur Öffentlichkeit und mit dem angrenzenden Ausland.

Die Forschungsarbeit wird in engem Bezug zur Praxis durchgeführt. Dies ist einerseits durch die Begleitkommission der Experten der VSS und andererseits durch den direkten Kontakt mit den Betreibern von Betriebsleitzentralen sowie Industriepartner gegeben.

Die Forschungsarbeit soll eine ganzheitliche Betrachtung der Problematik der IT-Security liefern. Es werden deshalb sowohl Systeme, die in Betrieb sind, als auch solche, die mittelfristig geplant sind, im Projekt berücksichtigt.

1.3 Methodik und Vorgehen

Das Ziel der Forschungsarbeit ist es, praxisorientierte Massnahmenkataloge für die Minderung des Gefahrenpotentials beim Aufbau zukünftiger VT-Systeme und der Verbesserung bereits operativer VT-Systeme bereit zu stellen. Um dieses Ziel zu erreichen, eignet sich ein Vorgehen angelehnt an das Verfahren des BSI auf.

Das Verfahren des BSI besteht aus vier Stufen, die in der folgenden Graphik dargestellt sind und nachgehend erläutert werden:

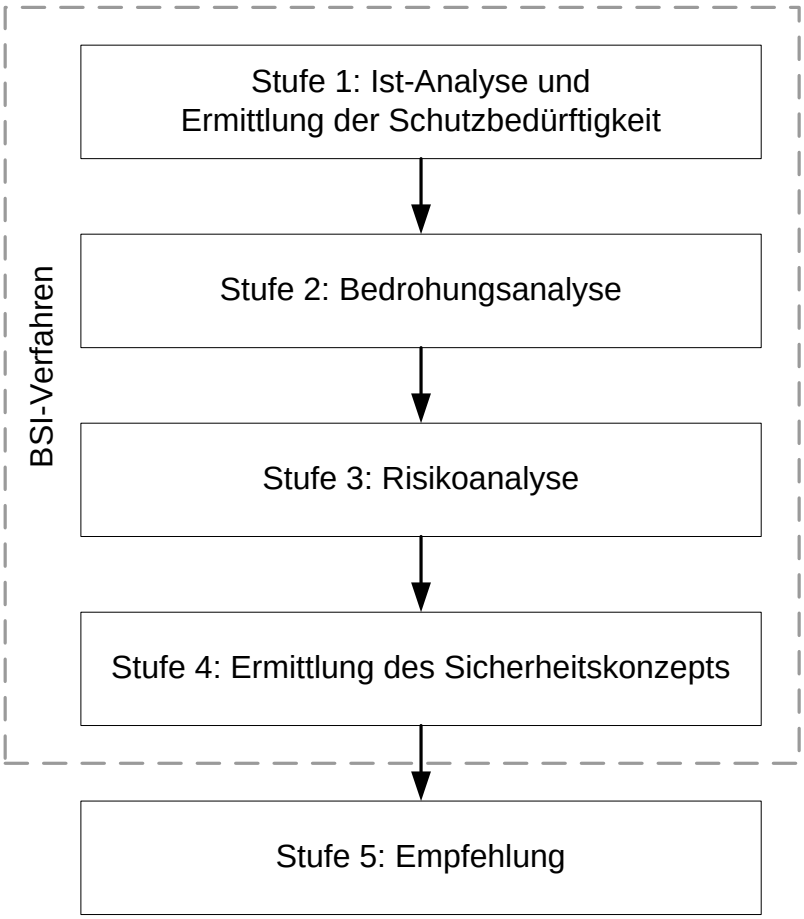


Abbildung 1: Stufen des BSI-Verfahrens (erweitert)

Dieses Verfahren wird den Zielen dieses Forschungsprojekts gerecht: der aktuelle Stand der IT-Security wird detailliert analysiert und konkrete Massnahmen werden vorgeschlagen, um allenfalls vorhandene Schwachstellen zu beseitigen. Zudem wird ein Sicherheitskonzept geliefert, das für Weiterentwicklungen eine gute Voraussetzung für ein den Anforderungen entsprechendes Sicherheitsniveau bietet. Dabei ist allerdings zu beachten, dass dieses Konzept nur eine auf dem aktuellen Wissensstand basierende Momentanaufnahme ist. Auf Grund der ständigen Weiterentwicklungen im Bereich der VT-Systeme, der Angriffstechniken und evtl. erweiterten Sicherheitsanforderungen neuer Systemkomponenten ist es deshalb notwendig, das Sicherheitskonzept regelmässig zu überprüfen und ggfs. anzupassen. Aus diesem Grund führen wir zusätzlich zu den vier Stufen des BSI-Verfahrens eine weitere Stufe "Empfehlung" ein, welche die langfristige Nutzung und Nachführung des Sicherheitskonzepts sicherstellt.

2 Literaturrecherche

2.1 Zusammenfassung

SCADA-Systeme werden zur Überwachung, Kontrolle und Steuerung von Industrieanlagen, von Systemen zur Verteilung lebenswichtiger Güter oder im Bereich des Transports und Verkehrs eingesetzt. Traditionell wurden SCADA-Netze isoliert von anderen Computer-Netzen betrieben. Es wurden proprietäre Protokolle und Komponenten verwendet. Lange Zeit galten SCADA-Systeme deshalb als unverwundbar. IT-Sicherheit spielte beim Design der Systeme keine grosse Rolle. Mit der Einführung von Standard-IT-Komponenten und -Protokollen sowie der zunehmenden Vernetzung von SCADA-Netzen mit Business-Netzwerken wurden SCADA-Netze allerdings vermehrt verwundbar.

Die Einführung von Standard-IT-Techniken bringt auch gewisse organisatorische Probleme mit sich. Das liegt an den unterschiedlichen Schutzanforderungen von SCADA-Netzen und Business-Netzen. In Business-Netzen sind Vertraulichkeit und Integrität die höchsten Schutzziele. In SCADA-Netzen hingegen hat Verfügbarkeit die oberste Priorität. Aus diesem Grund müssen beispielsweise Malwarescanner und Patches mit Vorsicht gehandhabt werden. Auch Penetration-Tests müssen vorsichtig durchgeführt werden. Da SCADA-Systemkomponenten meist über sehr wenig Rechenpower verfügen, wird auch der Einsatz von kryptographischen Funktionen erschwert.

Frühere Field-Visits und Penetration-Tests haben gezeigt, dass SCADA-Systeme über zahlreiche Sicherheitslücken verfügen. Das liegt mitunter daran, dass sich SCADA-Systeme meist über geographisch weite Gebiete erstrecken und gewisse Teile des Netzes nicht rund um die Uhr physisch überwacht werden können. Ausserdem sind die Systeme sehr heterogen. Oft werden unsichere proprietäre Protokolle eingesetzt. Die Kommunikation erfolgt zum Teil im Klartext. Nur schwache Authentifizierungsmechanismen werden verwendet. Da das Patch-Management ein sehr heikles Thema bei SCADA-Systemen ist, sind viele Systeme nicht auf dem aktuellsten Stand gehalten. Die Angriffe auf SCADA-Systeme häufen sich zudem stetig. Ausserdem werden immer mehr Angriffe "von Aussen" durchgeführt. Ein Angriff auf ein SCADA-System kann potenziell sehr schwere Folgen haben (einerseits Folgen für die Sicherheit der Menschen, andererseits auch Folgen für die Umwelt, sowie finanzielle Folgen).

Technische Massnahmen zum Schutz von SCADA-Systemen alleine können keine nachhaltige Sicherheit gewährleisten. Ein Mix aus technischen, prozeduralen und betrieblichen Massnahmen ist erforderlich. IT-Security ist ein stetiger Prozess. Die Gefahrenlandschaft verändert sich fortlaufend. Deshalb müssen die Risiken regelmässig neu überprüft werden und, falls angebracht (unter Berücksichtigung der entstehenden Kosten, bzw. der Folgen bei Eintreffen einer Bedrohung), entsprechende Massnahmen zur Verbesserung der Sicherheit eingeleitet werden. Eine IT-Security-Governance (oder Administration) stellt sicher, dass ein konsequenter und angebrachter Ansatz verfolgt wird und zwar über die gesamte Organisation.

Einige Institutionen haben bereits gewisse Guidelines bezüglich SCADA-Security veröffentlicht. Ausserdem existieren einige Standards und Guidelines zum Thema IT-Security im Allgemeinen.

2.2 Überblick SCADA Systeme

Prozessleitsysteme werden zur Überwachung, Kontrolle und Steuerung von Industrieanlagen, von Systemen zur Verteilung lebenswichtiger Güter (Strom, Wasser, Brennstoffe, usw.) oder im Bereich des Transports und Verkehrs (Eisenbahnen, Verkehrsleitsysteme, Post, usw.) eingesetzt [Beirer, 2008][MELANI, 2009][Lingwood, 2008]. Immer häufiger trifft man in diesem Zusammenhang auch auf den englischen Begriff SCADA (Supervisory Control and Data Acquisition) [Beirer, 2008][Lingwood, 2008]. Traditionell wurden solche SCADA-Systeme isoliert von Computernetzen betrieben. Ausserdem wurden nur sehr spezialisierte proprietäre Systeme und Individuallösungen verwendet. SCADA-Systeme wurden deshalb lange Zeit als "unverwundbar" angesehen [Byres, 2007]. Effizienz und hohe Verfügbarkeit waren die wichtigsten Kriterien beim Design von SCADA-Systemen - IT-Security wurde dabei kaum beachtet. SCADA-Netzwerke erstrecken sich oft über geografisch weite Gebiete [Igure, 2006][Carlson, 2002]. SCADA-Systeme haben meist sehr hohe Lebenszeiten, was Konsequenzen für aktuelle sowie zukünftige Systeme hat: aktuelle Systeme, welche bereits seit mehreren Jahren im Einsatz sind, wurden ohne Gedanken über IT-Security entworfen, wie bereits kurz angetönt. Das Prinzip von "Security by Obscurity" (Sicherheit soll dadurch gewährleistet sein, dass niemand die genauen Implementierungen kennt) wurde angewandt, mit dem Hintergedanken, dass die Systeme sowieso isoliert sind und nur von wenigen, vertrauensvollen Personen kontrolliert werden. Eine zweite Konsequenz ist, dass die Installationen meist sehr heterogen sind (in Bezug auf die Hersteller der Subsysteme und der verwendeten Technologien der Subsysteme) [Deck, 2004].

Allerdings werden aufgrund des steigenden Kostendrucks vermehrt offene Standards eingesetzt (Standardprotokolle wie Ethernet und TCP/IP). Dadurch konnten Entwicklungs- und Anschaffungskosten gesenkt und die Kompatibilität zwischen den Systemen verschiedener Hersteller erhöht werden. Allerdings werden die Systeme durch den Einsatz von Standard-IT-Protokollen und -Systemen auch vermehrt verwundbar. Das "Security by Obscurity"-Prinzip kann nicht mehr angewandt werden, da die offenen Standards und die damit verbundenen Sicherheitslücken sehr gut verstanden sind. Ausserdem werden SCADA-Netzwerke vermehrt an Business-Netzwerke angeschlossen, was die Gefahr zusätzlich erhöht [MELANI, 2009][Deck, 2004][Beirer, 2008][Falco, 2004][Igure, 2006][Mitretek, 1997].

Die Einführung von Standard-Techniken aus der klassischen IT-Welt bringt zudem gewisse technische und organisatorische Probleme mit sich. Das liegt unter anderem auch an den sehr unterschiedlichen Ansprüchen, die in der Office-IT und in der Prozesssteuerung an die Technik gestellt werden. So müssen in Steuerungssystemen häufig Echtzeitanforderungen erfüllt werden, welche in der klassischen IT-Welt weitgehend irrelevant sind. Auch die Definition der Sicherheits-Schutzziele ist in den beiden Welten völlig verschieden. So sind die wichtigsten Schutzziele in der Büro-IT-Welt Vertraulichkeit und Integrität der zu verarbeitenden Daten. Systemverfügbarkeit spielt eine eher untergeordnete Rolle. Im Prozessnetz und in Produktionssystemen sind die Schutzziele hingegen genau umgekehrt. Die Verfügbarkeit der Anlagen ist hier meistens das wichtigste Ziel [Beirer, 2008][Deck, 2004][Kilman, 2005]. SCADA-Systeme werden oft verwendet, um zeitkritische Vorgänge zu steuern. In diesem Fall können Standard-IT-Security-Praktiken ungeeignet sein. Anti-Malware-Scanner können beispielsweise ein System zeitweise verlangsamen, was für SCADA-Systeme unakzeptabel sein kann [Carlson, 2002][Kilman, 2005][Byres, 2007][CPNI]. Auch das Einspielen von Security-Patches muss mit Vorsicht betrachtet werden. Die Möglichkeit, dass ein Patch kritische Funktionen behindern kann, ist bei SCADA-Systemen nicht tolerierbar [Kilman, 2005][Byres, 2007]. Offenbar gibt es sogar zwei Einträge in der "Industrial Security Incident Database" (ISID) des British Columbia Institute of Technology (BCIT), wo unachtsames Einspielen von Patches zu Problemen geführt hat [Byres, 2007]. Auch die Durchführung von Penetration-Tests muss sorgfältig gehandhabt werden [Duggan, 2005][Robertson, 2003][Graham, 2006][CPNI]. Die Systeme können nicht einfach neu gestartet werden, um eventuelle Schwierigkeiten zu beheben [Deck, 2004]. Ausserdem verfügen die eingesetzten Komponenten (Sensoren, Aktoren) meist über sehr wenig Ressourcen, was den Einsatz von kryptographischen Protokollen sehr erschwert [Falco, 2004][Deck, 2004][Igure, 2006]. Allerdings muss hier auch in Betracht gezogen werden, dass Daten in SCADA-Netzwerken unterschiedliche

"Lebenszeiten" haben als Daten in Business-Netzen. So müssen die Daten in SCADA-Netzen oft nur für wenige Minuten geschützt werden im Unterschied zu Business-Netzen, wo die Daten über Tage, Monate oder gar Jahre geschützt werden müssen [Kilman, 2005].

Gemäss des Fachhandbuch BSA des ASTRA [ASTRA, 2010] sind SCADA-Systeme strukturiert aufgebaut. Die Systeme verfügen über verschiedene Ebenen, was eine klare Zuordnung der Funktionen voraussetzt. Folgende Ebenen kommen zur Anwendung gemäss [ASTRA, 2010]:

- Feldebene: Die Feldebene dient zur Erfassung von Daten und zur Ausgabe von Stellwerten eines Prozesses.
- Einzelsteuerebene: Auf dieser Ebene erfolgt die Ansteuerung der Feldebene, in der Regel durch mehr oder weniger autonome Steuerungen. Diese Ebene verbindet den Feldbus mit der Leistungselektronik.
- Gruppenleitebene: unterteilt die Prozesslogik auf mehrere Bereiche (z.B. Verkehrsabschnitt bei einer Verkehrssteuerung).
- Prozessleitebene: In dieser Schicht erfolgt die Umsetzung der Prozesssteuerungslogik.
- Bedienebene: ermöglicht die Visualisierung für den Operator und damit die Schnittstelle zum Menschen (Human Machine Interface, HMI).

2.3 Gefahren in SCADA-Systemen

Gemäss einem Bericht von Andrew Hildick-Smith [Hildick-Smith, 2005] können Gefahren durch beabsichtigte Angriffe auf SCADA-Systeme wie folgt gruppiert werden:

- Malware: Wie jedes IT-System sind auch SCADA-Systeme potentiell verwundbar durch Viren, Würmer, Trojaner und Spyware. Solche Malware kann Daten korrumpieren, die Kommunikation im Netzwerk überlasten und Back-Doors oder Key-Loggers installieren.
- Insider: Verärgerte Mitarbeiter stellen eine der grössten Gefahren dar, da sie die Systeme gut kennen und eventuelle Schwachstellen mutwillig ausnützen können.
- Hacker: Hacker sind externe Leute, die versuchen, in ein System einzudringen auf Grund der "Herausforderung".
- Terroristen: Terroristen sind vor allem daran interessiert, einen möglichst grossen physischen Schaden anzurichten, in dem sie zum Beispiel versuchen, SCADA-Systeme mit "falschen Werten" zu füttern, die Kontrolle der SCADA-Systeme zu übernehmen oder das Monitoring und Controlling der SCADA-Systeme auszuschalten.

Der Bericht von Andrew Hildick-Smith zeigt auch ein paar Gefahren/Schwachstellen auf, die speziell in SCADA-Netzwerken vorhanden sein können. Folgende Punkte werden u.a. genannt:

- Erfahrung der Mitarbeiter: Mitarbeiter von SCADA-Systemen sind es gewohnt, die Kontrollsysteme am Laufen zu halten. Es könnte die Ansicht vorhanden sein, dass die damit verbundenen Schutzziele (Verlässlichkeit und Verfügbarkeit) in Konflikt zu IT-Security-Massnahmen stehen. Die Entwicklung von Sicherheits-Policies könnte für SCADA-Mitarbeiter ein fremdartiges Konzept sein. Ausserdem könnte es sein, dass SCADA-Mitarbeiter die Empfehlung von IT-Fachleuten missbilligen.

- Schwachstellen im Betriebssystem: Die typischen IT-Betriebssystem-Schwachstellen sind auch in SCADA-Systemen vorhanden. Der Unterschied ist, dass die Systeme in Business-Umgebungen regelmässig aktualisiert werden können, was in SCADA-Systemen nicht so einfach ist, wie wir weiter oben gesehen haben. Insbesondere sei hier auch auf die Problematik der Verträglichkeit unterschiedlicher Antimalware-Software bei SCADA-Systemen erwähnt.

- Authentifizierung: In SCADA-Systemen sind oft gemeinsame Passwörter vorhanden (z.B. ein einziges Passwort für alle Leute im Picket-Dienst etc.). Gemeinsame Passwörter sind für die Mitarbeiter zwar sehr praktisch, allerdings geht dadurch auch jeglicher Sinn von Authentifizierung und Accountability verloren. Die Vertraulichkeit der Authentifizierung wird oft dadurch beeinträchtigt, dass Benutzernamen und Passwörter im Klartext gesendet werden.

- Remote-Zugang: Viele SCADA-Systeme verfügen über einen Remote-Zugang. Das kann eine Einwahlleitung sein (z.B. ISDN) oder eine VPN-Verbindung über das Internet.

- Verbindungen zwischen Systemen: Je mehr verschiedene Systeme miteinander verbunden werden, desto stärker ist das SCADA-System den verschiedenen Gefahren ausgesetzt. Wie bereits weiter oben diskutiert, werden Business-Netze aus wirtschaftlichen Überlegungen vermehrt mit SCADA-Netzen verbunden.

- Monitoring und Grundschutz: "Intrustion-Detection-Systeme" (IDS), also Systeme, welche einen potentiellen Angriff protokollieren können, werden im SCADA-Umfeld kaum eingesetzt. Firewalls und Antimalware-Software werden nicht universell eingesetzt. Das Durchschauen von Log-Files wird sehr oft vernachlässigt.

- Feld-Systeme: Systeme, die in der Feld-Ebene eingesetzt werden, haben oft eine sehr beschränkte Rechenleistung und wenig Speicher, so dass kryptographische Protokolle kaum eingesetzt werden können, wie bereits weiter oben diskutiert. Ein zweites Problem ist, dass solche Systeme oft für eine sehr lange Zeit im Einsatz sind.

- SCADA-Software: Applikationen, die im SCADA-Umfeld eingesetzt werden, verfügen oft über bescheidene Sicherheitsmassnahmen und weisen auch andere Design-Schwächen auf.

- Öffentlich verfügbare Informationen: Es ist meistens sehr einfach, an Informationen über SCADA-Systeme heranzukommen. So werben z.B. Systemlieferanten mit ihrer Erfahrung und geben Informationen über frühere Kunden preis. Weiterhin werden zum Teil in Ausschreibungen Informationen über die Netwerkkonfiguration mit IP-Adressen abgegeben.

- Physische Sicherheit: SCADA-Systeme erstrecken sich meist über grosse Distanzen, wobei viele Standorte unbemannt sind. Der physische Schutz der Systeme wird daher umso wichtiger. Allerdings sind verschiedene Verschlusssysteme nicht absolut hundertprozentig sicher.

An einer Black-Hat-Konferenz[1] im Jahre 2006 präsentierten Robert Graham und David Maynor ebenfalls gewisse Sicherheitsprobleme in SCADA-Netzwerken [Graham, 2006]. Robert Graham und David Maynor haben Penetration-Tests bei mehreren SCADA-Systemen durchgeführt. Unter anderem bestätigen sie, dass SCADA-Systeme kaum auf dem aktuellen Stand gehalten werden. Ausserdem stellten sie fest, dass sich viele SCADA-Betreiber gar nicht bewusst sind, wie stark sie mit dem Internet verbunden sind. Offenbar existieren viele unkontrollierte Zugänge zum Internet. Sogar scheinbar isolierte Netze werden über Links oder Notebooks mit dem Internet verbunden. Im Folgenden wollen wir etwas detaillierter auf ein paar Punkte eingehen, die Robert Graham und David

[1] http://www.blackhat.com/

Maynor während ihren Penetration-Tests gefunden haben:

- Wireless-Zugang bei einem Kraftwerk: Graham und Maynor haben bei einem Stromkraftwerk einen offenen Wireless-Zugang gefunden. Über DHCP konnten sie problemlos eine IP-Adresse beziehen. Nach ein paar Scans fanden sie heraus, dass der Wireless-Zugang mit dem gesamten Office-Netz verbunden war. Schliesslich kamen sie über das Office-Netz auf ein Solaris-System im Kontroll-Netz, indem sie einen 10-jahre alten Exploit[2] verwendeten.

- "Falsche" Netzwerk-Diagramme: Bei einer Ölfirma haben Graham und Maynor festgestellt, dass die Netzwerkpläne nicht der wirklichen Konfiguration entsprechen. So waren die verschiedenen Netzwerke sehr wohl an gewissen Punkten miteinander verbunden, obwohl das nirgendwo auf den Plänen vermerkt war.

- Notebooks: Ebenfalls bei einer Ölfirma musste die Produktion bei gewissen Anlagen gestoppt werden aufgrund eines Computer-Wurms. Der Wurm hat sich ausgebreitet, als jemand ein Notebook am System angeschlossen hat um ein gewisses Problem an der Ölplattform zu diagnostizieren.

- Öffentliche Informationen: Graham und Maynor bestätigen, dass es sehr einfach ist, detaillierte Informationen über die verwendeten Komponenten in SCADA-Systemen zu erhalten.

- Klartext-Kommunikation: Graham und Maynor bestätigen, dass die Kommunikation in SCADA-Netzen oft im Klartext erfolgt.

- Physischer-Zugang: Wie bereits weiter oben diskutiert, ist es sehr schwierig, SCADA-Systeme, welche geographisch sehr weit ausgedehnt sein können, physisch abzusichern.

- Auditing: Es wurden gemeinsame "Gruppen-Passwörter" verwendet. Dadurch können Aktivitäten von arglistigen Mitarbeitern kaum zurückverfolgt werden. Vorhandene IDS wurden kaum aktualisiert oder regelmässig überwacht.

- Modems: Modems waren in vielen Systemen vorhanden, damit die Lieferanten einen einfachen Wartungszugang haben. Das Problem war, dass die meisten Modems "Banner"[3] hatten. Mit Hilfe der Banner kann man über Google leicht an weitere Informationen herankommen, wie zum Beispiel Bedienungsanleitungen für die Geräte. Oft hatten die Geräte auch Standard-Benutzernamen und -Passwörter, die niemals seit der Auslieferung geändert wurden. Auch "Backdoor-Benutzernamen/Passwörter", die nicht geändert werden konnten, waren zum Teil vorhanden.

- Unsichere Applikationen: Graham und Maynor führten auch gewisse Source-Code-Audits von Applikationen durch. So stiessen sie auf unsichere Programmierpraktiken (zum Beispiel wurde Input von Netzwerk als vertrauenswürdig angesehen, ausserdem wurden Programmierkonstrukte verwendet, die bekannte Sicherheitslücken aufweisen). Authentifizierungs- oder Verschlüsselungsmassnahmen werden kaum berücksichtigt.

[2] Programm, welches die Sicherheitslücke in einem Computersystem ausnützt
[3] Banner sind für Hacker potentiell interessante Informationen über ein System wie zum Beispiel Hersteller, Systemversion, etc.

Eine Präsentation von Jerry Litteer und Ken Rohde listet auch gewisse Punkte auf, die während "Field-Visits" bei SCADA-Systemen gefunden wurden [Litteer, 2005]. Im Folgenden sollen ein paar dieser Punkte aufgelistet werden:

- Standard-Accounts und -Passwörter
- Gast-Accounts aktiv
- Port-Security wird kaum durchgesetzt
- Nicht verwendete Software befindet sich auf Systemen
- Nicht benötigte Services sind aktiv, z.B. auch die automatische Erkennung von USB-Sticks
- Shares mit exklusiven Schreibrechten
- Firewalls:
    - Firewall-Rules sind nicht kommentiert
    - Generische oder vereinfachte Rules werden verwendet
    - Alte oder temporäre Rules werden nicht entfernt
    - Logging nicht aktiviert
    - Zum Teil werden Firewalls mit direkten Verbindungen umgangen
- IDS werden kaum eingesetzt.

Aktuelle Untersuchungen bestätigen, dass die Anzahl der Attacken auf SCADA-Netzwerke ständig zunimmt. Zudem fand auch eine Verlagerung der Angreifer statt. So sind 70 Prozent der in der ISID (Industrial Security Incident Database) protokollierten Vorfälle vor dem Jahr 2000 auf Grund von Unfällen oder verärgerten Mitarbeitern. Seit 2001 sind fast 70 Prozent der Vorfälle auf Grund von externen Angriffen [Litteer, 2005][Igure, 2006][Byres, 2007].

Da SCADA-Systeme kritische Infrastrukturen steuern, ist es von grosser Bedeutung, die Sicherheit dieser Systeme zu gewährleisten. Ein Angriff auf ein SCADA-System kann verheerende Folgen haben, so kann zum Beispiel die öffentliche Gesundheit und Sicherheit gefährdet werden, die Umgebung kann beschädigt werden und nicht zuletzt kann ein solcher Angriff auch grossen finanziellen Schaden anrichten [Giani, 2008][Deck, 2004][Igure, 2006].

2.3.1 Aktuelle Vorfälle

Im Zusammenhang mit SCADA-Systemen gibt es immer mal wieder publik werdende IT-Vorfälle, welche die Brisanz des Themas deutlich aufzeigen.

So berichtete das Online-Portal von Austin News im Dezember 2009 von einem Vorfall in Austin, Texas (USA)[4]. Die Wechseltextanzeigen auf einer hoch frequentierten Strecke zeigten dort plötzlich die Meldung "Zombies ahead" (in etwa "Zombies zu erwarten") an. Angreifern ist es also scheinbar gelungen, in die lokalen VT-Systeme einzudringen, um die "falsche Anzeige" zu platzieren. Obwohl solche Vorfälle im ersten Moment zwar durchaus amüsant wirken, ist es ein absolut ernst zu nehmendes Thema: Es zeigt, dass die lokalen VT-Systeme grundsätzlich auf externe Angriffe verwundbar sind. Statt der "harmlosen" Falschanzeigen hätten die Angreifer wahrscheinlich noch weit schlimmere

[4] http://www.kxan.com/dpp/news/Road_signs_warn_of_zombies

Angriffe starten können. Man stelle sich vor, was passiert wäre, wenn Terroristen die VT-Systeme übernommen hätten.

Im September 2010 wurde publik, dass die iranische Nuklearanlage Buschehr Opfer eines sehr dedizierten Cyber-Angriffs wurde. Der Trojaner Stuxnet hatte laut der iranischen Agentur Mehr 30'000 Computer befallen. Offenbar greift Stuxnet sehr gezielt die von Siemens stammenden PLC-Systeme (Programmable Logic Controller) an, welche in den iranischen Industrieanlagen verwendet werden. Stuxnet nutzt dabei gemäss Quellen u.a. vier bis dato unbekannte, nicht öffentlich publizierte Schwachstellen aus (Zero-Day Exploits). Die Autoren des Trojaners mussten also irgendwie die Möglichkeit haben, die von Iran eingesetzen Siemens-Produkte genaustens auf Schwachstellen zu analysieren. Nicht zuletzt auch wegen der sehr ausgeklügelten Angriffsmechanismen wird deshalb vermutet, dass staatliche Organisationen hinter dem Angriff stehen. Laut NZZ-Online stellt der Experte und Buchautor Arne Schönbohm denn auch fest, dass "der Cyberspace mittlerweile als fünftes militärisches Schlachtfeld neben dem Boden, der Luft, dem Wasser und dem Weltraum gesehen werde". Stuxnet sei u.a. über USB-Sticks verbreitet worden, sodass auch Systeme befallen werden konnten, die gar nicht direkt über das Internet erreichbar waren. Laut Symantec handelt es sich offenbar um den ersten Wurm, welcher Industriesysteme nicht nur ausspionieren, sondern auch deren Funktionsweise gezielt manipulieren kann[5] [6] [7] [8] [9].

In der Literatur findet man ausserdem weitere bekannte Cyber-Vorfälle im Zusammenhang mit SCADA-Systemen. Im Folgenden sollen ein paar dieser Vorfälle kurz erwähnt werden. Genauere Infos zu den jeweiligen Vorfällen können in der Literatur nachgelesen werden [Graham, 2006][Hildick-Smith, 2005][Gresser, 2006]:

- Das Davis-Besse Atomkraftwerk in Ohio (USA) war während fast einem Jahr offline, nachdem der SQL-Slammer-Wurm im Januar 2003 zwei Systeme des Kraftwerks infiziert und für fünf, bzw. sechs Stunden lahm gelegt hat. Der Wurm erreichte die Systeme offenbar über einen Remote-Contractor-Link zum Firmennetz, welches seinerseits mit dem Prozessnetzwerk verbunden war.

- Im Jahr 2000 liess der frühere Angestellte Vitek Boden eine Million Liter Abwasser in die Küstengewässer von Queensland in Australien ausfliessen.

- Im Jahr 1992 hat ein früherer Angestellter von Chevron das Notfall-Alarmierungssystem in 22 Staaten der USA deaktiviert, was bis zu einem Vorfall, bei dem eine Alarmierung hätte ausgelöst werden sollen, unbemerkt blieb.

- Im Jahr 1997 gelingt es einem Teenager bei NYNEX einzubrechen und die Kommunikation beim Worcester Flughafen in Massachusetts (Air- und Ground-Communications) für sechs Stunden lahmzulegen.

- Im Jahr 2000 hat die Russische Regierung zugegeben, dass es Angreifern gelungen sei, die Kontrolle über die grösse Erdgas-Pipeline der Welt zu übernehmen (Gazprom).

- Im August 2003 wurden die Computer-Systeme von CSX Transportation durch eine Malware infiziert, wodurch der Passagier- und Frachtzugverkehr in Washington DC angehalten werden musste.

---

[5] http://blogs.forbes.com/andygreenberg/2010/09/22/theories-mount-that-stuxnet-worm-sabotaged-iranian-nuke-facilities/

[6] http://www.nzz.ch/nachrichten/international/iran_bestaetigt_cyber-angriff_durch_stuxnet_1.7686307.html

[7] http://www.schneier.com/blog/archives/2010/10/stuxnet.html

[8] http://www.heise.de/newsticker/meldung/Stuxnet-Wurm-kann-Industrieanlagen-steuern-1080584.html

[9] http://www.spiegel.de/netzwelt/netzpolitik/0,1518,720043,00.html

- Am 8. Januar 2008 ist es einem Teenager (14 Jahre alt) gelungen, sich in das Schienenkontrollsystem des Tramsystems der Stadt Lodz (Polen) einzuhacken. Offenbar ist dem Teenager irgendwie gelungen, mit einer modifizierten Fernseher-Fernbedienung die Weichensteller zu bedienen, wodurch vier Tram-Wagen entgleist sind[10].

2.4 IT-Security-Policies und bestehende Guidelines bezüglich SCADA-Security

Ein System kann nicht alleine durch technische Mittel abgesichert werden. Werden die technischen Mittel unachtsam eingesetzt, können trotz aller technischer Mittel Sicherheitslücken entstehen. Angebrachtes Verhalten aller Mitarbeiter wird vorausgesetzt, um eine best mögliche Sicherheit zu garantieren [Deck, 2004][Igure, 2006][CPNI].

Während der letzten 10 Jahre haben viele Firmen, welche sehr stark von der Informationstechnologie (IT) abhängig sind, gute IT-Security-Praktiken entwickelt. In der SCADA-Industrie besteht hier noch grosser Nachholbedarf [Igure, 2006].

Um Sicherheitsprobleme effektiv zu bekämpfen, muss SCADA-Sicherheit nachhaltig sichergestellt werden und zwar während des gesamten Lebenszyklus des Systems, inklusive Design, Installation, Betrieb, Wartung und Stilllegung. Nur die Einführung einer effektiven Security-Governance kann diese Voraussetzungen erfüllen [Campbell, 2003]. IT-Security-Praktiken müssen dabei speziell auf SCADA-Systeme angepasst werden [Robertson, 2003][CPNI].

Ein Bericht der Sandia National Laboratories (siehe Kapitel 0) [Campbell, 2003] enthält Empfehlungen, wie eine effektive Security-Administration (Governance) implementiert werden kann. Zunächst zählt der Bericht drei Komponenten für die Sicherstellung einer nachhaltigen Sicherheit auf:

- Es braucht eine effektive Security-Administration: Nur durch stetige Evaluation und Aufrechterhaltung kann Sicherheit garantiert werden. Effektive und nachhaltige Sicherheit ist deshalb abhängig von einem effektiven Security-Management.

- Technologie muss bezüglich Sicherheit verbessert werden: Wünschenswerte Verbesserungen sind u.a. sichere Protokolle, "billige" Verschlüsselung[11], Application-Layer-Stateful-Inspection für Firewalls, Accounts und Logging für Remote Telemetry Units (RTUs).

- Administration und Implementierung muss durch Dritte beurteilt werden (Assessment): Regelmässige Assessments durch Dritte sind nötig, um Probleme aufzudecken, die unentdeckt bleiben, entweder weil die Organisation "zu nahe" an den Problemen dran ist oder weil neue Taktiken und Tools der Organisation nicht bekannt sind.

Nur das Zusammenspiel der drei oben genannten Komponenten führt schlussendlich zu einer *nachhaltigen Sicherheit*. Neue, sichere Technologien alleine bringen keine nachhaltige Sicherheit. Assessments durch Dritte können nur eine Momentaufnahme der momentan vorhandenen Schwachstellen aufzeigen.

Die Empfehlungen für eine effektive Security-Administration des Berichts von Sandia werden sehr gut und prägnant von einem Bericht von Vinay M. Igure et al. [Igure, 2006] zusammengefasst: Zunächst müssen SCADA-Betreiber eine umfassende Liste von Sicherheitszielen definieren, welche erfüllt werden müssen, damit die Geschäftsziele des Betreibers erfüllt werden können. Diese Menge von Sicherheitszielen wird als "Control-

[10] http://www.theregister.co.uk/2008/01/11/tram_hack/

[11] Mit "billiger" Verschlüsselung ist gemeint, dass die benötigten kryptographischen Berechnungen nicht zu "teuer" (rechenintensiv) sein sollten (aus dem Grunde, dass Komponenten in der Feldebene meist nur über wenige Rechenressourcen verfügen).

Framework" bezeichnet. Sicherheitsziele können durchgesetzt werden durch den Einsatz einer guten "Security-Policy", einem "Security-Plan", welcher auf der Security-Policy aufsetzt und "Guidelines zur Implementierung" [Igure, 2006][Campbell, 2003][Kilman, 2005] (siehe auch Abbildung 2: SCADA Administrations-Hierarchie [Campbell, 2003]).

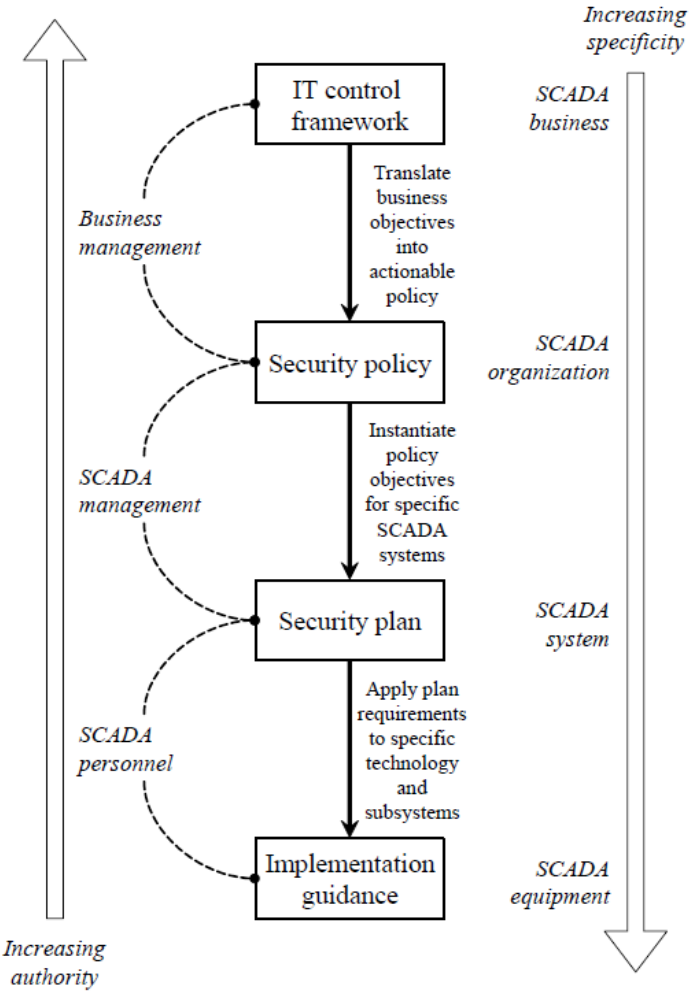


Abbildung 2: SCADA Administrations-Hierarchie

Entscheidend für den ganzen Prozess ist auch ein guter Konfigurationsmanagementplan und ein Auditierungs- und Assessmentplan.

Es gibt keine gemeinsame Security-Policy, welche von allen Firmen gemeinsam verwendet werden kann, da jede Firma unterschiedliche Sicherheitsziele verfolgt. Sandia hat deshalb ein Framework entwickelt, welches bei der Erstellung einer Security-Policy behilflich sein soll (dazu später mehr). Der Security-Policy muss ein Security-Plan folgen, welcher die Implementierung, den Betrieb und die Wartungsdetails sauber dokumentiert. Die Firmen können dazu auf bestehende und weit verbreitete Security-Standards zurückgreifen (siehe Kapitel 2.5).

IT-Security ist ein kontinuierlicher Prozess. SCADA-Netzwerke müssen regelmässig auf neue Schwachstellen geprüft und Software und Hardware müssen auf dem aktuellen Stand gehalten werden. Im Zusammenhang mit "regelmässiger Wartung" spricht man oft auch vom "Konfigurationsmanagement". Konfigurationsmanagement kann besonders bei SCADA-Systemen schwierig sein, wie bereits weiter oben diskutiert.

Das SCADA-Security-Policy-Framework von Sandia wird im Detail in einem Paper von Domique Kilman et al. [Kilman, 2005] beschrieben. Abbildung 3: SCADA-Security-Policy-Framework [Kilman, 2005] zeigt einen schematischen Aufbau des Frameworks. Wir wol-

len das Framework hier nicht im Detail besprechen (dazu sei auf die Literatur verwiesen). Das Framework gibt aber einen guten Überblick darüber, welche Bereiche durch die Security-Policy abgedeckt werden sollen oder müssen.

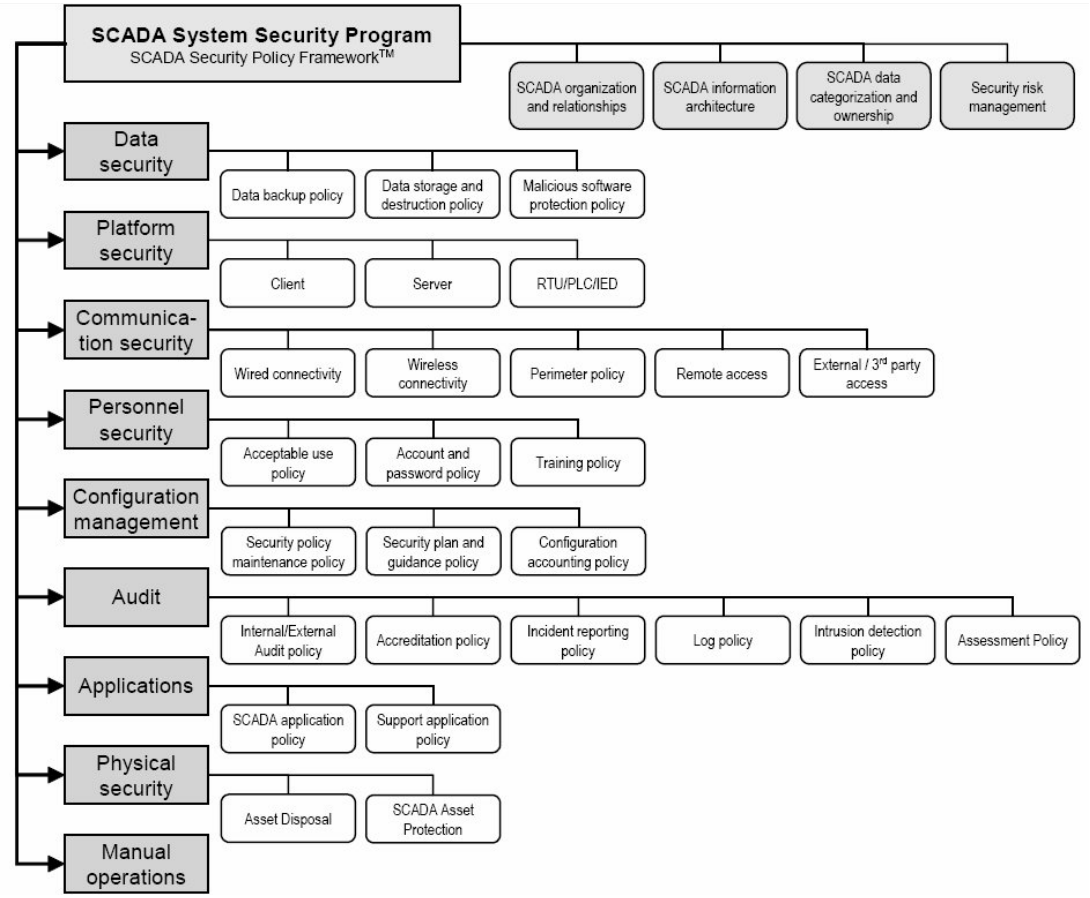


Abbildung 3: SCADA-Security-Policy-Framework

Ganz allgemein gesagt ist die Security-Policy ein formales Dokument, in welchem beschrieben wird, was durch Personen und Systeme in einer Organisation gemacht werden darf und was nicht. Der Inhalt der Security-Policy wird bestimmt durch die Sicherheitsziele einer Unternehmung und durch Resultate von Risiko-Beurteilungen. Die einzelnen Punkte in einer Security-Policy sind *Regeln* - keine Vorschläge oder Guidelines, welche die Mitarbeiter befolgen können oder nicht. Diese Regeln müssen klar und konsequent durchgesetzt werden. Security-Policies beinhalten keine detaillierten Konfigurationsregeln. Detaillierte Einstellungen und Konfigurationsregelen werden im "Security-Plan" oder bei den "Guidelines zur Implementierung" beschrieben [Kilman, 2005].

Eine Security-Policy sollte über folgende Unterkapitel verfügen [Kilman, 2005]:

- **Zweck** der Security-Policy
- **Geltungsbereich (Scope):** Hier wird spezifiziert, was alles durch die Security-Policy abgedeckt wird (zum Beispiel Maschinen, Menschen, Standorte, etc.)
- **Policy:** Hier werden die eigentlichen Regeln definiert (was darf, bzw. was darf nicht gemacht werden)
- **Verantwortlichkeiten:** Hier wird definiert, wer für was verantwortlich ist gemäss der Policy
- **Referenzen/Behörden:** Hier wird auf andere Policies oder Gesetze verwiesen, die ebenfalls eingehalten werden müssen (zum Beispiel Vorgaben des Bundes,

der Kantone, etc.)

- **Revision History:** Hier wird vermerkt, welche Änderungen am Dokument wann und von wem gemacht wurden

- **Vollzug:** Hier werden die Konsequenzen beschrieben, die im Falle einer Nichtbeachtung der Regeln, die in der Security-Policy definiert sind, in Kraft treten. Eventuelle rechtliche Schritte können hier auch vermerkt werden.

- **Ausnahmen:** Falls Ausnahmen, die von den Regeln der Security-Policy abweichen, vorhanden sind, müssen diese einzeln dokumentiert werden. Dazu gehört u.a., wie eine Ausnahme erlangt werden kann, wer Ausnahmen bewilligt und wo entsprechende Dokumentationen abgelegt werden.

In einer Präsentation bestätigt Bernie Robertson, dass sichere Technologien alleine nicht ausreichen, um eine vollumfängliche Sicherheit zu gewährleisten [Robertson, 2003]. Stattdessen braucht es einen Mix aus technischen, prozeduralen, personellen und betrieblichen Voraussetzungen. Robertson präsentiert zu diesem Zweck ein SCADA-Security-Framework, welches vom CPNI (Centre for the Protection of National Infrastructure - GB - siehe Kapitel 2.5) entwickelt wurde, um Prozesskontrollsysteme vor elektronischen Angriffen zu schützen [CPNI]. Das Framework besteht aus den folgenden sieben Elementen:

- **Understand the Business Risk:** Bevor ein Programm zur Verbesserung der Sicherheit gestartet werden kann, muss eine Organisation zuerst die Geschäftsrisiken verstehen, die durch potentielle Gefährdung der Prozesskontrollsysteme entstehen können. Nur mit guter Kenntnis der Geschäftsrisiken kann eine Organisation fundierte Entscheidungen über angemessene Sicherheits-Level und benötigte Verbesserungen aktueller Praktiken treffen. Die Geschäftsrisiken sollten regelmässig neu beurteilt werden, da sich die Gefahren ständig ändern. Um die Geschäftsrisiken zu bestimmen, muss eine formale Risikobeurteilung durchgeführt werden. Dazu gehören die folgenden vier Schritte:

    - **Understand the systems:** Hier geht es darum zu dokumentieren, welche Systeme überhaupt existieren, welche Rollen die einzelnen Systeme haben, wo sich die Systeme befinden, etc.

    - **Understand the threats:** Hier müssen Bedrohungen für die Prozesskontrollsysteme identifiziert und evaluiert werden. Mögliche Bedrohungen können sein: Denial of Service (DoS), gezielte Angriffe (zum Beispiel durch Hacker), Unfälle, etc.

    - **Understand the impacts:** Hier geht es darum, mögliche Folgen aufzuzeigen, falls eine mögliche Bedrohung tatsächlich eintreffen sollte. Mögliche Folgen könnten sein: Image-Verlust, finanzielle Verluste, Verletzung von Vorschriften (zum Beispiel Umwelt- oder gesundheitliche Vorschriften), etc.

    - **Understand the vulnerabilities:** Hier geht es darum, die Schwachstellen des Prozesskontrollsystems aufzudecken.

- **Implement Secure Architecture:** Hier geht es darum, basierend auf der Beurteilung der Geschäftsrisiken gewisse Massnahmen einzuleiten, welche die Sicherheit verbessern sollen. Dabei handelt es sich sowohl um technische, wie auch um prozedurale und betriebliche Massnahmen. Das Framework enthält einige Good-Practice-Guidelines bezüglich Netzwerkarchitektur, Firewalls, Remote-Access, Antimalware-Software, E-Mail und Internet-Zugang, System-Hardening, Backups und Recovery, Physische Sicherheit, System-Monitoring, Wireless Networking, Security Patching, Prüfungen des Personals, Passwörter und Accounts, Dokumentation des Security Frameworks, Security-Testing, etc.

- **Establish Response Capabilities:** Mögliche Bedrohungen für die Prozesskontrollsysteme verändern und entwickeln sich laufend. Die SCADA-Betreiber sollten deshalb die Sicherheit regelmässig neu überprüfen. Dazu gehören die Identifikation, Evaluation und Reaktion auf neue Schwachstellen, auf Veränderungen der Bedrohungen sowie auf elektronische "Sicherheitsvorfälle" (Würmer, Hacker-Angriffe). Formale Response-Management-Prozesse gewährleisten, dass jegliche Veränderungen der Risiken frühzeitig erkannt und nötige Massnahmen eingeleitet werden können.

- **Improve Awareness and Skills:** Der Erfolg aller technischer oder prozeduraler Security-Massnahmen ist direkt vom "menschlichen Faktor" abhängig. Das SCADA-Personal ist oft nicht vertraut mit IT-Security. Gleichzeitig sind IT-Security-Fachleute oft nicht vertraut mit Prozesskontrollsystemen. Das gegenseitige Verständnis kann mit Awareness-Programmen, Ausbildungen und Trainings verbessert werden.

- **Manage Third Party Risk:** SCADA-Betreiber sollten mit Lieferanten zusammenarbeiten um existierende Systeme abzusichern. Insbesondere sollten die Lieferanten dazu ermutigt werden, Sicherheit in ihren Produkten pro-aktiv zu berücksichtigen.

- **Engage Projects:** Sicherheit sollte bei System-Entwicklungen von Anfang an ein wesentlicher Bestandteil sein. Versuche, Sicherheit zu einem späteren Zeitpunkt zu integrieren, können teuer enden und erst noch weniger effektiv sein.

- **Establish Ongoing Governance (Policy, Standards and Assurance):** Eine formale Governance für das Management der Sicherheit der Prozesskontrollsysteme stellt sicher, dass ein konsequenter und geeigneter Ansatz verfolgt wird und zwar über die gesamte Organisation. Ohne eine solche Governance kann der Schutz ungenügend sein, was die Organisation zusätzlichen Risiken ausliefert. Ein effektives Governance-Framework enthält klare Rollen und Verantwortlichkeiten, eine stets aktuell gehaltene Security-Policy, Standards für das Management von Risiken von Prozesskontrollsystemen und die Zusicherung, dass die Security-Policy und die Standards tatsächlich angewendet werden.

Abbildung 4: SCADA-Security-Framework gibt einen guten Überblick über das von Bernie Robertson präsentierte Framework [Robertson, 2003].

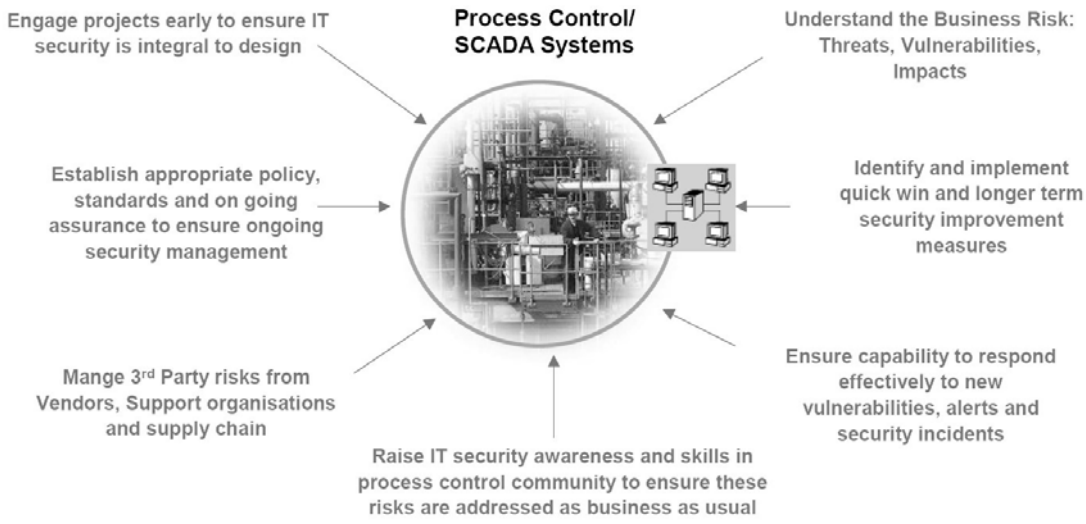


Abbildung 4: SCADA-Security-Framework

Bereits 1997 hat die Firma Mitretek Systems einen Bericht erstellt für das "Intelligent Transportation Systems (ITS) Joint Program Office" (USA) mit dem Titel "Protecting Our Transportation Systems: An Information Security Awarenewss Overview" [Mitretek, 1997]. Der Bericht enthält ein Framework für ein "Information-Security-Programm". Das Framework besteht aus den folgenden sechs Punkten:

- **Strategic Security Planning:** Es muss sichergestellt werden, dass IT-Sicherheit in einem systematischen Ansatz behandelt wird und mit den Zielen und der Mission der ITS-Unternehmung übereinstimmt.

- **Security Policy Analysis & Definition:** Hier werden Regeln definiert, welche sicherstellen sollen, dass die Sicherheitsziele (bezüglich Vertraulichkeit, Integrität und Verfügbarkeit) erreicht werden. Details für genaue Implementierungen werden im nächsten Schritt betrachtet.

- **Secure Solutions Integration:** Eine angebrachte Kombination aus technischen und nicht-technischen IT-Security-Massnahmen muss implementiert werden, um eine kostengünstige, robuste und benutzerfreundliche Lösung zu erreichen.

- **Security Awareness, Education & Training:** Benutzer müssen über die Bedrohungen, über Massnahmen zum Schutz des Systems vor den Bedrohungen und über die Sicherheits-Abläufe informiert werden.

- **Security Management:** Es braucht eine fortwährende Sicherheitsadministration, welche sowohl prozedurale wie auch technische IT-Security-Features miteinbezieht. Management-Prozeduren sollen periodisch überprüft und falls nötig angepasst werden. Dadurch wird die Systemsicherheit gewährleistet, auch in einem Notfall.

- **Security Assessment & Testing:** Resultate eines Security-Assessments informieren Systemadministratoren und Manager über den Sicherheitszustand des Systems. Assessments sind gute Indikatoren dafür, wie gut Sicherheits-Prozeduren befolgt werden. Ausserdem geben Assessments einen direkten Rückschluss darauf, wie gut technische Sicherheitsmassnahmen implementiert wurden. Normalerweise werden Assessments von unabhängigen Teams durchgeführt, so dass die Testresultate möglichst unverfälscht wiedergegeben werden können.

Die verschiedenen Frameworks bzw. Guidelines, die in diesem Kapitel diskutiert wurden, mögen auf den ersten Blick unterschiedlich aussehen. Allerdings finden sich gewisse Kernaussagen in allen Frameworks wieder. So ist die Erkenntnis, dass technische Massnahmen alleine keine nachhaltige Sicherheit gewährleisten können, entscheidend. Ein Mix aus technischen, prozeduralen und betrieblichen Massnahmen ist erforderlich. IT-Security ist ausserdem ein stetiger Prozess. Die Gefahrenlandschaft verändert sich ständig. Deshalb müssen die Risiken regelmässig neu überprüft werden und, falls angebracht (unter Berücksichtigung der entstehenden Kosten, bzw. der Folgen bei Eintreffen einer Bedrohung), entsprechende Massnahmen zur Verbesserung der Sicherheit eingeleitet werden. Eine IT-Security-Governance (oder Administration) stellt sicher, dass ein konsequenter und angebrachter Ansatz verfolgt wird und zwar über die gesamte Organisation.

2.5 Wichtige Institutionen

Dieses Kapitel soll bestimmte Institutionen auflisten, welche sich mit SCADA-Security oder IT-Security befassen und auch entsprechende Guidelines oder sonstige Dokumente/Hilfsmittel publiziert haben.

- Centre for the Protection of National Infrastructure (CPNI)[12]: Das CPNI erteilt Ratschläge, wie Schwachstellen bei kritischen Infrastrukturen in Grossbritannien

[12] http://www.cpni.gov.uk/

verhindert werden können. Das CPNI hat einen Katalog mit SCADA-Security-Good-Practice-Guidelines verfasst[13]. Ähnliche Organisationen in anderen Ländern sind:

  - US-CERT (US Computer Emergency Readiness Team)[14]: Das "Control Systems Security Program" (CSSP) des US-CERT hat eine Web-Page mit Standards und Referenzen rund um das Thema "Cyber Security in Kontrollsystemen" aufgeschaltet[15]. Unter Anderem findet man dort Ressourcen über die Erstellung von Policies; Patch-, Passwort-, und Konfigurationsmanagement; Remote-Zugänge; VPNs; etc.

  - GovCERT (Australian Government Computer Emergency Readiness Team)[16]

  - CCIP (Centre for Critical Infrastructure Protection - New Zealand)[17]

  - CCIRC (Canadian Cyber Incident Response Centre)[18]

- BITKOM[19]: BITKOM ist das Sprachrohr der IT-, Telekommunikations- und Neue-Medien-Branche. BITKOM vertritt mehr als 1.300 Unternehmen, davon gut 950 Direktmitglieder. Ein sehr interessantes Dokument, welches BITKOM veröffentlicht hat, ist der "Kompass der IT-Sicherheitsstandards" [BITKOM, 2007]. Das Dokument gibt einen guten Überblick über verschiedene internationale Standards zum Thema IT-Sicherheit. Ein weiteres interessantes Dokument unter dem Titel "Sicherheit für Systeme und Netze in Unternehmen - Einführung in die IT-Sicherheit und Leitfaden für erste Massnahmen" wurde veröffentlicht [BITKOM b]. Das letzte Dokument, welches hier erwähnt werden soll, wurde unter dem Titel "IT-Risiko- und Chancenmanagement in Unternehmen - Ein Leitfaden für kleinere und mittlere Unternehmen" veröffentlicht [BITKOM a].

- Bundesministerium des Innern (D)[20]: Insbesondere zwei Dokumente, welche vom Deutschen Bundesministerium des Innern verfasst wurden, sollen an dieser Stelle erwähnt werden: Zum Einen ist das der "Nationale Plan zum Schutz der Informationsstrukturen (NPSI)" [BMI, 2005], zum Anderen die "Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)" [BMI].

- Bundesamt für Sicherheit in der Informationstechnik (BSI - D)[21]: Zwei Dokumente, welche vom Bundesamt für Sicherheit in der Informationstechnik verfasst worden sind, sollen an dieser Stelle erwähnt werden: "Kritische Infrastrukturen in Staat und Gesellschaft" [BSI] und "Informationstechnik in der Prozessüberwachung und -steuerung" [BSI, 2008].

- Zentrum für sichere Informationstechnologie (A-SIT - A)[22]: Das Zentrum für sichere Informationstechnologie gibt im Auftrag des Österreichischen Bundeskanzleramtes (BKA) das "Österreichische Informationssicherheitshandbuch" heraus [A-SIT, 2007]. Das primäre Thema ist die Sicherheit der Information unter Verwendung sicherer Technologien, welche über die reine Informationstechnologie (IT) hinausgehen. In einem eigenen Kapitel wird die industrielle Sicherheit behandelt. Die Themen sind bewusst allgemein formuliert und richten sich sowohl an die öf-

[13] http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx
[14] http://www.us-cert.gov
[15] http://www.us-cert.gov/control_systems/csstandards.html
[16] http://www.ag.gov.au/www/agd/agd.nsf/page/GovCERT
[17] http://www.ccip.govt.nz/about-ccip.html
[18] http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx
[19] http://www.bitkom.org/
[20] http://www.bmi.bund.de
[21] http://www.bsi.bund.de
[22] http://www.a-sit.at/

fentliche Verwaltung als auch an die Wirtschaft bzw. Industrie.

- Sandia National Laboratory (USA)[23]: Das Sandia National Laboratory beherbergt das "Center for SCADA Security". Zum Aufgabengebiet des Centers gehören Forschung, Trainings, Red-Teams und Entwicklung von Standards. Gesponsert durch das US. Department of Energy (DoE) wurde in Zusammenarbeit mit dem Idaho National Engineering and Environmental Laboratory (INEEL) das National SCADA Testbed (NSTB) entwickelt [Fink, 2006]. Auf der Website befinden sich ausserdem verschiedene Dokumente zum Thema SCADA[24].

- National Institute of Standards and Technology (NIST - USA)[25]: Das Process Control Security Requirements Forum (PCSRF) unterstützt die Entwicklung von Standards für SCADA-Security[26]. Unter anderem hat NIST auch ein Handbuch zum Thema Computer Sicherheit herausgegeben [NIST, 1995], sowie einen Leitfaden zur Entwicklung von Security-Plänen [Bowen, 2006]. Weitere interessante NIST-Publikationen findet man auf der US-CERT-Seite[27].

- Melde- und Analysestelle Informationssicherung (MELANI - CH)[28]: In der Melde- und Analysestelle Informationssicherung MELANI arbeiten Partner zusammen, welche im Umfeld der Sicherheit von Computersystemen und des Internets sowie des Schutzes der schweizerischen kritischen Infrastrukturen tätig sind. Die Webseite von MELANI richtet sich an private Computer- und Internetbenutzer, sowie an kleinere und mittlere Unternehmen (KMU) der Schweiz. MELANI veröffentlicht unter Anderem halbjährliche Lageberichte, welche die wichtigsten Tendenzen und Entwicklungen rund um Vorfälle und Geschehnisse in den Informations- und Kommunikationstechnologien erläutern.

- Informatikstrategieorgan Bund (ISB - CH)[29]: Das Informatikstrategieorgan Bund (ISB) ist die Stabstelle des Informatikrates Bund (IRB). Es erarbeitet die Entscheidungsgrundlagen für die strategische Steuerung der Informatik in der Bundesverwaltung. Im ISB werden unter Anderem die Grundlagen der Informatiksicherheit für die Bundesverwaltung erarbeitet. Die Bundesinformatikverordnung (BinfV) und die Sicherheitsweisungen (WIsB) regeln die Zuständigkeiten und das Vorgehen bei der Umsetzung der Sicherheitsvorgaben.

- Verein InfoSurance (CH)[30]: Seit der Gründung 1999 setzt sich der Verein InfoSurance dafür ein, Privatpersonen und KMU für das Thema IT-Sicherheit zu sensibilisieren.

- ISO27000 Verzeichnis[31]: Die ISO 27000 Normenserie ist speziell für IT-Sicherheitaspekte reserviert. Unternehmen können sich nach diesen Standards zertifizieren lassen.

[23] http://www.sandia.gov
[24] http://www.sandia.gov/scada/documents.htm
[25] http://www.nist.gov
[26] http://www.isd.mel.nist.gov/projects/processcontrol/
[27] http://www.us-cert.gov/control_systems/csstandards.html
[28] http://www.melani.admin.ch/
[29] http://www.isb.admin.ch/
[30] http://www.infosurance.ch/site/
[31] http://www.27000.org

3 Schutzbedürftigkeit, Ist-Zustand

In der Ermittlung der Schutzbedürftigkeit wird aus der Sicht der Nutzer des IT-Systems ausgewählt und abgegrenzt, was Gegenstand der weiteren Untersuchungen ist. Dazu wird festgelegt, welche IT-Anwendungen aufgrund ihres Wertes schutzbedürftig sind.

Die Ermittlung der Schutzbedürftigkeit erfolgt mit folgenden Schritten:

- Erfassen der IT-Anwendungen und der zu verarbeitenden Informationen: Die Erfassung erfolgt mittels Interviews. Die Resultate sind in diesem Kapitel dargestellt.
- Festlegen der Schutzziele für die erfassten Anwendungen und Informationen. Dazu werden sie bezüglich der Grundbedrohungen bewertet. Die Bewertung erlaubt eine Auswahl der risikoträchtigen IT-Anwendungen. Die Synthese befindet sich im Kapitel 4.

Im folgenden Kapitel sind die aus den Interviews gewonnen Erkenntnisse zusammengefasst. Das Kapitel 3.1 enthält eine Übersicht der geführten Interviews und eine kurze Zusammenfassung. In den Kapitel 3.2 bis 3.13 werden die Informationen aus den Interviews strukturiert nach relevanten Themen der IT-Security dargestellt.

3.1 Interviews, Übersicht

Das primäre Ziel der Interviews ist es, sicherheitskritische Systeme, Daten und Prozesse zu identifizieren, welche in späteren Phasen des Projekts detailliert analysiert werden sollen. Es ging in dieser Phase noch nicht darum, Sicherheitsaspekte im Detail zu erfassen und zu untersuchen, sondern einen Gesamtüberblick zu erhalten.

Es wurden total 7 Interviews geführt mit Vertretern von der Verkehrsmanagementzentrale, verschiedenen Betriebsleitzentralen sowie mit dem ASTRA Bereich Verkehrssicherheit. Die einzelnen befragten Organisationen können der nachfolgenden Zusammenstellung entnommen werden. Für jedes Interview ist eine kurze Zusammenfassung der gewonnenen Erkenntnisse über die Sicherheitsaspekte der jeweiligen Systeme und Anlagen enthalten. Die gewonnen Erkenntnisse basieren ausschliesslich auf den Aussagen der Interviewpartner.

Organisation	Zentras, Stans / Gebietseinheit X
Interviewpartner	Heinz Schild, Systembetreuer übergeordnete Systeme (NW, OW) Ivo Achermann, Systembetreuer übergeordnete Systeme (LU)
Zusammenfassung	Es existiert eine heterogene Systemlandschaft mit grundsätzlich drei unabhängigen Netzen der Kantone LU, NW/OW und ZG. Diese Netzarchitektur ist historisch bedingt durch den früher kantonsweisen Betrieb der Anlagen. Als potenzielle Schwachstellen sind im Wesentlichen zu nennen: – Zugriff von externen Systemlieferanten (zur Systemwartung) mittels nur schlecht kontrollierbaren ISDN-Zugängen. – Zugriff von externen mobilen Geräten. Dabei ist der Zugriff mittels VPN grundsätzlich gut gesichert. Die Gefahr liegt in diesem Fall eher in der nicht kontrollierbaren Nutzung der dafür vorgesehenen Laptops für andere Zwecke oder in der Verwendung von nicht vorgesehenen Endgeräten und der damit verbundenen Gefahr des Einschleusens von Malware etc. in das System. – Fehlende IT-Sicherheitsrichtlinien für die Umsetzung und den Betrieb der Systeme.

Organisation	Betriebsleitzentrale Urdorf / Gebietseinheit VII
Interviewpartner	Kurt Amstad, Sektionsleiter Infrastruktur Strasse Christoph Schibli, Sektionsleiter Information Technology
Zusammenfassung	Die Systeme sind redundant ausgelegt und in sich autonom. Als einziges kritisches System ist das gesamte Kommunikationsnetz zu nennen. Als einzige realistische Bedrohung wird gemäss Interviewpartner ein "physischer" Angriff angesehen. Es gibt grundsätzlich keine Verbindungen nach aussen. Ausnahmen sind die Verbindung mit der KAPO Zürich. Ausserdem werden die neusten Malwaredefinitionen aus dem Internet von einem Norton-Server bezogen. Schliesslich können Zulieferer innerhalb eines be-

	schränkten Zeitrahmens auf spezifische Bereichsrechner zugreifen.

Organisation	Amt für Betrieb Nationalstrassen, Flüelen / Gebietseinheit XI
Interviewpartner	Markus Schuler
Zusammenfassung	Das gesamte Netz ist von externen Netzen entkoppelt. Das Kommunikationsnetz ist nicht segmentiert. Die Betriebssysteme der Betriebsrechner wie auch deren Anti Malware-Software werden regelmässig über einen zentralen Update-Server aktualisiert. Kritische Systeme sind redundant gehalten. Das Kommunikationsnetz ist ebenfalls redundant aufgebaut. Als grösstes Risiko für das System werden die durch die Systemlieferanten eingespielten Updates/Patches der Systeme betrachtet, da dies häufig direkt - ohne vorgängige Tests - auf dem produktiven System erfolgt.

Organisation	NSNW AG, Sissach / Gebietseinheit VIII
Interviewpartner	Stephan Vögeli, Leiter Betriebs- und Sicherheitsausrüstungen (BSA) Daniel Schärer, IT-Manager BSA Markus Würgler, Projektleiter BSA
Zusammenfassung	Die Systeme sind redundant ausgelegt und in sich autonom. Als kritisch zu betrachten sind die Zugriffe der Lieferanten. Diese erfolgen heute mit eigener Hardware, die von der NSNW nicht kontrolliert werden kann. Weiterhin ist das Kommunikationsnetz mit seinen Komponenten als kritisch zu betrachten.

Organisation	ASTRA, Bereich Verkehrssicherheit
Interviewpartner	Volker Fröse, Projektleiter Abschnitttsgeschwindigkeitskontrollanlagen
Zusammenfassung	Im Rahmen dieses Interviews wurde das sich in der Pilotphase befindliche System der Abschnittsgeschwindigkeitskontrollen untersucht. Bei der Abschnittsgeschwindigkeitskontrolle handelt es sich je um isolierte Systeme. Das System selbst speichert keine Daten. Bei Geschwindigkeitsüberschreitungen werden Daten an das Netz der Polizei übermittelt. Die Systeme werden automatisch betrieben. Jegliche Manipulation am System wird protokolliert. Die Integrität der Daten ist von entscheidender Bedeutung, da diese in juristischen Verfahren Bestand haben müssen. Ein Ausfall des Systems ist nicht kritisch.

Organisation	Verkehrsmanagementzentrale Schweiz in Emmen (VMZ-CH)
Interviewpartner	Marcel Balli, Fachverantwortlicher Informatik Daniel Landolt, Bereichsleiter Zentrale Informatik ASTRA Laurence Junker, ISB-O ASTRA
Zusammenfassung	Die Netzwerke der Büroautomation und VM sind getrennt. Als kritisch zu betrachten sind die organisatorischen Elemente: fehlende Policies mit den Lieferanten, die aufgrund des hohen Zeitdrucks beim Aufbau der VMZ-CH zu wenig berücksichtigt wurden. Es existieren diverse Verbindungen nach Aussen und nach innen. Lieferanten können sowohl vor Ort als auch Remote auf die Systeme zugreifen.

Organisation	ASTRA
Interviewpartner	Jürg Steiner, Projektleiter "Integrierte Applikationen" (INA)
Zusammenfassung	Bei diesem Interview wurde der Stand betreffend IT-Security im Projekt INA diskutiert. INA ist in zwei Realisierungsphasen unterteilt: – Phase 1: Erstellen von Applikationen für die Operatoren in den Leitzentralen und bei der Polizei. – Phase 2: Zentrales Schalten von Anlagen und Publikation von Informationen auf Internet. INA ist unterteilt in ein Basissystem (liefert die Basisdienste, auf denen die Fachdienste sich abstützen werden). In der Voranalyse (2008-2009) war das Thema IT-Security eher untergeordnet. Es gab nur minimale Anforderungen an die IT-Security. In der Zwischenzeit wurde das Thema höher eingestuft, da durch eine Begleitgruppe eine Risikobeurteilung durchgeführt

wurde. Dabei wurden die Bedrohungen (Risiken) in folgende fünf Kategorien unterteilt:

- Höhere Gewalt (Bsp.: "Personenausfall", "Grossveranstaltungen, Demonstrationen, Krawalle", "Feuer, Wasser, Blitz, etc.", etc.)
- Organisatorische Mängel (Bsp.: "Fehlende Betriebsmittel", "Fehlende Kontrollen, Tests, Auswertungen", "Fehlende Regelungen oder Prozesse", etc.)
- Menschliche Fehlhandlung (Bsp.: "Fahrlässigkeit, Unbeabsichtige Beschädigung", "Fehlerhafte Administration", "Nichtbeachtung Vorschriften", etc.)
- Technisches Versagen (Bsp.: "Datenverlust", "Hardwaredefekt", "Softwareschwachstelle", etc.)
- Vorsätzliche Handlungen (Bsp.: "Abhören, Auswerten, Analysieren, Hacken, Spoofing", Bösartige Software, Trojaner und Malware", etc.)

Die betrachteten Bedrohungen wurden dabei sehr generell formuliert, wie oben ersichtlich ist. Jede Bedrohung (Risiko) wurde gemäss den Kriterien Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit beurteilt. Zu diesem Zweck wurde für jede einzelne Bedrohung ein Wahrscheinlichkeitswert (Eintrittswahrscheinlichkeit) ermittelt (Wert zwischen 1 "unwahrscheinlich" und 5 "häufig" - die einzelnen Kategorien werden dabei dadurch unterschieden, wie häufig ein Event/Risiko innerhalb einer gewissen Anzahl Tage eintritt: z.B. unwahrscheinlich = 1 Mal alle 100'000 Tage; häufig = fast ein Mal täglich). Ausserden wurden für jede Bedrohung vier Werte für das Schadensausmass (je ein Wert für die Beeinträchtigung der Vertraulichkeit, Verfügbarkeit, etc. durch die entsprechende Bedrohung) bestimmt (Wert zwischen 1 "vernachlässigbar" und 4 "katastrophal" - die einzelnen Kategorien werden u.a. nach finanziellen Schäden unterschieden, aber auch durch Einschränkung gesetzlicher und vertraglicher Pflichten, Umweltschäden, Umfälle, Krankheiten, Verletzung der Persönlichkeitsrechte, etc.). Dadurch konnten pro Bedrohung insgesamt vier "Risikowerte" (Produkt aus Wahrscheinlichkeit und Schadensausmass) berechnet werden (je für Vertraulichkeit, Verfügbarkeit, etc.). Aus der Risikoanalyse entstanden minimale Sicherheitsanforderungen, die jetzt noch verfeinert werden. Ziel ist, dass diese Anforderungen vom Lieferanten des INA-Basissystems umzusetzen sind.

3.2 Netzwerkinfrastruktur

In diesem Unterkapitel soll untersucht werden, wie gut die verschiedenen Netze bei den Interviewpartnern voneinander separiert sind, welche Kommunikationskanäle- und Protokolle eingesetzt werden, ob und wie die Kommunikation gesichert wird und ob kritische Systemkomponenten redundant ausgelegt sind. Zusammengesetzt erhalten wir so einen Überblick über die vorhandene Netzwerkinfrastruktur.

Praktisch alle Interviewpartner haben angegeben, dass die verschiedenen Netze gut voneinander getrennt sind. Eine Ausnahme bildet AfBN: Hier werden virtuelle LANs verwendet, welche jeweils mehrere Anlagen wie zum Beispiel Lüftung oder Beleuchtung zusammenfassen. Die VLANs sind untereinander durch Firewalls entkoppelt. Einzelne VLANs erstrecken sich aber teilweise über die ganze Gebietseinheit und können wegen des Datenaustausches zum Leitsystem und der Tunnelreflexe zu anderen Anlagen aus technischen Gründen nicht weiter segementiert werden. Dies wird vom Interviewpartner als Schwachstelle betrachtet.

Bei den eingesetzten Kommunikationskanälen und -protokollen scheint es keine allzu grosse Übereinstimmung zwischen den verschiedenen Interviewpartnern zu geben. Bei Zentras wird in der Regel OPC[32] zwischen den Komponenten verwendet. Zentras setzt zum Teil auch proprietäre Protokolle ein. Ausserdem verfügen kritische Komponenten bei Zentras über eine zusätzliche Leitung, so dass beim Ausfall aller höherwertigen Kommunikationen ein Rückfall in einen sicheren Zustand gewährleistet ist. Zentras verwendet im Rechenzentrum TCP/IP als Basisprotokoll. Im Netz Luzern sollen ausserdem bei künftigen Systemen die Applikationsprotokolle auf XML basieren. In Urdorf basieren die Protokolle auch auf XML. Bei der Abschnittsgeschwindigkeitskontrolle (AGK) des ASTRA erfolgt der Austausch der Daten innerhalb und zwischen den Komponenten verschlüsselt. Bei den festen Anlagen erfolgt die Kommunikation über ein eigens für die AGK verlegtes Glasfasernetz des ASTRA. Bei der geplanten mobilen AGK-Anlage werden Daten mittels GSM und VPN bzw. per WLAN zwischen den Komponenten übermittelt.

[32] http://www.opcfoundation.org/

Auch bei der Sicherung der Kommunikation werden zum Teil unterschiedliche Techniken eingesetzt. Bei Zentras werden Firewalls zur Sicherung eingesetzt. Ports und zugreifende Rechner werden überwacht. Der ISDN-Zugriff erfolgt über Remote Access Service (RAS): es können nur konfigurierte, bekannte Anrufnummern einwählen. Auch bei AfBN werden Ports (inkl. IP-Adressen) überwacht. Ein Fernzugriff ist nur über dedizierte Laptops möglich. Der Zugriff erfolgt dabei über VPN. Der VPN-Zugang ist über einen USB-Schlüssel gesichert. Jeder Fernzugriff muss angemeldet und individuell vom Systembetreiber freigegeben werden. Die Freigaben sind zeitlich klar eingeschränkt. Die Laptops lassen nur die VPN-Verbindung mit dem Betriebsnetz zu, eine andere Verbindung (z.B. Internet) ist nicht möglich. Auch in Urdorf ist der Zugriff auf Bereichsrechner für Lieferanten gesichert und zeitlich begrenzt. Bei der AGK des ASTRA ist die Punkt-zu-Punkt-Kommunikation verschlüsselt.

Die meisten Interviewpartner haben bestätigt, dass kritische Komponenten redundant ausgelegt sind. Eine Ausnahme bildet die AGK des ASTRA, wo eine redundante Auslegung der Systeme als nicht relevant betrachtet wird. Bei Zentras sind die Netzwerke nur logisch, nicht jedoch physisch redundant gehalten (die Redundanz verläuft im selben physischen Kabel, so dass bei einem Unterbruch des Kabels auch die Redundanz ausfällt). Bei AfBN bestehen für wichtige Systeme (z.B. Server, Disks, Netzwerkanschlüsse) Redundanzen, welche zum Teil auch räumlich getrennt sind. Nach Möglichkeit wurden auch alle Lichtwellenleiter (LWL) in getrennten Kabelkanälen verlegt. In Urdorf sind die Glasfasernetze redundant ausgelegt. Systeme sind autonom und in sich geschützt. Bei NSNW sind das Videomanagementsystem und das Server-Leitsystem, sowie der Netzwerk-Backbone redundant ausgelegt.

Zusammenfassung:

- Die Netze sind im Allgemeinen gut isoliert mittels VLANs und/oder Firewalls.
- Es werden oft dedizierte Netze eingesetzt.
- Zum Teil kommen proprietäre Protokolle zum Einsatz. TCP/IP und XML-basierte Applikationsprotokolle werden auch eingesetzt.
- Zur Sicherung der Kommunikation wird zum Teil Port-Überwachung und Überwachung der zugreifenden Rechner durchgeführt. Teilweise erfolgt die Kommunikation auch verschlüsselt (u.a. kommt VPN zum Einsatz).

3.3 Remote-Access und öffentliche Schnittstellen

Je mehr Schnittstellen nach Aussen existieren, desto stärker wird ein System angreifbar. Deshalb ist es entscheidend, auch im Hinblick auf die detaillierte Risikoanalyse, dass alle Schnittstellen nach Aussen bekannt sind. In diesem Unterkapitel wird untersucht, welche Schnittstellen zu anderen Systemen existieren und welche öffentlichen Schnittstellen vorhanden sind, bzw. welche Möglichkeiten es gibt für Remote-Zugriffe.

Bei jedem Interviewpartner existieren unterschiedliche Schnittstellen zu anderen Systemen. Bei Zentras existieren grundsätzlich nur wenige Schnittstellen zwischen den Systemen. Diese Schnittstellen werden als "nicht kritisch" betrachtet. Es werden keine "externen Daten" bezogen. Zentras stellt u.a. Bilder der VMZ zur Verfügung. Die Bilder werden als analoges Signal an das BIT-Netz übertragen. Die Verkehrszentralen des ASTRA (Zentralen in den Gebietseinheiten) verfügen je über einen ISDN-Anschluss, über welchen das ASTRA die Daten direkt bezieht (Daten für Verkehrszählungen). Zentras selbst greift über einen separaten Anschluss zu Wartungszwecken ebenfalls auf die Verkehrszentralen zu, ohne jedoch Daten zu beziehen. Zentras übermittelt definierte Ereignismeldungen an die Polizei. Ausserdem hat Zentras Zugriff auf die Besprechungsanlage verschiedener Tunnels. Auch auf die Glatteiswarnanlage kann zugegriffen werden. Bei AfBN existiert ein Kommunikationsnetz (Ethernet), über welches die Bereichsrechner miteinander verbunden sind. Das übergeordnete Leitsystem (ÜLS) setzt auf dem Kommunikationsnetz auf. Das Kommunikationssystem ist komplett isoliert. Für die Bildübertragungen existiert ein ATM-Netz. Die Schnittstellen zu den externen Systemen sind über Firewalls gesichert. Bei den externen Netzen handelt es sich ebenfalls um isolierte Netze. Es werden u.a. Bilder an verschiedene externe Systeme übermittelt. Bei der AGK des ASTRA erfolgt eine Übermittlung der Daten ins Netz der Polizei. Das AGK-System greift ausser-

dem die Schaltbefehle von dynamischen Geschwindigkeitsanzeigen ab, damit die aktuell signalisierte Geschwindigkeit erfasst werden kann. In Urdorf existieren Schnittstellen mit der KaPo Zürich und dem Citylink. Auch bei NSNW existieren gewisse Schnittstellen. So findet ein periodischer Datentransfer von Videobildern auf den Webserver in der DMZ statt via FTP-Push. Ausgewählte Benutzer (VM-CH, Viasuisse) haben Zugang zu diesem Webserver via Benutzernamen und Passwort.

Bezüglich öffentlicher Schnittstellen zu den Systemen und Daten und Remote-Zugriff haben viele Interviewpartner angegeben, dass es grundsätzlich keine öffentlichen Schnittstellen gibt. Allerdings beziehen gewisse Interviewpartner die neuesten Malwaredefinitionen aus dem Internet. So existiert zum Beispiel in Urdorf eine Verbindung zum Internet für Malwareupdates. Die Verbindung wird nach dem Update allerdings wieder getrennt. Der Zugriff erfolgt über eine dezidierte Leitung inkl. Firewall. Bei NSNW existiert eine Verbindung zum Internet für Malwareupdates der Laptops des Pikett-Diensts. Gewisse Interviewpartner verfügen auch über bestimmte Zugänge für die Wartung. So haben bei Zentras im Netz NW/OW verschiedene Anbieter für die Systemwartung einen ISDN-Zugang zu den Netzen. Auch im Netz LU gibt es ISDN-Zugänge, welche sehr schwer zu kontrollieren sind. Die ISDN-Zugänge sollen zukünftig durch VPN-Zugänge abgelöst werden. Bei der AGK des ASTRA kann für Wartungszwecke mit einem dedizierten Laptop auf die Anlage zugegriffen werden (Zugang zum System nur mit diesem Laptop möglich). Der Laptop wird bei der Polizei unter Verschluss gehalten. In Urdorf existiert ein zeitbegrenzter Zugriff für Lieferanten auf die Bereichsrechner über eine gesicherte Internetleitung. Der externe Rechner, mit welchem die Lieferanten zugreifen, wird über das System identifiziert und kann nur auf einen bestimmten Bereichsrechner zugreifen. Bei NSNW gibt es einen VPN-Zugang für Lieferanten. Der Zugang zu den Systemen muss angemeldet werden und erfolgt immer über eine Firewall und auf dedizierten Geräten. Auch für den Pikett-Dienst existiert ein VPN-Zugang. Für Anlagen abseits der Autobahn (z.B. Stromverteilung, Pumpwerke) existiert ein Zugriff via GPRS (VPN).

Zusammenfassung:

- Grundsätzlich existieren nur wenige Schnittstellen zwischen den Systemen.
- Es werden kaum "externe Daten" bezogen, sondern eher Daten nach Aussen geliefert.
- Grundsätzlich existieren keine öffentlichen Schnittstellen. Gewisse Interviewpartner beziehen allerdings aktuelle Malwaredefinitionen aus dem Internet.
- Es existieren auch gewisse Zugänge für die Wartung. Dazu werden u.a. ISDN-Zugänge (die zum Teil nur schwer zu überwachen sind) und VPN-Zugänge verwendet. VPN-Zugänge müssen zum Teil angemeldet werden und sind nur für einen gewissen Zeitraum verfügbar.

3.4 Authentifizierung und Authentisierung

In diesem Unterkapitel sollen die vorhandenen Authentifizierungs- und Authentisierungsmechanismen untersucht werden. Solide Mechanismen sind notwendig, damit es für unbefugte Personen nicht möglich ist, sich Zugang zu den Systemen zu verschaffen.

Bezüglich Authentifizierung und Authentisierung haben die Interviewpartner unterschiedliche Aussagen gemacht. Zwei Interviewpartner (Zentras und NSNW) verwenden zum Teil "Gruppenaccounts" oder "Shared Accounts". Bei Zentras erfolgt der Zugriff auf die Systeme über drei unterschiedliche Benutzergruppen (Benutzer, Administratoren, Polizei). Im Netz LU werden persönliche Benutzerkonten, sowie "Shared Accounts" geführt. Im Netz OW/NW gibt es persönliche Benutzerkonten. AfBN verwendet ein Active Directory um sämtliche Benutzerkonten und entsprechende Berechtigungen zentral zu verwalten. In Urdorf sind Access-Control-Mechanismen implementiert. Es wird sichergestellt, dass sichere Passwörter verwendet werden. Passwörter müssen periodisch geändert werden. Die Logins werden zentral von der Sektion IT verwaltet und mindestens monatlich überprüft. Bei NSNW wird der Zugang zum Betriebsleitsystem über Accounts für einzelne Benutzer geregelt. Der Zugang zur Anlagenebene erfolgt über "Gruppenaccounts". Logins werden zentral von der IT-BSA verwaltet.

Zusammenfassung:

- Zum Teil werden Gruppenaccounts oder Shared Accounts verwendet.
- Meistens werden allerdings persönliche Konten verwendet.
- Die Logins werden zentral verwaltet (z.B. über Active Directory).

3.5 Sicherheitsrichtlinien

Das Ziel von Sicherheitsrichtlinien ist die Definition und Beschreibung der Massnahmen zur Gewährleistung der Informationssicherheit innerhalb einer Organisation. Dabei kann es sich um organisatorische und auch technische Massnahmen handeln.

Sicherheitsrichtlinien für die BSA sind bei den analysierten Organisationen kaum vorhanden. Nur bei einer der befragten Organisationen sind spezifische Sicherheitsrichtlinien erarbeitet worden. Des Weiteren liegen bei den untersuchten Organisationen keine Notfallpläne vor, die das Verhalten bei Stör-, Not- und Katastrophenfällen des IT-Systems regeln würden. Dies im Gegensatz etwa zu Notfallplänen für Ereignisse in den Anlagen selbst, welche für alle relevanten Anlagen vorliegen.

Teilweise existieren Sicherheitsrichtlinien von der Betriebsorganisation übergeordneten Organisationen, wie beispielsweise dem Kanton. Diese Richtlinien fokussieren jedoch nicht auf den Bereich der BSA und werden von den Betriebsorganisationen bis jetzt auch nicht auf die BSA oder ihre Bedürfnisse übertragen. Eine dieser übergeordneten Sicherheitsrichtlinien ist die "Weisungen über die Informatiksicherheit in der Bundesverwaltung" [WIsB]. Diese regelt die Organisation, das Sicherheitsverfahren und die Netzwerksicherheit. Sie bestimmt die technischen, baulichen, organisatorischen und personellen Anforderungen. Der Schwerpunkt dieser Weisung liegt in technischen und organisatorischen Vorgaben bezüglich der Authentifizierung sowie der Netzwerksicherheit. Sie enthält aber auch eine Liste der minimalen Sicherheitsanforderungen und Verantwortlichkeiten für den generellen Schutzbedarf.

Obwohl in den befragten Organisationen kaum explizit dokumentierte Sicherheitsrichtlinien vorhanden sind, werden dennoch implizit gewisse Sicherheitsrichtlinien gelebt. Dies äussert sich u.a. in organisatorischen Massnahmen bei der Vergabe von Zugängen für Wartungsfirmen mittels Antragsformularen, der Regelungen für die Nutzung von Laptops oder bei der Prüfung von Sicherheitsaspekten bei Systemabnahmetests. Diese impliziten Sicherheitsrichtlinien wurden in der Regel durch die verantwortlichen Systembetreuer eingeführt und werden an neue Mitarbeiter bei der Einarbeitung weitergegeben.

Bei den Gebietseinheiten handelt es sich um neue Organisationen, die durch das Zusammenlegen mehrerer kantonaler Organisationen zustande gekommen sind. Die VMZ-CH ist eine Organisation, die komplett neu aufgebaut wurde. Bei gewissen Gebietseinheiten und auch bei der VMZ-CH kann deshalb deutlich festgestellt werden, dass die betriebliche Organisation noch im Aufbau begriffen ist. Dies äussert sich neben der heterogenen Systemlandschaft auch in heterogenen Vorgaben für die Lieferanten.

Die Verantwortung für die Informationssicherheit liegt in allen untersuchten Betrieben direkt beim Systemverantwortlichen der BSA, d.h. es gibt keine separate Stelle oder Person, welche sich explizit und vertieft mit Sicherheitsaspekten von BSA befasst und die Systembetreuer in diesen Fragen unterstützen könnte. Einzig bei der VMZ-CH existiert ein der Organisation zugewiesener Informatiksicherheitsbeauftragter (ISB-O), der jedoch aus organisatorischen Gründen kaum Einfluss auf die Betriebsorganisation der BSA hat.

Einzelne Betriebsorganisationen haben ein Sicherheitskonzept oder eine Sicherheitsprüfung erstellen lassen.

Zusammenfassung:

- In den meisten Organisationen fehlen dokumentierte Sicherheitsrichtlinien.
- Auch von übergeordneten Organisationen werden keine Sicherheitsrichtlinien vorgegeben, oder diese sind zumindest nicht bekannt.

- Es existieren keine Notfallpläne für die IT-Systeme.
- Es existieren heterogene Vorgaben für Lieferanten zwischen den einzelnen Organisationen, teilweise sogar innerhalb der gleichen Organisation.

3.6 Physischer Zugangsschutz

Der physische Zugangsschutz dient dazu, die Systeme und Geräte baulich vor dem Zutritt unbefugter Personen zu schützen. Dabei sind die technischen Installationen insbesondere vor Diebstahl, Feuer, Wasser, Störung der Stromversorgung oder Hitze (z.B. Ausfall der Klimaanlage) zu schützen.

Aus den geführten Interviews ist ersichtlich, dass die Situation in Bezug auf die Massnahmen zur Sicherstellung des physischen Zugangsschutzes äusserst heterogen ist.

Die Systeme für die Bedienung der Betriebsleitzentralen (BLZ) stehen in verschlossenen Räumen, eine systematische Überwachung des Zutritts mit Protokollierung ist jedoch nur einzeln vorhanden oder für die Zukunft geplant. Die Serversysteme der BLZ stehen entweder in verschlossenen eigenen Rechenzenter-Räumen oder sind ausgelagert (z.B. bei der Polizei).

Die Systeme der BS-Anlagen vor Ort (z.B. Bereichsrechner) stehen in verschlossenen Räumen und Schränken. Bei neu projektierten Systemen werden vermehrt die Zugänge überwacht und protokolliert (z.B. AGK).

Die Abgabe der Schlüssel für den Zutritt der Mitarbeiter ist geregelt und dokumentiert. Fallweise existieren Schliesskonzepte.

Der Zutritt für Lieferanten ist äusserst unterschiedlich geregelt. Teilweise werden die Lieferanten bei Einsätzen vor Ort begleitet, teilweise erhalten Lieferanten Schlüssel und haben somit einen unabhängigen Zugang zu den Systemen. Bei einigen Organisationen müssen sich Lieferanten vor dem Einsatz anmelden und die Schlüssel bei der BLZ abholen.

Der Schutz gegen die häufigsten Bedrohungen (Brandschutz, Wasserschutz, Stromausfall) erfolgt über Rauchmelder, Brandschutzklappen, Sprinkleranlagen und USV. In den Rechenzentren werden vereinzelt bereits Gaslöschanlagen eingesetzt. Weiterhin werden einzelne Systeme redundant ausgelegt.

Zusammenfassung:

- Der physische Zugangsschutz der BS-Anlagen auf der Prozessleitebene, d.h. bei den Bereichsrechnern, welche die Steuerungsaufgaben und die sicherheitsrelevanten Funktionen übernehmen, ist geregelt. Es besteht jedoch Verbesserungspotential in der Zugangsüberwachung sowie in der Vereinheitlichung der Schutzmassnahmen bei den häufigsten Bedrohungen.
- In den Betriebsleitzentralen besteht Bedarf an vertiefter Analyse bezüglich Regelung und Überwachung des Zugangs sowohl für Mitarbeiter als auch für die Lieferanten.

3.7 Prozess der Rechtevergabe an Mitarbeiter

Kennzeichnend für die Systeme der BSA ist deren sehr begrenzte Anzahl von Benutzern. Die Anzahl Mitarbeiter mit einem Zugriff auf das System der BSA ist daher für Systemadministratoren gut überschaubar. Im Fall der externen Systembenutzer ist dies jedoch oft nicht der Fall. Für Systemlieferanten werden teilweise unpersönliche Benutzerkonten eingerichtet, die von mehreren Personen des Systemlieferanten gemeinsam genutzt werden. In diesen Fällen fehlt den Systembetreibern die Übersicht der Personen, welche tatsächlich auf das System zugreifen.

Die Benutzerkonten und -rechte werden in allen befragten Organisationen über eine zentrale Stelle verwaltet. In der Regel erfolgt die Verwaltung der Benutzerrechte direkt durch

den Systemadministratoren des BSA Systems. Eine systematische, regelmässige Überprüfung der Benutzerkonten und der Löschung von nicht mehr benötigten Konten findet nicht in allen Organisationen statt, was durch die überschaubare Benutzeranzahl erklärbar ist.

Zusammenfassung:

- Eine Übersicht der externen Systembenutzer ist oft nicht systematisch vorhanden.
- Eine regelmässige Überprüfung und Aktualisierung der Benutzerkonten und -rechte ist nicht standardisiert.

3.8 Grundsätzliche Identifikation kritischer Systeme und Daten

In diesem Unterkapitel geht es darum, Systeme und Daten zu identifizieren, die von den Interviewpartnern grundsätzlich als kritisch angesehen werden. Die gewonnen Informationen dienen als Hinweis, welche Systeme in der detaillierten Analyse besonders genau betrachtet werden sollten. Die Interviewpartner wurden gebeten, Systeme und Daten zu identifizieren, die sie als besonders kritisch betrachten (inkl. Systeme, die in Zukunft hinzukommen könnten). Ausserdem wurden die Interviewpartner gebeten, sich realistische Angriffszenarien zu überlegen. Schliesslich wurde untersucht, welche Daten von Aussen bezogen werden.

Bezüglich der besonders kritischen Systeme und Daten haben die Interviewpartner unterschiedliche Aussagen gemacht. Bei Zentras werden folgende Systeme als kritisch betrachtet: Verkehrssteuerungsanlage, Brandmeldeanlage, Lüftungssteuerung, Netzwerk/Kommunikationsnetz und Notruftelefonanlage. Daten werden im Allgemeinen als nicht kritisch betrachtet. Einzig die Bilddaten weisen eine gewisse Sensibilität auf. Die Bilddaten sind allerdings maximal 24 Stunden in den Systemen verfügbar. AfBN hat keine expliziten Systeme oder Daten genannt, die besonders schützenswert wären. Allerdings werden gewisse Punkte als kritisch betrachtet. So wird das Einspielen von Softwareupdates durch Lieferanten im Rahmen der Wartung als kritisch angesehen. Auch die nicht vorhandene Segmentierung der einzelnen Netzteile wird als kritisch betrachtet (virtuelle LANs sind in Folge technischer Einschränkungen nicht getrennt). Als Folge der kaum vorhandenen Segmentierung des Systems kann sich Malware relativ einfach ausbreiten. Videodaten werden als nicht kritisch betrachtet. Es findet eine Ringspeicherung statt, mit welcher die Videosequenzen maximal 24 Stunden gespeichert werden. Bei ausgewählten Ereignissen findet eine automatische Speicherung von Bildern in einem separaten Speicher statt. Diese Daten werden nur auf Anfrage der Polizei/Justiz zur Verfügung gestellt. Beim ASTRA wird die Verfügbarkeit des Systems als nicht kritisch betrachtet (ein Ausfall des Systems hat keine kritischen Auswirkungen). Die erhobenen Daten sind allerdings sensibel, da es sich um persönliche Daten handelt (Fahrzeug, Fahrer, Insassen). Insbesondere auch die Kombination des Fahrzeugs mit dem Ort, an welchem es registriert wurde, ist schützenswert. Die Integrität der Daten ist sehr wichtig, da diese als Grundlage und Beweismittel für gerichtliche Verfahren dienen. Für das ganze Verfahren/System muss gewährleistet sein, dass keine Manipulationen statt finden können, da ansonsten die registrierten Verstösse vor Gericht angefochten werden können. In Urdorf wird das ganze Kommunikationsnetz als kritisches System genannt (Bei einem Ausfall gibt es keine übergeordnete Steuerung mehr). Kritische Daten sind keine vorhanden. Die Daten werden sowieso alle 10 Sekunden überschrieben. Die Integrität der Daten ist allerdings relativ wichtig. Videos werden nicht aufgezeichnet und haben aus Datenschutzgründen eine schlechte Auflösung. Bei NSNW wird als kritisches System das ganze Backbone des Kommunikationsnetzes inklusive Komponenten (Router, Switches) angesehen. Videodaten von Ereignissen werden aufgezeichnet und auch langfristig vor Ort gespeichert. Bei Bedarf werden diese der Polizei zugänglich gemacht. Die Datenübergabe erfolgt dabei rein manuell (z.B. via CD). Die Auflösung ist jedoch qualitativ nicht sehr hoch. Es ist keine Erkennung von Personen oder Nummernschildern möglich. Videodaten werden in Form von aufgezeichneten Ereignissen, Login-Daten in Form von verschlüsselten Dateien gehalten. Bei Abnahme erfolgt ein Backup der System-Software inkl. Archivierung in einem externen Datentresor.

Auch bezüglich möglicher Szenarien, die den Betrieb beeinträchtigen würden, haben sich

die Interviewpartner unterschiedlich geäussert. Zentras nannte als mögliches Szenario zum Beispiel das Auslösen von Ereignissen, welche ein Tunnelrot bewirken, was eine Tunnelschliessung und somit einen Verkehrsunterbruch zur Folge hätte. Datendiebstahl (z.B. von Bildmaterial) wird auch als realistisches Szenario angesehen. Bei Zentras gilt grundsätzlich, dass das Ausmass eines Systemausfalls sinkt, je näher man an die Feldebene gelangt. Bei AfBN wird ein Malware-Ausbruch als realistisches Szenario angegeben. Aufgrund der limitierten Segmentierung der Netze ist die Ausbreitung einer Malware grundsätzlich nur schwer zu verhindern. Beim AGK des ASTRA wird Vandalismus als mögliches Szenario angegeben. Auch die Witterung könnte einen negativen Einfluss auf die Anlage haben. In Urdorf kann man sich als realistischen Angriff am ehesten einen "physischen" Angriff vorstellen (zum Beispiel das Legen eines Brandes in einem Tunnel). Falls das ganze Kommunikationsnetz zusammenbrechen würde, wäre das nicht allzu schlimm (Steuerung vor Ort wäre so zum Beispiel immer noch möglich). Bei NSNW werden der Ausfall des Backbones oder einer Kommunikationskomponente (z.B. Switch), der Ausfall des Betriebsleitsystems und der Ausfall eines Objektrechners in einem Tunnel als mögliche Szenarien angegeben. Durch die Gliederung der Anlagenstruktur kann sich ein Ausfall allerdings nicht auf andere Anlagen ausbreiten.

Gewisse Interviewpartner beziehen von Aussen die neusten Malwaredefinitionen. Ansonsten werden kaum Daten von Aussen bezogen. Zentras leitet ausserdem auch keine Daten nach aussen weiter. Bei AfBN bestehen vereinzelte Schnittstellen, über welche Daten in externe Netze übermittelt werden. Beim AGK des ASTRA werden bei Verstössen Daten ins Polizeinetz übermittelt. In Urdorf existiert eine Verbindung mit der KAPO Zürich und mit dem Citylink. Auch bei NSNW werden gewisse Daten nach aussen weitergegeben, zum Beispiel für die Steuerung von Wechseltextanzeigen oder Gefahrenanzeigen in den Kantonen AG, SO und BE (über separates VLAN).

Bei den meisten Interviewpartnern sind gewisse Komponenten in Planung/Realisierung. Im Netz LU der Zentras sind ein Breitbandkommunikationssystem und ein übergeordnetes Leitsystem (ÜLS) geplant. Beim AfBN sind konkret keine wesentlichen Änderungen geplant. Allenfalls wird eine engere Anbindung an das kantonale Netzwerk für gewisse Datenübertragungen zu prüfen sein. Eine einfacher zu handhabende technische Lösung für den Fernzugriff wird als mittel-/längerfristiges Ziel formuliert. Beim AGK des ASTRA sind die Anlagen aktuell nur für die Messung der Geschwindigkeit vorgesehen. Weitergehende Nutzungen sind derzeit bewusst nicht vorgesehen. Allerdings wären die Anlagen auch in der Lage, andere Funktionen zu übernehmen wie zum Beispiel Fahndungskontrollen (Erkennung von gefahndeten Fahrzeugen oder Verfolgung von gefährlichen Gütern). In Urdorf ist eine DMZ geplant. Über die DMZ soll u.a. ein gegenseitiger Datenaustausch mit der Stadt Zürich möglich sein. Ausserdem könnten sich über die DMZ Pikett-Leute von zu Hause aus einloggen und müssten nicht mehr vor Ort gehen. Geplant ist auch die Anbindung von LSA/VDE über die "Luftschnittstelle". Bei NSNW läuft zurzeit die Planung eines neuen Netzwerks. Dieses wird auch zukünftig ein separates Netz bleiben. Es wird vermutlich Schnittstellen zur VMZ-CH geben.

Zusammenfassung:

- Gewisse Interviewpartner verfügen über sensible Daten. Integrität spielt zum Teil auch eine Rolle. Im Allgemeinen werden die Daten allerdings nicht als kritisch betrachtet.
- Fast alle Interviewpartner verfügen über gewisse Systeme, die sie als kritisch betrachten.
- Oft werden physische Angriffe als mögliche Angriffsszenarien genannt.
- Es werden kaum Daten von Aussen bezogen. Gewisse Interviewpartner beziehen allerdings die neuesten Malwaredefinitionen von Aussen.
- Bei den meisten Interviewpartnern sind gewisse Komponenten in Planung/Realisierung. Allerdings hat keiner der Interviewpartner speziell vermerkt, dass diese Komponenten als kritisch betrachtet werden.

3.9 Backup und Logging

Regelmässige Backups sind nötig, so dass im Falle eines Ausfalls des Systems kein entscheidender Datenverlust entsteht. Mit Hilfe von Logging-/Auditing-Mechanismen können eventuelle Vorfälle besser nachvollzogen werden.

Backups werden von den Interviewpartnern grundsätzlich durchgeführt. Ausnahmen gibt es beim AGK des ASTRA und in Urdorf. Beim AGK des ASTRA werden die Daten nicht gesichert. Übertretungen werden jedoch bei der Polizei archiviert. Das Backup der Anlagen-Konfiguration ist über ein Service-Level-Agreement (SLA) zwischen der Polizei und dem Lieferanten sichergestellt. In Urdorf werden überhaupt keine Backups gemacht. Es existiert zwar ein Fileserver für Betriebsdaten in der Betriebsleitzentrale, die Daten werden zurzeit aber nicht statistisch ausgewertet. Die Server sind mit einem RAID ausgestattet. Bei Zentras im Netz Luzern werden einmal jährlich Images der Rechner erstellt. Eine häufigere Sicherung der Systeme ist nicht notwendig. Die Systemlieferanten verfügen in der Regel selbst auch noch Images der Rechner. Es gibt grundsätzlich nur wenige Daten, die gespeichert werden. In diesem Fall erfolgt die Datenhaltung in Datenbanken, welche über eigenständige Backupmechanismen verfügen. In NW/OW ist ein jährliches Image der Rechner geplant. Bei AfBN sind während der Garantiezeit die Lieferanten für die Wiederherstellung des Betriebs verantwortlich. Ausserhalb der Garantiezeit werden im Rahmen der Wartungsarbeiten periodisch Backups erstellt. Betriebsrelevante Daten werden laufend gesichert. Bei älteren Komponenten besteht die Schwierigkeit darin, dass eine grosse Abhängigkeit zur Hardware besteht. Bei einem Ausfall der Hardware ist es schwierig, diese HW-Komponente zu ersetzen. Bei NSNW werden Betriebsdaten zentral erfasst und archiviert. Die Daten werden in einem Datentresor archiviert. Die Backup-Prozeduren werden überwacht. Recoveries wurden bisher nicht regelmässig getestet, bisher durchgeführte Recoveries waren jedoch erfolgreich. Die Verantwortung liegt bei der IT-BSA. Es existieren Checklisten für den Backup-Betrieb.

Grundsätzlich sind Auditing-Mechanismen bei den Interviewpartnern vorhanden. Allerdings werden bei Zentras die ISDN-Zugänge im Netz LU nicht geloggt. Im Netz NW/OW werden die ISDN-Zugänge auf der Firewall zwar geloggt, allerdings fand noch nie eine Auswertung der Log-Files statt. Bei AfBN werden Logging-Mechanismen verwendet, welche durchgeführte Operationen registrieren, so dass die Ereignisse im Problemfall rekonstruiert werden können. Beim AGK des ASTRA wird jedes Login protokolliert. Auch jede Manipulation wird protokolliert (inkl. Öffnen des Rechnerschrankes). Auch in Urdorf wird ein Logging durchgeführt. Es existieren persönliche Logins, so dass im Nachhinein nachvollzogen werden kann, war wann was gemacht hat. Bei NSNW werden für die grösseren Systeme (BLS) Log-Files geführt. Persönliche Logins sind vorhanden.

Zusammenfassung:

- Praktisch alle Interviewpartner führen Backups durch.
- Auch Auditing-Mechanismen sind grundsätzlich vorhanden.

3.10 Regelmässige Prüfung kritischer Systeme

Regelmässige Prüfungen kritischer Systeme dienen dazu, einen möglichst reibungslosen Betrieb sicherzustellen und eventuell ausfallgefährdete Systeme frühzeitig zu ersetzen, bzw. Schäden frühzeitig zu beheben.

Die regelmässige Prüfung der kritischen Systeme wird nicht von allen Interviewpartnern gleich gehandhabt. Bei Zentras werden die Systeme bei der Einführung und bei grösseren Anpassungen systematisch geprüft. Bei AfBN ist eine klare Organisation vorhanden. Bei der AGK des ASTRA prüft sich die Anlage automatisch selbst in regelmässigen Abständen. In Urdorf gibt es keine konkreten, regelmässigen Tests. Abnahmetests werden allerdings durchgeführt. Manchmal werden auch bei Tunnelreinigungen Tests durchgeführt. Bei NSNW finden regelmässige funktionale Prüfungen der Anlagen statt. Die Resultate der Prüfungen werden dokumentiert. Die Anlagen überwachen sich automatisch. Das Betriebsleitsystem überwacht, ob die Anlagen verfügbar sind. Im Falle einer Störung erfolgt automatisch eine Alarmierung. Prozesse und Arbeitsanweisungen für den Pikett-

Dienst sind definiert. Ausserdem werden kritische Komponenten als Ersatzteile vorgehalten.

Zusammenfassung:

- Kritische Systeme werden grundsätzlich von allen Interviewpartnern geprüft. Allerdings werden Tests unterschiedlich gehandhabt: Zum Teil werden Tests nur bei Einführung neuer Systeme und bei grösseren Änderungen der Systeme durchgeführt, bei anderen Interviewpartnern finden regelmässige Prüfungen statt. Gewisse Anlagen überwachen sich auch automatisch.

3.11 IT-Grundschutz und Update-Management

In diesem Unterkapitel soll der IT-Grundschutz und das Update-Management untersucht werden. Zum IT-Grundschutz zählen Massnahmen wie zum Beispiel Antimalware-Software oder Personal Firewalls. Ein konsequentes Update-Management stellt sicher, dass die Systeme auf dem aktuellsten Stand gehalten werden und so vor neuen Bedrohungen besser geschützt sind.

Bezüglich IT-Grundschutz verwenden die meisten Interviewpartner Antimalware-Software. Bei Zentras verfügen ältere Betriebsnetze in Luzern allerdings über keinen Malwareschutz. Bei der AGK des ASTRA sind überhaupt keine Sicherheitsmassnahmen vorgesehen. Beim NSNW gibt es im BSA-Netzwerk keinen Malwareschutz, da das System geschlossen ist.

Der Softwareupdateprozess wird unterschiedlich gehandhabt von den verschiedenen Interviewpartnern. Bei Zentras werden kleinere Anpassungen oft direkt vor Ort vorgenommen. So wird der Malwareschutz im Netz NW/OW alle zwei Wochen mittels USB-Stecker aktualisiert. In diesem Fall erfolgen keine vorgängigen Prüfungen. Bei AfBN existiert ein zentraler Update-Server, welcher Betriebssystem-Updates sowie Malwareschutz-Aktualisierungen aus dem Internet bezieht. Die Aktualisierung der Betriebsrechner erfolgt sodann kontrolliert über diesen Update-Server. Bei der AGK des ASTRA sind Testsysteme, wo neue Updates vorgängig überprüft werden können, geplant. Bei Systemerneuerung wird der "normale" Abnahmeprozess durchlaufen. Ein Change-Management gibt es nicht. In Urdorf werden keine Betriebssystemupdates durchgeführt (Der Stand des ÜLS ist "eingefroren"). Wenn neue Rechner ins ÜLS eingebunden werden müssen, werden diese zuerst in einem Testverbund geprüft. Bei NSNW ist der Softwareupdateprozess nicht klar geregelt. Die Lieferanten haben einen ziemlich grossen Spielraum. Auf der Anlagenebene (Prozessleitsystem) wird der Software-Release bei der Abnahme "eingefroren", wobei Fehlerkorrekturen in der ersten Betriebsphase möglich sind. Grössere Änderungen laufen über Projekte und sind dann eher als Ersatz der bestehenden Systeme zu verstehen. Auf Stufe des Betriebsleitsystems werden neue Releases beim Lieferanten getestet und dann auf dem BLS eingespielt. Das Change-Management wird pragmatisch gelebt: Nicht jede Änderung wird systematisch über das Change-Management verfolgt.

Zusammenfassung:

- Die meisten Interviewpartner verwenden Antimalware-Software.
- Bezüglich Update-Management werden unterschiedliche Techniken angewendet. Bei gewissen Interviewpartnern werden kleinere Anpassungen direkt vor Ort gemacht. Andere Interviewpartner verwenden zentrale Updateserver. Gewisse Interviewpartner führen gar keine Softwareupdates durch, d.h. der Stand der Software wurde auf einer bestimmten Version eingefroren. Zum Teil sind auch Testsysteme vorhanden, um neue Versionen vorgängig zu prüfen.

3.12 Private Nutzung der Laptops und Mitführen sensitiver Daten

Die private Nutzung der Laptops ist ein sehr kritischer Punkt. Bei unachtsamer Verwendung könnte beispielsweise Malware auf den Laptop gelangen, die sich dann in den Netzen der Interviewpartner ausbreiten, sobald der Laptop angeschlossen wird. Das wird besonders dann zum Problem, wenn der Softwarestand eingefroren wurde. Beim Mitfüh-

ren sensitiver Daten müssen spezielle Schutzmassnahmen beachtet werden, sodass die Daten nicht durch Dritte auf einfache Art und Weise manipuliert werden können. Die Vertraulichkeit muss ebenfalls sichergestellt werden.

Praktisch alle Interviewpartner haben angegeben, dass eventuell vorhandene Laptops nicht für die private Nutzung verwendet werden dürfen. Bei Zentras stehen im Netz LU drei Laptops für den externen Zugriff über LUNET zur Verfügung. Dabei handelt es sich um extra konfigurierte Rechner, die nicht anderweitig verwendet werden dürfen. Bei AfBN dürfen Laptops ebenfalls nicht für private Zwecke verwendet werden, was aufgrund der Vorkonfiguration der Laptops auch gar nicht möglich ist. Auch beim ASTRA ist die private Nutzung von Laptops untersagt. In Urdorf sind auf den Laptops nur die benötigten Anwendungen installiert. Zusätzliche Software kann nicht installiert werden. Die private Nutzung der Laptops ist ebenfalls untersagt. Bei NSNW wird die private Nutzung der Laptops über das IT-Reglement (BL) geregelt. Insbesondere ist kein E-Mail-Verkehr im BSA-Netzwerk erlaubt. Mitarbeiter des Pikett-Diensts haben Zugriff auf die Laptops als "normaler" Benutzer. Es kann keine Software installiert werden.

Bei keinem der Interviewpartner gibt es Mitarbeiter, welche sensitive Daten auf sich tragen.

Zusammenfassung:

- Praktisch alle Interviewpartner haben angegeben, dass Laptops nicht für die private Nutzung verwendet werden dürfen. Die Laptops sind ausserdem meist auch so konfiguriert, dass keine zusätzliche Software installiert werden kann.
- Es gibt keine Mitarbeiter, welche sensitive Daten auf sich tragen.

3.13 Software- und System-Entwicklung

In diesem Unterkapitel soll untersucht werden, wie Sicherheit bei der Entwicklung von Software und Systemen von den Interviewpartnern berücksichtigt wird. Ausserdem soll untersucht werden, ob entwickelte Software und Systeme bei der Abnahme systematisch auf Sicherheit geprüft werden.

Kein Interviewpartner hat angegeben, dass Software entwickelt wird. Zentras hat vermerkt, dass bei der Ausschreibung neuer Systeme auf die Kompetenz des Pflichtenheft-Verfassers sowie der Systemhersteller selbst vertraut wird. In Urdorf gibt es bei der Einführung neuer Systeme einen Integrationsprozess. Aufträge für neue Systeme werden öffentlich ausgeschrieben.

Systematische Prüfungen der entwickelten Systeme und Software auf Sicherheit bei der Abnahme werden unterschiedlich gehandhabt. Bei Zentras werden alle Anforderungen gemäss Pflichtenheft bei der Abnahme eines neuen Systems geprüft. Kritisch sind kleinere Anpassungen (Wartungsarbeiten), die im laufenden Betrieb direkt vor Ort gemacht werden. Bei AfBN sind vollständige Tests durch die Lieferanten durchzuführen (vertraglich geregelt). Durch die Gebietseinheit werden lediglich Stichproben getestet. Tests für neue Komponenten können nur teilweise auf produktivem System gemacht werden. Es existiert nicht für jede Anlage ein Testsystem. Die Risiken, welche sich aus den weitgehend fehlenden Testmöglichkeiten ergeben, werden dadurch eingeschränkt, dass versucht wird, in kleinen Entwicklungsschritten vorzugehen. Einmal jährlich findet ein Integraltest des Systems statt. Beim AGK des ASTRA gibt es Funktionstests bei der Systemabnahme. In Urdorf werden Systeme abgenommen. Die Schnittstellen werden mit einem spezifischen Werkzeug geprüft. Es existiert ein MMI-Gremium mit Beteiligten aus KAPO, Betrieb und ÜLS. Bei NSNW gibt es keine spezifische Prüfung auf Sicherheit. Die Schwerpunkte liegen bei der Verfügbarkeit und der Zuverlässigkeit der Systeme, d.h. die Funktionalität steht im Vordergrund.

Zusammenfassung:

- Software wird bei keinem Interviewpartner entwickelt.

- Alle Interviewpartner führen gewisse Tests bei der Systemabnahme durch. Dabei handelt es sich jedoch eher um funktionale Tests. Sicherheitstests werden kaum durchgeführt (Funktionalität steht im Vordergrund).

4 Schutzbedürftige Anwendungen und Systeme

4.1 Abgrenzung der Anwendungen

Eine erste Abgrenzung der zu untersuchenden Anwendungen wird bereits in den Zielen des Forschungsprojekts festgelegt:

"Untersuchen der Verkehrstelematik-Anwendungen, elektromechanische Anlagen für Strassen und Tunnels, Verkehrs- und Betriebsleitsysteme sowie zugehörige Netzwerk- und Kommunikations-komponenten auf Sicherheitslücken."

Diese Abgrenzung wurde, im Rahmen der Schutzbedürftigkeitsanalyse, nochmals überprüft. Bei der aktuell betrachteten System- und Anwendungslandschaft sowie aus den Informationen der laufenden Projekte auf Bundesebene zur Vereinheitlichung des Systemarchitektur und der Anwendungen, stehen die Aufgaben des Verkehrsmanagements sowie diejenigen zur Ereignisbewältigung im Vordergrund. Die IT-Security wird daher im Zusammenhang mit den Anwendungen des Verkehrsmanagements (lenken, leiten, steuern) sowie der Ereignisbewältigung (Unfall, Brand, Naturereignisse, …) betrachtet. Diese Anwendungen sind auch diejenigen die für eine optimierte Nutzung der vorhandenen Verkehrskapazitäten und gleichzeitige Sicherstellung einer effizienten Verkehrsabwicklung sorgen.

Übertragen auf die Systemebenen stehen die Applikationen und Systeme der Betriebs- und Sicherheitsausrüstungen im Zentrum der Betrachtung. Dabei wird die IT-Security von der Betriebsleitebene bis auf die Gruppenleitebene untersucht. Die Einzelleit- bzw. Feldebene werden aufgrund der hohen Heterogenität und der damit verbundenen starken Lieferantenabhängigkeit dabei ausgeschlossen.

4.2 Schutzziele der Anwendungen

Die klassischen Schutzziele der IT-Sicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Sowohl anhand der Ergebnisse der Interviews (siehe Kapitel 3) als auch anhand der Literaturstudie (siehe Kapitel 2) lässt sich schliessen, dass in der VT der Verfügbarkeit der Systeme die höchste Priorität dieser Schutzziele zugeordnet werden muss. Die Aufgaben des Verkehrsmanagements - ob Überwachung oder Steuerung - können nur dann zuverlässig und kontinuierlich durchgeführt werden, wenn die Verfügbarkeit der Systeme sehr hoch ist.

Als nächstes ist die Integrität zu erwähnen. Die Integrität ist in der VT insofern relevant, als die Integrität der Systeme selbst und der zwischen Systemen und Anwendungen ausgetauschten Daten eine Grundvoraussetzung ist, dass die Systeme und Anwendungen korrekt funktionieren und damit die Basis für hohe Verfügbarkeit erst ermöglichen.

Die Vertraulichkeit geniesst im Vergleich zur Verfügbarkeit und Integrität eine untergeordnete Rolle, insbesondere deshalb, weil es in den VT nur wenige Daten gibt, die bezüglich ihrer Geheimhaltung sehr kritisch sind. Zu dieser Kategorie gehören eigentlich nur Videodaten; aber auch diese werden nicht als hochkritisch eingestuft und zudem ist deren Qualität meist bewusst reduziert, um deren Wert für Dritte zu reduzieren. Dennoch ist zu beachten, dass die Vertraulichkeit dennoch beachtet werden muss. Wenn sich z.B. Benutzer bei einem System authentisieren, so müssen die verwendeten Credentials (z.B. Benutzername und Passwort) verschlüsselt - also vertraulich - übertragen werden, damit diese von Dritten nicht mitgelesen und verwendet werden können.

Zusammenfassend lässt sich also sagen, dass Verfügbarkeit das primäre Schutzziel ist und dass die Integrität von Systemen und Daten und die Vertraulichkeit gewisser Daten bedeutend sind, um das primäre Ziel zu erreichen. Entsprechend richten sich realistische Bedrohungen auch direkt gegen die Verfügbarkeit der VT-Systeme. Die Motivation eines Angreifers kann dabei vielfältig sein und reicht von einfacher "Sabotage" (man will einfach zeigen, dass man "es kann") bis zu kriminellen Absichten zur finanziellen Bereicherung

(z.B. durch Erpressung der Betreiber und Lahmlegung der VT-Systeme bei Nichterfüllung der Forderungen).

Eine erste Beurteilung der besonders kritischen - und damit besonders schützenswerten - Komponenten bzw. Anwendung der VT-Systeme ist bereits zum jetzigen Zeitpunkt möglich:

- An erster Stelle sind die Remote-Zugänge zu nennen, weil sie grundsätzlich (wenn sie nicht genügend abgesichert sind) weltweit (also von überall her) zugänglich sind. Dies erhöht das Risiko im Vergleich zu einer nur lokal durchführbaren Attacke (z.B. dem Aufbrechen eines Schlosses im Tunnel, um physisch Zugang zu einer IT-Anlage zu erhalten), massiv.
- Ein weiteres Risiko, das ebenfalls mit den Remote-Zugängen zusammenhängt, sind die Rechner (oft Laptops), die für den Zugang verwendet werden. Ist ein solcher Rechner einmal angeschlossen und hat er (oder der Benutzer) sich erfolgreich authentisiert, kann sich - unter der Annahme der Rechner ist mit Malware infiziert - von diesem Rechner Malware in die VT-internen Systeme und Netze ausbreiten.
- Schliesslich stellt auch das weitgehende Fehlen verbindlicher, schriftlich formulierter Sicherheitsrichtlinien ein nicht zu unterschätzendes Problem dar. Dies erhöht das Risiko, dass Mitarbeiter (unabsichtlich) Fehler unterlaufen oder dass Sicherheitsmechanismen unterwandert werden (z.B. durch die Wahl eines schwachen Passworts auf einem relevanten System).

Dies sind nur einige Beispiele, die direkt und ohne umfassende Analyse aus den bisherigen Erkenntnissen hervorgehen. Eine detailliertere Aufzählung der besonders risikoreichen Anwendungen und Komponenten oder gar eine starke Einschränkung auf einzelne Systeme möchten wir an dieser Stelle jedoch noch nicht machen. Dies wird in der nächsten Projektphase, der Bedrohungsanalye (siehe Kapitel 5), geschehen, wo sowohl Angriffsszenarien, potentielle Angriffspunkte und existierende Schutzmassnahmen detailliert analysiert und miteinander in Relation gebracht werden.

Darüber hinaus ist insbesondere auch zu beachten, dass sich die einzelnen Komponenten kaum isoliert für sich alleine betrachten lassen, da z.B. das Kompromittieren eines Rechner via einen Remote-Zugang wahrscheinlich nur die erste Stufe eines realistischen Angriffs darstellt, um dann weiter ins System vordringen und eine entsprechend mächtige Attacke zu initiieren. Aus diesem Grund wird bei der detaillierten Analyse im weiteren Verlauf des Projekts insbesondere auch darauf geachtet, dass sich die Kompromittierung eines Teilsystems nur möglichst limitiert auf Umsysteme weiterverbreiten kann, um so den Schaden möglichst zu begrenzen.

5 Bedrohunsanalyse

Bei der Bedrohungsanalyse geht es darum, aufgrund der Informationen aus den Kapiteln 2, 3 und 4 realistische Bedrohungsszenarien für die VT-Systeme zu definieren. Dabei wird das gesamte Spektrum an möglichen Angreifern berücksichtigt. Insbesondere werden neben dem aussenstehenden Hacker auch interne Mitarbeiter wie Betreiber und Systemadministratoren betrachtet.

Um ein möglichst umfangreiches Bild über mögliche Bedrohungsszenarien zu erhalten, haben wir einen so genannten "Attack-Tree" erstellt (Kapitel 5.1). Aus dem Attack-Tree haben wir dann verschiedene Angriffsvektoren herauskristallisiert und in zusammengehörige "Angriffsgruppen" gruppiert (Kapitel 5.2, 5.3).

5.1 Attack-Tree

Die Idee des Attack-Trees wurde 1999 von Bruce Schneier, einem weltweit anerkannten Kryptologen, in einem Journal veröffentlicht [Schneier, 1999].

Attack-Trees bieten einen formalen, methodischen Ansatz, um die Sicherheit eines Systems zu beschreiben, basierend auf verschiedenen Attacken. Attacken gegen ein System werden in einer Baumstruktur dargestellt, wobei der so genannte "Root-Knoten" (der oberste Knoten des Baumes) das Hauptangriffsziel darstellt. "Innere Knoten" des Baumes stellen Unterziele dar, wobei deren "Kind-Knoten" Wege aufzeigen, um diese Unterziele zu erreichen.

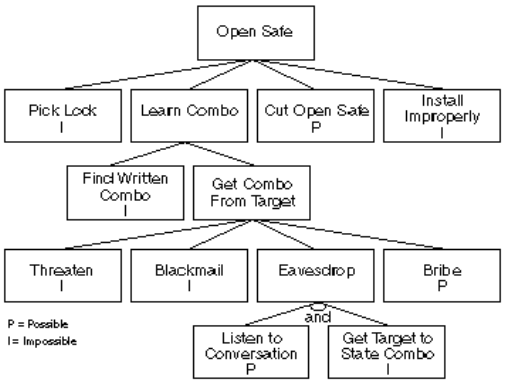


Abbildung 5: Angriffsknoten

Abbildung 5: Angriffsknoten [Schneier, 1999] verdeutlicht die Idee von Attack-Trees. Es wird ein Attack-Tree dargestellt, der verschiedene Möglichkeiten aufzeigt, um einen physischen Safe zu öffnen. Als Hauptangriffsziel wird denn auch "open safe" (Safe öffnen) aufgeführt. Um den Safe zu öffnen, gibt es für den Angreifer nun verschiedene Möglichkeiten: Schloss knacken (pick lock), Kombination herausfinden (learn combo), Safe aufbrechen (cut open safe) oder der Safe wurde unsachgemäss installiert, sodass der Angreifer den Safe einfach knacken kann (install improperly). Um die Kombination herauszufinden, muss der Angreifer entweder eine niedergeschriebene Kombination finden (find written combo) oder er muss die Kombination von einem Opfer erhalten (get combo from target). In diesem Sinne steigt man nun immer tiefer den Baum hinunter, bis man die gewünschte Granularität erreicht hat.

Beachten Sie auch, dass es so genannte "OR-Knoten" und "AND-Knoten" gibt (in Abbildung 5: Angriffsknoten sind alle Knoten, die nicht mit "and" gekennzeichnet sind, OR-Knoten). OR-Knoten zeigen verschiedenen Alternativen auf, um ein bestimmtes Ziel zu erreichen: Um den Safe zu öffnen, hat der Angreifer beispielsweise vier verschiedene Möglichkeiten. Es reicht allerdings, eine der vier möglichen Attacken durchzuführen. AND-Knoten zeigen verschiedene Schritte auf, die nötig sind, um ein gewisses Ziel zu er-

reichen. Um zum Beispiel ein "Eavesdropping" (lauschen, horchen) durchzuführen, muss sich der Angreifer eine Konversation anhören und ausserdem das Opfer dazu bringen, die Kombination zu erwähnen.

Des Weiteren können den Knoten des Attack-Trees "Attribute" zugeordnet werden. In Abbildung 5 wurden so genannte "binäre Attribute" verwendet (I für impossible - d.h. die entsprechende Attacke ist unmöglich, P für possible - d.h. die entsprechende Attacke ist ausführbar). Wir wollen an dieser Stelle nicht genauer auf Attribute eingehen und verweisen hier auf die Literatur.

Attack-Trees können auch in schriftlicher Form niedergeschrieben werden. Abbildung 6 zeigt eine schriftliche Version des Attack-Trees aus Abbildung 5.

```
Attack: Open Safe
OR
1. Pick Lock
2. Learn Combo
   OR
   2.1 Find Written Combo
   2.2 Get Combo From Target
       OR
       2.2.1 Threaten
       2.2.2 Blackmail
       2.2.3 Eavesdrop
             AND
             2.2.3.1 Listen to Conversation
             2.2.3.2 Get Target to State Combo
       2.2.4 Bribe
3. Cut Open Safe
4. Install Improperly
```

Abbildung 6: Angriffsknoten - Schriftliche Form

Abbildung 7 bis Abbildung 11 zeigen den Attack-Tree, welchen wir erstellt haben, um verschiedene Bedrohungsszenarien auf die VT-Systeme zu eruieren. Als oberstes Hauptangriffsziel haben wir "Betrieb stören" aufgeführt. Dann haben wir uns überlegt, dass es grundsätzlich vier verschiedene "Ebenen" in einem VT-System gibt, wo der Betrieb gestört werden kann: Webserver, Bedienebene, Feldebene, Rest des Netzes (Prozessleitebene, Gruppenleitebene, Einzelleitebene) (siehe Kapitel 2.2). Innerhalb der verschiedenen "Ebenen" gibt es nun generelle "Angriffsziele", die grundsätzlich in mehreren "Ebenen", in jeweils unterschiedlichen Formen, auftreten können. Folgende Angriffsziele werden beispielsweise erwähnt:

- Einschränkung der Verfügbarkeit durch nicht bösartige berechtigte Benutzer
- Einschränkung der Verfügbarkeit mittels Cyberattacke, ohne Systemkompromittierung
- Einschränkung der Verfügbarkeit mittels Cyberattacke, mit Systemkompromittierung
- Einschränkung der Verfügbarkeit durch physische Attacke

Um die oben aufgelisteten Angriffsziele nun zu erreichen, müssen gewisse Teilangriffsziele erreicht werden. Insbesondere werden folgende Teilangriffsziele erwähnt:

- Angreifbare Systeme identifizieren
- Zugang zu den Systemen erhalten
- Attacke durchführen

Innerhalb dieser Teilangriffsziele wird nun vermehrt auch auf die verschiedenen Angriffstypen eingegangen. So kann man zum Beispiel als Insider angreifbare Systeme identifizieren oder aber auch als externer Angreifer mit Hilfe von Social-Engineering-Techniken oder verschiedenen Analysemethoden.

```
Attack: Betrieb stören
OR
1. Webserver kompromittieren
   OR
   1.1 Einschränkung der Verfügbarkeit mittels Cyberattacke, ohne
       Systemkompromittierung
       (Ziel: Betrieb stören, ohne aber Systeme zu übernehmen und damit
       tiefergreifende oder längerfristige Attacken durchzuführen)
       1.1.1 Angreifbare Systeme identifizieren
             OR
             1.1.1.1 Insiderkenntnisse (Mitarbeiter; auch Ehemalige)
             1.1.1.2 Social Engineering (Fragen nach Informationen)
             1.1.1.3 Mittels Analysemethoden
                     AND
                     1.1.1.3.1 Information Gathering (IP-Adressen, E-Mail-Adressen,
                               VPN-Konfigurationsdaten, Telefonnummern,
                               Firewallkonfigurationen, Domainnamen, Google-Hacking,
                               Webcrawling, etc.)
                     1.1.1.3.2 Offene Ports und Schwachstellen detektieren
                               AND
                               1.1.1.3.2.1 Portscan
                               1.1.1.3.2.2 Vulnerability Scan (Nikto, Nessus, WebApp
                                           Security Scanners)
                               1.1.1.3.2.3 Manual Web Application Assessment (Browser
                                           Plug-ins, Web Proxies, Directory Listing -
                                           OWASP A7, Sourcecode Disclosure, Sample Files,
                                           Canonicalization Attacks, etc.)
                               1.1.1.3.2.4 Enumeration
       1.1.2 Attacke ausführen
             OR
             1.1.2.1 DoS/DDoS Attacke
                     OR
                     1.1.2.1.1 ICMP floods (Ping of Death)
                     1.1.2.1.2 Fragmentation overlap
                     1.1.2.1.3 Loopback floods
                     1.1.2.1.4 Nukers
                     1.1.2.1.5 IP Fragmentation
                     1.1.2.1.6 SYN flood
                     1.1.2.1.7 UDP floods
                     1.1.2.1.8 Reflective amplification (Mit Bot-Netzen)
                     1.1.2.1.9 Application layer
             1.1.2.2 Malware verbreiten (Die Malware soll dazu dienen, Systeme lahm zu legen
                     (z.B. durch aggressives Scanning oder durch logisches Zerstören der
                     Systeme))
                     OR
                     1.1.2.2.1 Durch absichtliche Installation eines Mitarbeiters
                     1.1.2.2.2 Durch Ausnützen einer Schwachstelle im System
                               (z.B. Remote File Inclusion)
   1.2 Einschränkung der Verfügbarkeit mittels Cyberattacke, mit Systemkompromittierung
       (Ziel: Betrieb stören und Systeme zu übernehmen um damit tiefergehende oder
       längerfristige Attacken durchzuführen)
       AND
       1.2.1 Angreifbare Systeme identifizieren (siehe 1.1.1)
       1.2.2 Zugang zu den Systemen erhalten
             OR
             1.2.2.1 Als berechtigter Benutzer (Mitarbeiter, ausgewählte "externe" Benutzer
                     (Viasuisse, VMZ))
             1.2.2.2 Als ehemals berechtigter Benutzer
                     OR
                     1.2.2.2.1 Installation einer Backdoor während der Benutzer noch berechtigt
                               Zugang hatte
                     1.2.2.2.2 Durch Nutzung von Zugangsberechtigungen, die dem Benutzer nicht
                               entzogen wurden
             1.2.2.3 Als externer Angreifer
                     OR
                     1.2.2.3.1 Mittels Impersonation
                     1.2.2.3.2 Durch Cyberattacke
                               OR
                               1.2.2.3.2.1 Session Hijacking (eine gültige Session übernehmen,
                                           z.B. mit Hilfe von XSS - Cookie Stealing; Sniffing
```

Abbildung 7: Betrieb stören - Teil 1

```
                                    und Replaying von Daten; über schwache Session IDs;
                                    schlecht gewählte Timeouts; etc.)
                            1.2.2.3.2.2 Known Exploits
                            1.2.2.3.2.3 SQLi (Benutzernamen und PWs auflisten; PWs müssen
                                    evtl. noch gecrackt werden)
                            1.2.2.3.2.4 Unvalidated Redirects and Forwards (OWASP A8 -
                                    http://www.owasp.org/images/0/0f/OWASP_T10_-_2010_
                                    rc1.pdf - z.B. Forward auf Admin-Bereich
                                    der Webseite)
                            1.2.2.3.2.5 Phishing
                            1.2.2.3.2.6 Sniffing
                            1.2.2.3.2.7 Brute Forcing/Dictionary PW Guessing (auch nicht
                                    geänderte Standard PWs (z.B. Webserver Standard PWs,
                                    PHPmyAdmin Standard PWs, etc.))
                            1.2.2.3.2.8 CSRF (z.B. PW ändern - <img src="http://example.com/
                                    update_account.asp?new_password=evil">)
                            1.2.2.3.2.9 SSI (Server side includes)
        1.2.3 Attacke durchführen
              OR
              1.2.3.1 Stehlen sensitiver Informationen, z.B. Webcam Daten
              1.2.3.2 Daten löschen/korrumpieren
              1.2.3.3 Malware installieren, die Schwachstellen in Browsern ausnützen können
                      (drive-by downloads)
              1.2.3.4 Webseite verunstalten (Website defacement) auch um z.B. auf der Webseite
                      basierte Aktionen (Schneeräumung) zu behindern
                      OR
                      1.2.3.4.1 XSS
                      1.2.3.4.2 HTTP Response Splitting (inkl. Cache Poisoning)
                      1.2.3.4.3 Domain Hijacking (Webseite "übernehmen" => falls ein
                                Registrar schwache Authentisierungsmassnahmen verwendet (z.B.
                                wird nur auf die E-Mail-Adresse des Administrators geschaut),
                                kann ein Angreifer den DNS-Record "stehlen" und auf eine
                                beliebige IP-Adressen zeigen lassen -> siehe auch:
                                http://www.darknet.org.uk/2006/09/domain-stealing-or-how-to-
                                hijack-a-domain/)
                      1.2.3.4.4 Text-/Bildinformation verändern
2. Bedienebene kompromittieren
   OR
   2.1 Einschränkung der Verfügbarkeit durch nicht bösartige berechtigte Benutzer
       (Ziel: Kein Angriffsziel sondern Fehlmanipulationen)
       OR
       2.1.1 Einspielen von Patches/OS Updates/Virenupdates (durch Mitarbeiter oder
             Lieferanten; Patches, die sich irgendwie nicht "vertragen" mit
             Betriebssystem, können System lahm legen)
       2.1.2 Logische Bedienfehler (aus Versehen Signale falsch stellen)
       2.1.3 Physische Bedienfehler (aus Versehen Stecker ziehen)
       2.1.4 Einstecken eines mit Viren verseuchten Laptops/USB Sticks (z.T. werden
             Virenupdates mit USB-Sticks durchgeführt)
       2.1.5 Allgemeine Wartungsarbeiten, welche direkt vor Ort am laufenden System
             gemacht werden (durch Mitarbeiter oder Lieferanten; bei unsachgemässer
             Installation einer neuen Systemkomponente kann das System lahm gelegt
             werden)
   2.2 Einschränkung der Verfügbarkeit mittels Cyberattacke, ohne
       Systemkompromittierung
       (Ziel: Betrieb stören, ohne aber Systeme zu übernehmen und damit
       tiefergehende oder längerfristige Attacken durchzuführen)
       AND
       2.2.1 Angreifbare Systeme identifizieren
             OR
             2.2.1.1 Insiderkenntnisse (Mitarbeiter, Lieferant; auch Ehemalige)
             2.2.1.2 Social Engineering (Fragen nach Information)
             2.2.1.3 Mittels Analysemethoden
                     AND
                     2.2.1.3.1 Information Gathering (IP-Adressen, E-Mail Adressen,
                               VPN-Konfigurationsdaten, Telefonnummern,
                               Firewallkonfigurationen, Domainnamen, Informationen
                               von/über Lieferanten, etc.)
                     2.2.1.3.2 Offene Ports und Schwachstellen detektieren
                               AND
                               2.2.1.3.2.1 Portscan
```

Abbildung 8: Betrieb stören - Teil 2

```
                        2.2.1.3.2.2 Vulnerability Scan
                        2.2.1.3.2.3 Enumeration
    2.2.2 Attacke ausführen
          OR
          2.2.2.1 DoS/DDoS Attacke (siehe 1.1.2.1)
          2.2.2.2 Malware verbreiten (Die Malware soll dabei dazu dienen, Systeme
                  lahmzulegen (z.B. durch agressives Scanning oder durch logisches
                  Zerstören der Systeme))
                  OR
                  2.2.2.2.1 Durch absichtliche Installation eines Mitarbeiters oder
                            Lieferanten (auch böswillig manipulierte Software => Software,
                            die im Hintergrund etwas Böswilliges macht)
                  2.2.2.2.2 Einstecken eines verseuchten Laptops/USB Sticks
                            OR
                            2.2.2.2.2.1 Durch Mitarbeiter oder Lieferant nach unsachgemässem
                                        Umgang mit dem Laptop
                            2.2.2.2.2.2 Durch Angreifer nach Diebstahl eines Laptops
                  2.2.2.2.3 Durch verseuchte E-Mail Attachments
                  2.2.2.2.4 Durch Ausnutzen einer Schwachstelle im System
                  2.2.2.2.5 Durch Kompromittieren der Viren-Update-Server
2.3 Einschränkung der Verfügbarkeit mittels Cyberattacke, mit
    Systemkompromittierung
    (Ziel: Betrieb stören und Systeme zu übernehmen um damit tiefergehende
    oder längerfristige Attacken durchzuführen. Dies beinhaltet auch z.B.
    die Übernahme der Kontrolle von VT-Anlagen wie Tunnelanzeigen)
    AND
    2.3.1 Angreifbare Systeme identifizieren (siehe 2.2.1)
    2.3.2 Zugang zu den Systemen erhalten
          OR
          2.3.2.1 Als berechtigter Benutzer (Mitarbeiter, Lieferant, Polizei)
          2.3.2.2 Als ehemals berechtigter Benutzer (Mitarbeiter, Lieferant)
                  OR
                  2.3.2.2.1 Installation einer Backdoor während der Benutzer noch
                            berechtigt Zugang hatte
                  2.3.2.2.2 Durch Nutzung von Zugangsberechtigungen, die dem
                            Benutzer nicht entzogen wurden
          2.3.2.3 Als externer Angreifer
                  OR
                  2.3.2.3.1 Mittels Impersonation (Ausgeben als Mitarbeiter, Lieferant,
                            Polizist)
                  2.3.2.3.2 Durch Cyberattacke
                            OR
                            2.3.2.3.2.1 Dial-Up Hacking (VPN, ISDN)
                                        OR
                                        2.3.2.3.2.1.1 Mit gestohlenem Wartungs-Laptop (evtl.
                                                      sind Credentials hardcoded)
                                        2.3.2.3.2.1.2 Mit einem unbeteiligten Gerät
                            2.3.2.3.2.2 Sniffing (z.B. Network PW Exchange)
                            2.3.2.3.2.3 Brute Forcing/Dictionary PW Guessing (auch
                                        Standard PWs und Gastaccounts berücksichtigen)
                            2.3.2.3.2.4 Social Engineering (z.B. Phishing)
                            2.3.2.3.2.5 Ausnutzen von Schwachstellen (z.B. nicht gepatchte
                                        Vulnerability)
                            2.3.2.3.2.6 Malware verbreiten (siehe 2.2.2.2) (Die Malware
                                        soll dabei dazu dienen, dass der Angreifer die
                                        infizierten Systeme kontrollieren kann, entweder
                                        durch autonomes Verhalten oder durch Kontaktaufnahme
                                        mit einen Rechner des Angreifers, wodurch das
                                        infizierte System ferngesteuert werden kann. Auch
                                        Keyloggers könnten installiert werden)
                            2.3.2.3.2.7 Wireless Hacking (evtl. auch GSM, GPRS)
    2.3.3 Attacke durchführen
          OR
          2.3.3.1 Stehlen sensitiver Informationen (z.B. AGK-Personendaten);
                  Bild-Videomaterial (sensitive Daten könnten veröffentlicht werden)
          2.3.3.2 Daten löschen/korrumpieren (z.B. Logging-Daten, Videobilder, Prognosen
                  über Verkehrszahlen, etc.)
          2.3.3.3 Strassenanlagen "bedienen" (Signalisation, Glatteiswarnanzeige, Tunnel
                  schliessen, Tunnelbesprechnungsanlage, etc.)
          2.3.3.4 Software installieren (z.B. um eine Backdoor zu kreieren, Firewall-Regeln
```

Abbildung 9: Betrieb stören - Teil 3

```
                abändern, etc.)
   2.4 Einschränkung der Verfügbarkeit durch physische Attacke
       (Ziel: Betrieb stören, ohne aber Systeme zu übernehmen und damit tiefergehende
       oder längerfristige Attacken durchzuführen)
       AND
       2.4.1 Zugang zu den Systemen erhalten
             OR
             2.4.1.1 Als berechtigter Benutzer (Mitarbeiter, Lieferant)
             2.4.1.2 Als ehemals berechtigter Benutzer (Mitarbeiter, Lieferant)
                     OR
                     2.4.1.2.1 Durch Nutzung von Schlüsseln, die dem
                               Benutzer nicht entzogen wurden
             2.4.1.3 Als externer Angreifer
                     OR
                     2.4.1.3.1 Mittels Impersonation (Ausgeben als Mitarbeiter oder
                               Lieferant)
                     2.4.1.3.2 Durch Einbruch (das kann sehr einfach sein, da die Systeme
                               z.T. nur ungenügend abgesichert sind)
       2.4.2 Attacke durchführen
             OR
             2.4.2.1 Feuer legen
             2.4.2.2 Server ausstecken/herunterfahren
             2.4.2.3 Kabel durchschneiden/ausstecken
             2.4.2.4 Backup-Tapes zerstören/stehlen
   2.5 Einschränkung der Verfügbarkeit durch Unfall
       (Ziel: Kein Angriffsziel, sondern durch einen Unfall wird die Verfügbarkeit
       des Systems eingeschränkt)
       OR
       2.5.1 Gasexplosion
       2.5.2 Wasserleitung defekt
3. Feldebene kompromittieren
   OR
   3.1 Einschränkung der Verfügbarkeit durch physische Attacke
       (Ziel: Betrieb stören, ohne aber Systeme zu übernehmen und damit tiefergreifende
       oder längerfristige Attacken durchzuführen)
       AND
       3.1.1 Zugang zu den Systemen erhalten (siehe 2.4.1)
       3.1.2 Attacke durchführen
             OR
             3.1.2.1 Feuer legen (z.B. in einem Tunnel)
             3.1.2.2 Feldkomponenten mit Gewalt zerstören
             3.1.2.3 Kabel ausstecken/durchtrennen
             3.1.2.4 Brandmeldesensor manipulieren
             3.1.2.5 Videokameras ausstecken
   3.2 Einschränkung der Verfügbarkeit durch "Cyberattacke" vor Ort
       (Ziel: Betrieb stören und Systeme übernehmen. Anlagen sollen kontrolliert
       werden. Um die Systeme kontrollieren zu können, ist ein entsprechender
       Service-Laptop nötig) => der Servicelaptop ist absolut zwingend bei AGK-Systemen
       AND
       3.2.1 Zugang zu den Systemen erhalten (siehe 2.4.1)
       3.2.2 Attacke durchführen
             OR
             3.2.2.1 Stehlen sensitiver Informationen; Bild-Videomaterial
             3.2.2.2 Strassenanlagen "bedienen"
             3.2.2.3 Feldkomponenten umprogrammieren (z.B. so, dass Alarme nicht mehr
                     gemeldet werden. Auch Zugangsinformationen könnten geändert werden)
   3.3 Einschränkung der Verfügbarkeit durch ungünstige Witterungsverhältnisse/
       Naturkatastrophen
4. "Rest des Netzes" kompromittieren (Prozessleitebene, Gruppenleitebene, Einzelleitebene)
   (Idee: System kann hier grundsätzlich ähnlich kompromittiert werden wie auf Level
   "Bedienebene", allerdings dürften die Systeme auf dieser Stufe weniger nach
   aussen exponiert sein)
   OR
   4.1 Einschränkung der Verfügbarkeit durch nicht bösartige berechtigte Benutzer
       (Ziel: Kein Angriffsziel, sondern Fehlmanipulation) (siehe 2.1)
   4.2 Einschränkung der Verfügbarkeit durch Unfall oder Versehen
       (Ziel: Kein Angriffsziel, sondern durch einen Unfall wird die Verfügbarkeit
       des Systems eingeschränkt)
       OR
       4.2.1 Bagger durchtrennt aus Versehen Kabel beim Graben eines Lochs
```

Abbildung 10: Betrieb stören - Teil 4

```
4.3 Einschränkung der Verfügbarkeit mittels Cyberattacke, ohne Systemkompromittierung
    (Ziel: Betrieb stören, ohne aber Systeme zu übernehmen und damit tiefergehende
    oder längerfristige Attacken durchzuführen)
    (siehe 2.2; verseuchte E-Mail-Attachments und kompromittierte Virenupdateserver
    können auf dieser Ebene wahrscheinlich vernachlässigt werden)
4.4 Einschränkung der Verfügbarkeit mittels Cyberattacke, mit Systemkompromittierung
    (Ziel: Betrieb stören und Systeme zu übernehmen um damit tiefergehende oder
    längerfristige Attacken durchzuführen. Dies beinhaltet auch z.B. die Übernahme der
    Kontrolle von VT-Anlagen wie Tunnelanzeigen)
    (siehe 2.3)
4.5 Einschränkung der Verfügbarkeit durch physische Attacke
    (Ziel: Betrieb stören, ohne aber Systeme zu übernehmen und damit tiefergreifende oder
    längerfristige Attacken durchzuführen)
    AND
    4.5.1 Zugang zu den Systemen erhalten (siehe 2.4.1)
    4.5.2 Attacke durchführen
          OR
          4.5.2.1 Feuer legen
          4.5.2.2 Rechner herunterfahren/ausstecken (z.B. Gruppenrechner/Tunnelrechner)
          4.5.2.3 Rechner mit Gewalt zerstören (z.B. Gruppenrechner/Tunnelrechner)
          4.5.2.4 Kabel absichtlich ausstecken/durchtrennen (z.B. in irgendeiner
                  Verteilzentrale, wo die Kabel zusammenlaufen)
```

Abbildung 11: Betrieb stören - Teil 5

5.2 Angriffsvektoren

Die hier aufgeführten Angriffsvektoren stammen aus unserem Attack-Tree (Kapitel 5.1). Es werden alle möglichen Angriffsvektoren, die sich aus dem Attack-Tree ableiten lassen, aufgeführt. Gewisse Angriffsvektoren wurden bereits vorgruppiert (z.B. Software-Schwachstellen ausnutzen). Die Reihenfolge, in welcher die nachfolgenden Angriffsvektoren aufgelistet werden, hat keine tiefere Bedeutung. Die Angriffsvektoren sind also nicht etwa nach Gefährlichkeit oder Ausführungsschwierigkeit sortiert.

- Insiderkenntnisse
- Social Engineering (Impersonation, Phishing, Nachfragen nach Informationen)
- Information Gathering
- Portscanning
- Software-Schwachstellen detektieren (z.B. Vulnerability Scanner, Enumeration, Manual Webapplication Assessment)
- Software-Schwachstellen ausnutzen (Known Exploits, DoS/DDoS, Malware)
- Zugriff auf System als ehemals berechtigter Benutzer (mit Schlüsseln, nicht entfernte Benutzerkonten)
- Dial-Up/Wireless Hacking
- Brute Forcing/Dictionary PW Guessing
- Physische Attacken und Unfälle (Feuer legen, Einbruch, etc.)
- Sniffing
- Fehlmanipulation durch berechtigte Benutzer (Patches/OS-Updates/Malwareupdates, logische/physische Bedienfehler, Einstecken eines mit Malware verseuchten Laptops, Allgemeine Wartungsarbeiten am System)
- Strassenanlagen bedienen
- Stehlen sensitiver Informationen
- Daten löschen/korrumpieren
- Web-Cyberattacken (Session Hijacking, SQLi, Unvalidated Redirects and Forwards, CSRF, SSI, XSS)
- Website verunstalten
- Feldkomponenten umprogrammieren

5.3 Gruppierung der Angriffsvektoren

In diesem Kapitel werden die in Kapitel 5.2 identifizierten Angriffsvektoren in Angriffsgruppen gruppiert. Die Gruppen sind dabei so gewählt, dass jede Gruppe ein ganz bestimmtes Angriffsziel beschreibt. Die Angriffsvektoren einer Angriffsgruppe zeigen somit verschiedene Möglichkeiten auf, wie das Angriffsziel der entsprechenden Angriffsgruppe (ganz oder teilweise) erreicht werden kann. Es wurde versucht, die einzelnen Gruppen möglichst umfangreich mit potentiellen Angriffsvektoren zu beschreiben. Es können deshalb auch Angriffsvektoren aufgeführt sein, die so nicht in Kapitel 5.2 erwähnt wurden. Im Anhang I sind die Beziehungen zwischen den Angriffsvektoren und den Angriffsgruppen in einer Matrix dargestellt.

In Kapitel 6 "Verifikation bereits umgesetzter Sicherheitsmassnahmen" wird geprüft, wie gut die von den Interviewpartnern aktuell umgesetzten Sicherheitsmassnahmen gegen diese Angriffsgruppen schützen.

5.3.1 Zusammenstellen eines umfangreichen Profils mit Hilfe öffentlicher Informationen (Information Gathering)

Angreifer können sich mit Hilfe öffentlich zugänglicher Informationen ganze Profile über ihre Opfer zusammenstellen. Informationen, die für einen Angreifer interessant sein können, sind z.B. IP-Adressen, E-Mail-Adressen, VPN-Konfigurationsdaten, Telefonnummern, Firewall-Konfigurationen, Domainnamen, etc. Es ist deshalb wichtig, nur die nötigsten Informationen zu veröffentlichen. Wo immer möglich, sollten öffentlich zugängliche Informationen eingeschränkt werden.

Angriffsvektoren:

- Google Hacking (filetype:pcf site:example.com; Index of /password; etc.)
- Webcrawling (Firmenwebseiten auf lokalen Computer kopieren und mit speziellen Tools nach interessanten Informationen durchsuchen. Möglicherweise sind auskommentierte "Testpasswörter" im HTML-Code vorhanden etc.)
- Facebook, Jobwebseiten (evtl. geben Jobausschreibungen Informationen über den momentanen Security-Standard einer Firma Preis), Internetarchive (archive.org, thememoryhole.org), Internetforen (z.B. publizierte Firewallkonfigurationen etc.)
- WHOIS & DNS Enumeration (IP-Adressen und Domainnamen herausfinden)
- DNS Interrogation (zone transfer)
- Network Reconnaissance (Komplettes Profil der Netzarchitektur des Opfers zusammenstellen: traceroute, automatisierte Programme, etc.)

5.3.2 Scanning und Enumeration

Damit externe Angreifer Schwachstellen überhaupt ausnutzen können, müssen sie die Schwachstellen zuerst "entdecken". Damit der Angreifer gar nicht erst auf die verwundbaren Systeme gelangen kann, ist es wichtig, dass Firewalls konsequent eingesetzt und sicher konfiguriert werden. Ausserdem sollten nicht benötigte Services deaktiviert werden.

Angriffsvektoren:

- Nach offenen Ports scannen
- Ping Sweeps
- ICMP Queries
- Betriebssystem bestimmen
- Enumeration (Banner Grabbing, etc.)
- Nach Schwachstellen scannen (Nessus, Nikto, OpenVAS)

5.3.3 Ausnutzen von softwarebedingten Systemschwachstellen

Systeme, welche nicht gepatcht sind, lassen sich sehr einfach ausnutzen (z.B. mit "Point-and-Click-Malware"). Malware kann z.B. über absichtliche Installation eines Mitarbeiters, über E-Mail-Attachments oder kompromittierte Malwareupdateserver verbreitet werden. Systeme (v.a. diejenigen, die nach aussen exponiert sind), sollten deshalb stets auf dem aktuellsten Software-Stand gehalten werden. Ausserdem müssen die eingesetzten Systeme sicher konfiguriert werden (z.B. Webserver-Hardening, etc.).

Angriffsvektoren:

- Schwachstellen ausnutzen mit bekannten Exploits (www.exploit-db.com; Metasploit; Script-Kiddies, die irgendetwas ausprobieren wollen)
- Malware verbreiten, welche aggressives Scanning durchführt, um System lahmzulegen
- Backdoors installieren
- Malware verbreiten, die Rechner fernsteuern kann (Zombies)
- Keyloggers installieren
- DoS/DDoS
- Malware installieren, die Schwachstellen im Browser ausnutzen können
- Web-Cyberattacken (Session Hijacking, SQLi, Unvalidated Redirects and Forwards, CSRF, SSI, XSS)
- Manual Webapplication Assessment (Mit Browser Plug-ins, Web Proxies (z.B. Webscarab), Directory-Listing, Source Code Disclosure, Sample Files, Canonicalization Attacks)
- Webseiten verunstalten
- Daten löschen/korrumpieren
- Sensitive Daten stehlen
- Strassenanlagen bedienen für arglistige Zwecke

5.3.4 Password Cracking

Unsichere Passwörter können einfach von einem Angreifer gecrackt werden. Sichere Passwörter müssen deshalb "erzwungen" werden. Standardpasswörter bei Komponenten müssen geändert werden.

Angriffsvektoren:

- Brute Forcing
- Dictionary PW Guessing/Rainbowtables

5.3.5 Eindringen in das System über unsicher konfigurierte Remote-Zugänge oder Wireless-Zugänge

Die ganze Security-Architektur und damit verbundene Abwehrmassnahmen sind nichts wert, wenn man trotzdem über unsicher konfigurierte Remote-Zugänge oder Wireless-LAN ins System eindringen kann. Remote-Zugänge sollten deshalb genau überprüft werden. Unnötige Zugänge müssen entfernt werden. Wenn Wireless-LAN unbedingt notwendig ist, muss es sicher konfiguriert werden (z.B. WPA statt WEP).

Angriffsvektoren:

- VPN-Hacking (z.B. IKE-Aggressive-Mode hacken, etc.)
- Wardialing (einen Bereich möglicher Telefonnummern durchtesten mit spezieller Wardialing-Software - evtl. mit einem gestohlenen Laptop. Die ISDN-Zugänge beruhen ja zum Teil auf "Geheimhaltung der Telefonnummern")
- WEP-/WPA-Hacking
- GSM-/GPRS-Hacking (AGK will für mobile Stationen auch GSM-Zugang einbauen)

5.3.6 Sniffing

Durch einfaches Sniffen des Netzwerkverkehrs können Angreifer leicht an sensible Daten herankommen. Deshalb ist es wichtig, dass der Netzwerkverkehr wenn möglich verschlüsselt wird (zumindest sensible Daten).

Angriffsvektor:

- Sniffing (z.B. PW Exchange, etc.)

5.3.7 Social Engineering

Social Engineering ist ein sehr mächtiges Werkzeug. Mit Hilfe von Social-Engineering-Techniken kann ein Angreifer z.B. Informationen erhalten, welche nicht öffentlich zugänglich sind. Das kann so weit gehen, dass der Angreifer Passwörter oder sonstige heikle Daten in Erfahrung bringen kann. Social Engineering ist auch ein möglicher Kanal, um Malware zu verbreiten. Benutzer müssen deshalb auf solche Attacken sensibilisiert werden (z.B. kuriose E-Mail-Nachrichten mit Skepsis betrachten etc.).

Angriffsvektoren:

- Physischen Zugang als verkleideter Lieferant/Mitarbeiter erhalten
- Phishing (Mitarbeiter werden über E-Mail z.B. auf eine gefälschte Seite gelockt, wo sie gebeten werden, ihr Passwort zu übermitteln auf Grund von "irgendwelchen Sicherheitsvorkehrungen")
- E-Mail mit vertrauenswürdiger Absender-Adresse versenden (z.B. Adresse eines Lieferanten/Administrators/Mitarbeiters) um an interne Informationen (IP-Adressen, Domainnamen, Telefonnummern, Passwörter, etc.) ranzukommen
- Sich am Telefon als Lieferant/Mitarbeiter ausgeben, um sich einen Remotezugang freischalten zu lassen
- Ein E-Mail versenden, das schädlichen Code enthält (das kann Malware sein, die sich im Anhang befindet. HTML-Nachrichten können direkt schädlichen Script-Code enthalten)

5.3.8 Fehlmanipulation durch berechtigte Benutzer

Durch Fehlmanipulation der Benutzer kann die Sicherheit entscheidend geschwächt werden, auch wenn die eingesetzten technischen Mittel an sich ausreichend wären. Die Mitarbeiter müssen auf Sicherheitsprobleme sensibilisiert und im Umgang mit den Systemen geschult werden.

Angriffsvektoren:

- Patches/OS-Updates/Malwareupdates, welche System lahm legen können
- Logische/physische Bedienfehler
- Einstecken eines mit Malware verseuchten Laptops/USB Sticks
- Allgemeine Wartungsarbeiten am System (durch Mitarbeiter oder Lieferanten - bei unsachgemässer Installation einer neuen Systemkomponente kann das System lahm gelegt werden)

5.3.9 Angriffe durch unmotivierte oder verärgerte Mitarbeiter

Unmotivierte und verärgerte Mitarbeiter stellen ein sehr hohes Gefährdungspotenzial dar. Da sie die Systeme gut kennen und auch über gewisse Zugangsberechtigungen verfügen, können sie einen erheblichen Schaden am System anrichten. Die Rechte eines Benutzers sollten beim Eintritt und beim Austritt konsequent gemanagt werden. Dazu gehört die Vergabe der "richtigen" Schlüssel, der "richtigen" Rechte am Computersystem, etc. Beim Austritt des Mitarbeiters müssen diese Rechte entsprechend sauber wieder entfernt

werden.

Angriffsvektoren:

- Backdoors installieren
- Insiderkenntnisse (z.B. veröffentlichen sensibler Daten in einem öffentlichen Forum, aber auch ausnutzen der Kenntnisse für arglistige Zwecke)
- Strassenanlagen bedienen für arglistige Zwecke (als berechtigter Benutzer)
- Absichtliche Verbreitung von Malware (Einstecken eines verseuchten Laptops oder USB-Sticks)
- Sensitive Daten stehlen
- Daten löschen/korrumpieren
- Zugang zum System über nicht entfernte Benutzerkonten
- Zugang zum System über Schlüssel, die dem Benützer nicht entzogen worden sind
- Feldkomponenten umprogrammieren

5.3.10 Physische Attacken/Unfälle

Physische Attacken oder Unfälle können erheblichen Schaden anrichten und ausserdem für die Sicherheit der Mitarbeiter sowie der Verkehrsteilnehmer sehr gefährlich sein. Die Systeme müssen deshalb ausreichend vor unbefugtem Zutritt geschützt werden (z.B. durch Anbringen von sicheren Schlössern etc.). Ausserdem müssen angebrachte Schutzmassnahmen (z.B. Brandmelder) installiert werden.

Angriffsvektoren:

- Einbruch (z.B. in ein BLZ-Gebäude oder in eine Tunnelanlage)
- Feuer legen (z.B. in BLZ, Tunnels, etc.)
- Beschädigung von Feldkomponenten (Sensoren/Aktoren)
- Rechner (Tunnelrechner/Gruppenrechner) mit Gewalt zerstören
- Rechner (Tunnelrechner/Gruppenrechner) herunterfahren/ausstecken
- Kabel durchtrennen/ausstecken
- Brandmeldesensor manipulieren (z.B. in Tunnel, BLZ)
- Videokameras ausstecken
- Gasexplosion (in BLZ)
- Server ausstecken/herunterfahren
- Backup-Tapes zerstören
- Defekte Wasserleitung (in BLZ)
- Feldkomponenten umprogrammieren

6 Verifikation bereits umgesetzter Sicherheitsmassnahmen

In Kapitel 5, Bedrohungsanalyse, haben wir mögliche Bedrohungsszenarien für die VT-Systeme definiert. In diesem Kapitel soll nun untersucht werden, wie gut die aktuell umgesetzten Sicherheitsmassnahmen vor den identifizierten Bedrohungen schützen. Dazu werden die in Kapitel 5.3 aufgestellten "Angriffsgruppen" jeweils in einem eigenen Unterkapitel gesondert betrachtet und Mängel der aktuell umgesetzten Sicherheitsmassnahmen aufgedeckt. Ausserdem haben wir einen Servicelaptop eines Interviewpartners auf Schwachstellen untersucht. Die Resultate dieser Untersuchung ist im Kapitel 6.11 dokumentiert.

6.1 Information-Gathering

Wie bereits in Kapitel 5.3 angetönt geht es beim Information-Gathering (auch Footprinting genannt) darum, mit Hilfe öffentlich zugänglicher Informationen ein möglichst umfangreiches Profil über sein Opfer zusammenzustellen. Bei einer ausgedehnten Cyberattacke stellt Information-Gathering immer den ersten Schritt dar. Es bildet sozusagen den Grundstein für eine erfolgreiche Attacke. Je mehr Informationen man in dieser Phase über sein Opfer erhält, desto gezielter kann eine Attacke ausgeführt werden. Information-Gathering darf also durchaus als einer der wichtigsten Schritte einer Cyberattacke bezeichnet werden.

Information-Gathering wird nicht nur zur Vorbereitung von Cyberattacken durchgeführt. Auch zum Beispiel bei physischen Banküberfällen bereiten sich die Täter intensiv auf die Attacke vor, indem sie sich im Vorfeld der Attacke möglichst viele Informationen über die anzugreifende Bank beschaffen. So wird zum Beispiel untersucht, wo sich überall Kameras befinden, wie viele Fluchtwege es gibt, welche Alarmierungsmechanismen installiert sind, etc.

In einem Penetration-Test wird Information-Gathering durchgeführt, damit man eine Ahnung davon erhält, was Angreifer "alles sehen können". Wenn man weiss, was Hacker sehen können, so kennt man auch potentiell exponierte Sicherheitsschwachstellen des eigenen Systems, was wiederum dabei hilft, eine mögliche Ausnutzung der Schwachstellen zu verhindern [McClure, 2009].

Information-Gathering ist also auch in einem Penetration-Test ein sehr wichtiger Schritt. Trotzdem scheint es so, dass sich viele Organisationen der Gefahr unbeabsichtigt veröffentlichter Sicherheitsinformationen nicht richtig bewusst sind. Besonders kritisch dabei ist, dass ein Angreifer Informationen über ein Opfer "passiv" sammeln kann, also ohne je in direkten Kontakt mit einem Firmenserver zu treten. Information-Gathering ist somit für potenzielle Opfer nicht detektierbar (man spricht deshalb auch von *Passive* Information-Gathering) [Ollmann, 2004].

Hacker und Penetration-Tester konzentrieren sich beim Information-Gathering insbesondere auf folgende Informationen (die folgende Liste ist nicht abschliessend) [McClure, 2009]:

- Öffentlich zugängliche Informationen
  - Firmenwebseiten
  - Partnerorganisationen
  - Firmenstandorte
  - Informationen über Angestellte: Telefonnummern, Kontaktinformationen, E-Mail-Adressen, Personelle Informationen über Angestellte
  - Security-Policies, technische Details über eingesetzte System-Komponenten
  - Archivierte Informationen

  - Verärgerte Mitarbeiter
  - Etc.
- Domainnames
- IP-Adressen
- Systemarchitektur
- Access-Control-Mechanismen und entsprechende Access-Control-Lists (ACL)
- Intrusion-Detection-Systeme (IDS)
- Etc.

Die Möglichkeiten, die sich einem Angreifer bei Kenntnis der oben erwähnten Informationen bieten, sind vielfältig. So können z.B. E-Mail-Adressen oder Telefonnummern und weitere Informationen über Angestellte für Social-Engineering-Attacken missbraucht werden. Telefonnummern (insbesondere ganze Bereiche von Telefonnummern) sind aber auch für War-Dialing-Attacken (siehe Kapitel 6.5) sehr interessant. Auch die Kenntnis von Partnerorganisationen kann sehr interessant sein. So ist es zum Beispiel möglich, dass Partnerorganisationen (z.B. Lieferanten) zusätzliche sensitive Informationen über die Zielorganisation liefern (z.B. Informationen über verwendete IT-Technologien, etc.). Oft werben Partnerorganisationen auch mit Referenzen über ihre Kunden. Security-Policies und Details über eingesetzte Komponenten sind ebenfalls sehr wertvolle Informationen für einen Angreifer. Bei Kenntnis von Security-Policies kann der Angreifer Wege suchen, wie er die eingesetzten Sicherheitsmassnahmen (z.B. Firewalls) umgehen kann. Die Kenntnis der eingesetzten technischen Komponenten erlaubt dem Angreifer, sich detaillierte Informationen über die Komponenten im Internet zu beschaffen (z.B. Bedienungsanleitungen, Standardpasswörter, publizierte Schwachstellen, etc.). Domainnames und IP-Adressen erlauben dem Angreifer, sich ein detailliertes Bild über die Netzwerkarchitektur zu verschaffen. Diese Information ermöglicht es, anspruchsvolle und ausgeklügelte Attacken zu einem späteren Zeitpunkt auszuführen [McClure, 2009][Ollmann, 2004].

6.1.1 Techniken und Ressourcen

An dieser Stelle wollen wir ein paar häufig verwendete Information-Gathering-Techniken auflisten und kurz etwas näher beleuchten. Für detaillierte Informationen verweisen wir auf die Literatur [McClure, 2009][Ollmann, 2004].

- Firmenwebsites nach Kontakten absuchen: Telefonnummern, E-Mail-Adressen, Standorte, etc.
- WHOIS-Queries: Die Domainnamen und IP-Adressen, die im Internet verwendet werden, müssen irgendwo zentral verwaltet werden. Auf so genannten WHOIS-Servern erhält man Zugang zu diesen Informationen. Das ist besonders für Hacker interessant, um beispielsweise IP-Adressblöcke und Namensserver seines Opfers zu bestimmen. Aber auch Kontaktinformationen lassen sich abfragen (gemeint sind Kontaktinformationen der Person/Organisation, die eine bestimmte Domain oder einen bestimmten IP-Adressblock registrieren liess). Mögliche Kontaktinformationen, die sich herauslesen lassen, sind Namen, E-Mail-Adressen, Telefonnummern, etc.
- Google-Hacking: Die erweiterten Suchmöglichkeiten von Google bilden ein sehr mächtiges Werkzeug, um an sensitive Informationen heranzukommen. So kann man zum Beispiel mit `site:example.com` die Suche auf die Domain example.com und Subdomains davon beschränken. Mit `filetype:type` (für `type` kann z.B. pdf, doc, xls, etc. stehen) kann man nach Dateien bestimmten Typs suchen. Auf diese Weise können zum Beispiel sensitive Dokumente ausfindig gemacht werden. Weitere interessante Optionen sind `inurl:url` (sucht nach Dokumenten, die mit der URL `url` referenziert sind oder in dessen URL `url` vorkommt) und `intitle:title` (Dokumente, die `title` im Titel enthalten). Die gerade erwähnten Suchoptionen können natürlich auch miteinander kombiniert werden, um mächtige und effektive Suchanfragen zu formulieren. Google-Hacking ist derart effektiv, dass es sogar eine Webseite gibt, die sich ausschliesslich mit diesem Thema beschäftigt[33].

[33] http://johnny.ihackstuff.com/ghdb/

- Forced-Browsing: Bezeichnet eine Technik, mit der versucht wird, verschiedene Verzeichnisse auf einem Webserver ausfindig zu machen, die nicht direkt verlinkt sind (d.h. es gibt auf der "regulären Webseite" keinen Link, welcher auf solche Verzeichnisse zeigt). Solche Verzeichnisse können zum Beispiel sensitive Informationen enthalten. Forced-Browsing wird häufig mit entsprechenden Tools automatisiert (z.B. DirBuster[34]).
- SMTP-Headers: Mit SMTP (Simple Mail Transfer Protocol) werden E-Mail-Nachrichten vom Host des Verfassers zu dessen E-Mail-Server und zwischen verschiedenen Zwischenstationen versendet. Das Protokoll schreibt dabei vor, dass Adressinformationen über die Zwischenstationen, bei denen eine E-Mail-Nachricht vorbeigekommen ist, in den so genannten "E-Mail-Header" eingetragen werden müssen. Für Angreifer können solche Informationen sehr interessant sein, nicht zuletzt deshalb, weil in diesen E-Mail-Header firmeninterne IP-Adressen abgebildet sein können. Auch die Adresse des Mail-Servers einer Organisation ist natürlich im E-Mail-Header vorhanden. Nun erhält ein Angreifer wahrscheinlich nicht einfach so eine E-Mail-Nachricht von einem Mitarbeiter der Zielorganisation. Allerdings kann er einen SMTP-Bounce forcieren: Dabei sendet er eine E-Mail-Nachricht an einen fiktiven User der Organisation (d.h. an einen Benutzer, der mit Sicherheit nicht existiert). Da der User nicht existiert, wird der Mailserver der Zielorganisation mit grosser Wahrscheinlichkeit eine Fehlermeldung generieren und diese per Mail an den Angreifer zurücksenden. Die Headers dieser "Fehlermeldungs-E-Mail" enthalten dann auch wieder potentiell interessante Informationen.
- robots.txt: Die Datei robots.txt wird verwendet, um Webcrawlern und Suchrobotern (wie sie zum Beispiel von Suchmaschinen wie Google zur Indexierung von Webseiten verwendet werden) mitzuteilen, welche Verzeichnisse auf einem Webserver nicht gecrawlt (indexiert) werden sollen. Webadministratoren geben in dieser Datei also Verzeichnisse an, bei denen sie aus irgendwelchen Gründen verhindern wollen, dass diese indexiert, und somit öffentlich verfügbar gemacht werden. Oftmals sind das Verzeichnisse, die sensitive Informationen oder Seiten mit Logins zu irgendwelchen Services oder Administrationstools beinhalten (z.B. phpMyAdmin, Webmail, etc.). Die Datei robots.txt kann ohne weiteres von potentiellen Angreifern eingesehen werden, indem sie einfach die URL www.example.com/robots.txt aufrufen (natürlich wird vorausgesetzt, dass die Datei auch tatsächlich existiert).
- Suche nach möglichen Subdomains einer Organisation.
- HTML-Source-Code-Analyse: Dabei wird die Webseite einer Organisation auf den lokalen Rechner des Angreifers kopiert (Mirroring) und mit speziellen Tools nach interessanten Informationen durchsucht (z.B. Passwörter, Kommentare mit sensitiven Informationen, etc.).
- Personensuche: Personensuchdienste, wie zum Beispiel yasni.ch, suchen aus verschiedensten Quellen (zum Beispiel Facebook, Yellowpages, Amazon, etc.) Informationen über eine bestimmte Person zusammen. Diese Informationen können potenziell sehr wertvoll sein und zum Beispiel für Social-Engineering-Attacken missbraucht werden.
- Network-Reconnaissance: Dieser Begriff umschreibt eine Technik, bei der man sich mit gewissen Tools (z.B. traceroute) ein detailliertes Bild über die Netzwerkarchitektur des Opfers verschafft. So können zum Beispiel Router, Firewalls, Subnetze, etc. identifiziert werden.
- DNS-Interrogation: Hierbei fragt man die Nameserver der Zielorganisation nach interessanten Informationen (IP-Adressen, vorhandene Hosts, Mailserver, etc.) an. Eine der mächtigsten Techniken (bezüglich der Informationen, die man dadurch erhalten kann) ist der so genannte Zone-Transfer. Zone-Transfers an sich sind nichts Schlimmes. Ein Zone-Transfer wird normalerweise zwischen zwei DNS-Servern einer Organisation durchgeführt, um sich gegenseitig zu synchronisieren. Zone-Transfers sollten allerdings nicht von jedem beliebigen Host aus durchgeführt werden können, da in einem Zone-Transfer detaillierte Informationen über interne Hosts und IP-Adressen ausgetauscht werden können. Ebenfalls eine interessante Technik ist das DNS-Bruteforcing. Dabei wird im Wesentlichen ein Bereich von IP-Adressen durchprobiert

[34] http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project

(Reverse-DNS-Lookup), um zu schauen, welche Hosts tatsächlich vorhanden sind. Vorzugsweise werden dazu automatisierte Scripts verwendet.

- Google-Newsgroups-Interface[35]: Mit dem Newsgroups-Interface der Google Suchmaschine können öffentliche Newsgroups nach Informationen abgesucht werden. Newsgroups können Postings mit potenziell sehr sensitiven Informationen enthalten. So kommt es durchaus vor, dass Systemadministratoren ganze Firewallkonfigurationen ihrer Organisation veröffentlichen, um nach Lösungen für ein Problem zu fragen.

Für einige der oben erwähnten Techniken (insbesondere DNS-Interrogation, WHOIS-Queries) gibt es im Internet frei nutzbare Online-Network-Tools. Mit diesen Tools kann ein Angreifer kaum zurückverfolgt werden, da die resultierenden Requests nicht vom Host des Angreifers, sondern vom Server des Onlinedienstes abgeschickt werden (die Anfragen sind "stealthier"). Folgende Webseiten bieten solche Network-Tools an:

- http://network-tools.com
- http://news.netcraft.com
- http://emailstuff.org

6.1.2 Ausgeführte Tests

Um eine Ahnung davon zu erhalten, wie viele und welche Informationen über die verschiedenen Interviewpartner erhältlich sind, haben wir im Rahmen dieses Forschungsprojektes auch ein Information-Gathering durchgeführt. Dabei sind wir von den Informationen ausgegangen, die wir während der Interviews von den Interviewpartnern erhalten haben. Folgende Techniken sind dabei zum Einsatz gekommen:

- Firmenwebseiten nach Kontakten absuchen
- WHOIS-Queries (Domain-Name-Informationen, Informationen über IP-Adressblöcke)
- Google-Hacking
- Forced-Browsing
- SMTP-Bounce
- robots.txt
- Suche nach möglichen Subdomains
- Personensuche
- Google-Newsgroups-Interface
- DNS-Interrogation
- Network-Reconnaissance

6.1.3 Folgerungen

Folgende Dinge sind uns während den Tests speziell aufgefallen:

- Bei gewissen Nameservern konnten Zone-Transfers durchgeführt werden.
- Die Registrant-Informationen, die bei WHOIS-Servern eingesehen werden können, sind in praktisch allen Fällen viel zu detailliert.
- Lieferanten werben mit Kundenreferenzen. So konnten Informationen über eingesetzte Technologien gewonnen werden.
- Gewisse Webseiten enthalten sensitive Dokumente (z.B. Organigramme, ganze Telefonlisten, technische Spezifikationen, Finanzpläne, Geschäftsberichte, etc.).
- Einige Weblogins konnten ausfindig gemacht werden.
- Bei einem Webserver können problemlos Verzeichnisse mit sensitiven Informationen im Webbrowser eingesehen werden.
- Bei einem Nameserver konnten DNS-Reverse-Lookup-Queries durchgeführt werden.

[35] groups.google.ch

6.2 Scanning und Enumeration

Nachdem man mit Hilfe von Information-Gathering-Techniken (siehe Kapitel 6.1) erste Informationen über sein Opfer gesammelt hat (z.B. IP-Adressblöcke, Domainnamen, etc.), geht es in der Scanning-Phase nun darum herauszufinden, welche Systeme überhaupt von aussen erreichbar und welche Ports/Services auf diesen Systemen offen sind. Es wird also sozusagen nach offenen "Türen und Fenstern" gesucht, über welche man allenfalls in das System eindringen kann.

Aufgrund der Resultate aus der Scanning-Phase wird schliesslich versucht, die erreichbaren Systeme und Services, die von den Systemen angeboten werden, genauer auf bekannte Schwachstellen zu untersuchen. Im Unterschied zu früheren Phasen einer Attacke (also Information-Gathering und Scanning) stellt der Angreifer jetzt aber aktive Verbindungen zu den Zielsystemen her und stellt direkte, gezielte Anfragen an die Systeme. Solche Verbindungen sollten demnach geloggt oder sonst irgendwie identifiziert werden [McClure, 2009]. Informationen, die normalerweise während der Enumeration-Phase gesucht werden, sind Benutzernamen, schlecht geschützte Netzwerk-Shares und alte Softwareversionen mit bekannten, öffentlich publizierten Schwachstellen. Enumerations-Techniken sind stark abhängig von den gesammelten Informationen aus der Scanning-Phase, d.h. je nachdem welche Ports und Services auf den Systemen erreichbar sind, müssen unterschiedliche Techniken und Tools angewendet werden. Deshalb existieren auch einige Tools, welche Portscanning direkt mit Enumerations-Techniken kombinieren. So kann zum Beispiel das Tool Superscan[36] ein System scannen und, falls offene Ports gefunden wurden, direkt auch ein Banner-Grabbing durchführen, um detailliertere Informationen über verwendete Softwareversionen der erreichbaren Services zu erhalten. Auch nmap[37] erlaubt es, Banner von erreichbaren Services einzuholen.

Häufig kommen nach der Scanning-Phase auch so genannte "Vulnerability-Scanner" (Schwachstellen-Scanner) zum Einsatz. Solche Scanner testen ein Zielsystem aktiv auf bekannte Schwachstellen - unbekannte, bisher nicht publizierte Schwachstellen (vgl. zero-day attacks[38]) können mit solchen Tools allerdings nicht aufgedeckt werden. Populäre Schwachstellen-Scanner sind zum Beispiel "nessus"[39] oder das Open-Source-Tool "OpenVAS"[40]. Für den Web-Bereich gibt es spezielle, dedizierte Schwachstellenscanner: Nikto[41] ist ein Beispiel eines Web-Server-Schwachstellenscanner, welcher nach spezifischen Schwachstellen in der Web-Server-Software sucht. Ausserdem gibt es weitere Tools, um Webapplikationen detailliert auf Schwachstellen zu untersuchen, wie zum Beispiel das Open-Source-Tool w3af[42]. Solche Schwachstellenscanner, die auf eine bestimmte Art von Applikationen (z.B. Webapplikationen) spezialisiert sind, können auch unbekannte, bisher nicht veröffentliche Schwachstellen in einer Applikation ausfindig machen.

Am Schluss der Scanning- und Enumeration-Phase ist der Angreifer im Besitz einer Liste von erreichbaren Hosts und Services, die von den Hosts angeboten werden, inkl. potentieller Schwachstellen. Ausserdem (je nach offenen Services) kann ein Angreifer auch im Besitz von gültigen User-IDs sein, sowie eventuell vorhandenen Netzwerk-Shares, etc. Diese Informationen können nun verwendet werden, um bekannte Exploits auszutesten oder eigene Exploits zu schreiben, um das System teilweise oder komplett zu kompromittieren. Bekannte Schwachstellen werden entweder direkt von Schwachstellen-Scannern geliefert oder dann verwendet der Angreifer öffentlich zugängliche Datenbanken, welche bekannte Schwachstellen zu bestimmten Services und Applikationen dokumentieren (z.B. die "Common Vulnerabilities and Exposures" Datenbank, CVE[43]). Öffentlich zugäng-

[36] http://www.foundstone.com/us/resources/proddesc/superscan.htm
[37] http://nmap.org/
[38] http://en.wikipedia.org/wiki/Zero-day_attack
[39] http://www.nessus.org/nessus/
[40] http://www.openvas.org/
[41] http://cirt.net/nikto2
[42] http://w3af.sourceforge.net/
[43] http://cve.mitre.org/

liche Exploits zu bekannten Schwachstellen können z.B. bei Exploits Database[44] oder bei Metasploit[45] eingesehen werden. Gültige User-IDs können dazu verwendet werden, um Password-Cracking-Versuche zu beschleunigen. Wenn bereits einige gültige User-IDs bekannt sind, müssen nur noch verschiedene Passwortmöglichkeiten für die entsprechenden User-IDs durchprobiert werden, ohne auch noch mögliche User-IDs austesten zu müssen. Schlecht geschützte Netzwerk-Shares können Zugang zu sensitiven Dokumenten gewähren.

6.2.1 Techniken und Ressourcen

In diesem Abschnitt möchten wir ein paar Techniken, die häufig während der Scanning- und Enumeration-Phase verwendet werden, etwas näher beleuchten. Für detailliertere Informationen verweisen wir auf die Literatur [McClure, 2009].

Techniken für die Scanning-Phase:

- Ping-Sweeps: Mit herkömmlichen Pings[46] kann bestimmt werden, ob ein gewisses Host-System erreichbar ist oder nicht. Angreifer möchten aber meistens ein ganzes Netzwerk nach erreichbaren Hosts abscannen. Dazu bedienen sie sich einer Technik, die im Allgemeinen als "Ping-Sweep" bekannt ist. Dabei können mehrere IP-Adressen gleichzeitig überprüft werden. Normalerweise verwenden Pings ICMP-Echo-Request-Nachrichten. Häufig werden Echo-Request-Pakete allerdings von Firewalls geblockt. Damit Ping-Sweeps trotzdem möglich sind, können auch UDP oder TCP Pakete gesendet werden. Der Vorteil dabei ist, dass gewisse Ports (wie z.B. Port 80) selten von Firewalls geblockt werden. Gewisse Tools (z.B. hping3[47]) erlauben auch das Fragmentieren von Paketen, wodurch die Wahrscheinlichkeit noch geringer wird, dass die Pakete von einem Access-Control-Device (z.B. einem Intrusion-Detection-System (IDS)) erkannt werden. Bekannte Ping-Sweep-Utilities sind z.B. fping[48], hping3 oder nmap.
- ICMP-Queries: Neben den "herkömmlichen" ICMP-Echo-Request-Nachrichten, die standardmässig beim Pingen verwendet werden, können im Prinzip beliebige ICMP-Nachrichten an Hosts gesendet werden, um verschiedenste Informationen über das Ziel-System in Erfahrung zu bringen. Voraussetzung ist natürlich immer, dass entsprechende ICMP-Pakete nicht von der Firewall geblockt werden. Interessante ICMP-Pakete sind zum Beispiel ICMP-Type-13 (TIMESTAMP) und ICMP-Type-17 (ADDRESS MASK REQUEST). ICMP-Type-17-Nachrichten können an Router gesendet werden, um die Netzmaske eines gewissen Subnetzes zu erhalten. Durch die Kenntnis der Netzmaske eines Subnetzes ergeben sich folgende Vorteile: Einerseits ist dann die Netzadresse bekannt, wodurch man den ganzen IP-Range des Subnetzes kennt. Andererseits kennt man dann aber auch die Broadcastadresse, welche zum Beispiel für DoS-Attacken verwendet werden kann. Entsprechende Tools, um spezielle ICMP-Nachrichten abzuschicken, sind zum Beispiel icmpquery[49] oder icmpush[50].
- Portscanning: Beim Portscanning werden offene Ports auf einem Zielsystem detektiert. Eines der wohl bekanntesten Portscanning-Utilities ist nmap. Nmap ist ein sehr mächtiges Tool und erlaubt unter Anderem die Auswahl verschiedener Scanning-Techniken (wie z.B. TCP-Connect-Scan, TCP-SYN-Scan, XMAS-Scan, UDP-Scan, etc - genauere Details zu den verschiedenen Scanning-Techniken werden in der nmap-Dokumentation beschrieben[51]).

---

[44] http://www.exploit-db.com
[45] http://www.metasploit.com/framework/modules/
[46] Bei einem herkömmlichen Ping wird eine ICMP-Echo-Request-Nachricht an den Ziel-Host gesendet. Ist der Host erreichbar, antwortet er mit einer ICMP-Echo-Response-Nachricht. Für weitere Erklärungen, siehe http://de.wikipedia.org/wiki/Ping_%28Daten%C3%BCbertragung%29
[47] http://www.hping.org/
[48] http://fping.sourceforge.net/
[49] http://www.angio.net/security/
[50] http://linux.die.net/man/8/icmpush
[51] http://nmap.org/book/man-port-scanning-techniques.html

- OS-Fingerprinting: Angreifer interessieren sich neben offenen Ports insbesondere auch für die verwendeten Software- und Betriebssystemversionen, um so spezifischere Schwachstellen und entsprechende Exploits ausfindig zu machen. Ein Tool, welches die Detektion von Betriebssystem- und Softwareversionen erlaubt, ist wiederum nmap[52] [53].

Techniken für die Enumeration-Phase:

- Basic Banner-Grabbing: Banner-Grabbing ist die fundamentalste Enumerations-Technik. Banner-Grabbing beinhaltet im Prinzip nichts Anderes, als sich über eine Shell mit dem Zielsystem zu verbinden und den Output zu beobachten, welcher vom Zielsystem zurückgesendet wird. Diese Informationen (z.B. Software-Versionen, Betriebssystemversionen, etc.) können sehr interessant sein für einen Angreifer, um nach bekannten Schwachstellen und entsprechenden Exploits zu suchen. Diese Technik eignet sich für viele allgemein bekannte Services, welche auf Standardports antworten, wie z.B. HTTP - Port 80, SMTP - Port 25, FTP - Port 21, etc. Tools, welche sich für Banner-Grabbing bewährt haben, sind telnet und nc (netcat) [54].
- Enumeration bekannter Netzwerk-Services: Wie bereits weiter oben kurz angetönt, ist die Enumerations-Phase stark abhängig von den Resultaten aus der Scanning-Phase. Je nachdem, welche Ports auf dem Zielsystem offen sind, müssen unterschiedliche Techniken verwendet werden. So können zum Beispiel bei VPN-Systemen (häufig UDP-Port 500, aber auch TCP-Port 1723 etc. - siehe nächsten Punkt) spezielle Footprinting-Tools eingesetzt werden, mit welchen zum Beispiel schwache Cipher, die vom VPN-Server unterstützt werden, ausfindig gemacht werden können. Auch bei Webservern (Port 80, 443, 8080, etc.) können spezielle Tools eingesetzt werden, um den Webserver und insbesondere auch darauf ausgeführte Webapplikationen sehr detailliert auf entsprechende Schwachstellen zu untersuchen (z.B. w3af oder nikto - siehe "Schwachstellenscanner" weiter unten).
- Footprinting von VPN-Systemen: Viel zu oft wird angenommen, dass VPN-Systeme inhärent sicher sind, da VPN-Systeme offenbar die gesamte Kommunikation verschlüsseln und es somit für einen Angreifer unmöglich sein sollte, Daten mitzulesen. VPN-Systeme können aber sehr wohl angegriffen werden, wenn sie nicht sicher konfiguriert wurden. So kann es zum Beispiel sein, dass das VPN-System schwache Cipher unterstützt. Ein weiterer möglicher Angriffspunkt sind VPN-Systeme, welche den "Aggressive-Mode" mit "Pre-Shared-Secret-Authentifizierung" (PSK) unterstützen. Letztere Konfiguration ermöglicht Offline-Bruteforce-Attacken auf den gemeinsamen Schlüssel (shared secret). Die Firma NTA-Monitor[55] hat ein interessantes Paper über mögliche VPN-Schwachstellen veröffentlicht [Hills, 2005]. Ausserdem hat die Firma das Tool "ike-scan"[56] entwickelt, mit welchem VPN-Systeme detailliert untersucht werden können.

6.2.2 Ausgeführte Tests

Im Rahmen dieses Forschungsprojekts durften wir die Systeme von insgesamt drei Interviewpartnern aktiv austesten. Dabei sind folgende Techniken zur Anwendung gekommen:

- Portscanning
- OS-Fingerprinting
- Schwachstellen-Analyse-Tools
- Enumeration
- VPN-Footprinting

[52] http://nmap.org/book/man-os-detection.html
[53] http://nmap.org/book/man-version-detection.html
[54] http://netcat.sourceforge.net/
[55] http://www.nta-monitor.com/
[56] http://www.nta-monitor.com/tools/ike-scan/

6.2.3 Folgerungen

Folgende Punkte sind uns bei den Tests speziell aufgefallen:

- Bei den Webplattformen werden zum Teil nicht vertrauenswürdige Zertifikate eingesetzt. Dadurch erscheint im Browser beim Besuchen der Seite eine entsprechende Fehlermeldung. Das Problem dabei ist nun, dass legitime Benutzer, welche die Seite besuchen, nicht wissen können, ob sie tatsächlich mit dem "richtigen" Server kommunizieren, oder aber mit einem Server, welcher unter Kontrolle eines böswilligen Angreifers ist. Mit anderen Worten: Wenn das Zertifikat ungültig ist, kann die wahre Identität des Servers nicht bestätigt werden. Zertifikate sollten deshalb von einer öffentlich anerkannten "Certificate Authority" (CA)[57] signiert werden. Dadurch kann die Gültigkeit des Zertifikats vom Browser verifiziert werden, womit ein User schlussendlich die Garantie erhält, dass er tatsächlich mit dem gewünschten Server kommuniziert.
- Die getesteten VPN-Systeme unterstützen unter Anderem den DES-Cipher[58], wodurch ein Angreifer so genannte "Version-Downgrade-Attacken" durchführen kann. DES gilt seit einiger Zeit als unsicher und sollte deshalb nicht mehr unterstützt werden. Dass DES als unsicher gilt, liegt insbesondere auch an der viel zu kurzen Schlüssellänge von lediglich 56 bits. An Stelle von DES sollte heutzutage AES[59] mit einer Schlüssellänge von 128 bits oder 256 bits eingesetzt werden. Weitere Informationen bezüglich "sicheren Schlüssellängen" findet man auf www.keylength.com.
- Zum Teil werden veraltete Softwareversionen eingesetzt. Das Problem dabei ist, dass für veraltete Softwareversionen häufig publizierte Schwachstellen und entsprechende Exploits existieren. Solche Schwachstellen können also einfach von Angreifern ausgenutzt werden. Die Systeme sollten demnach stets mit entsprechenden Patches und Softwareupdates auf dem aktuellsten Stand gehalten werden.
- Bei einigen Servern wird HTTP-Authentifizierung eingesetzt. HTTP-Authentifizierung bringt insbesondere zwei Probleme mit sich: Erstens werden die Zugangsdaten (Credentials) im Klartext zum Server übermittelt. Mit einem Sniffer ist das Abhören der Zugangsdaten somit trivial. Das zweite Problem ist, dass HTTP-Authentifizierung anfällig auf Bruteforce-Attacken ist, d.h., dass man mit geeigneten Tools (z.B. Hydra[60], verschiedene Fuzzing-Tools, welche z.B. im Tool WebScarab[61] oder im Tool w3af enthalten sind) verschiedene Passwortmöglichkeiten durchprobieren kann. Da sehr häufig schwache Passwörter gewählt werden, kann sich ein Angreifer so einfach in das System hacken.
- Bei einigen Webservern ist Forced-Browsing möglich.
- Bei einigen Systemen wurden die Banner offensichtlich nicht gefälscht. Das Problem dabei ist, dass jeder potentielle Angreifer sehr einfach bestimmen kann, welche Software- und Betriebssystemversionen auf dem Zielsystem ausgeführt werden. Bei Kenntnis von entsprechenden Softwareversionen kann der Angreifer schliesslich nach publizierten Schwachstellen suchen. Eventuell sind sogar vorgefertigte Exploits vorhanden, mit denen das System sehr einfach kompromittiert werden kann. Die Kenntnis der Systemversionen erlaubt aber auch, im Internet nach Anleitungen für die entsprechenden Systeme zu suchen. Eventuell handelt es sich bei dem Zielsystem zum Beispiel um einen Router, bei welchem das Standardpasswort nicht deaktiviert wurde.
- Beim Portscanning gewisser Hosts fiel uns auf, dass einige Ports zwar nicht offen waren, aber auch nicht von der Firewall gefiltert wurden (während andere Ports allerdings gefiltert wurden). Diese Ports sind zwar auf dem Zielsystem nicht offen, aber trotzdem für einen Angreifer theoretisch erreichbar. Falls ein solcher Port also trotzdem vorübergehend geöffnet würde, wären dieser Port und der entsprechende Service sehr wohl für einen Angreifer sichtbar und somit auch angreifbar. Grundsätzlich sollten alle Services, die nicht absolut notwendig für den operativen Betrieb sind, auf dem Zielsystem deaktiviert und auch von der Firewall blockiert werden.

[57] http://en.wikipedia.org/wiki/Certificate_authority
[58] http://de.wikipedia.org/wiki/Data_Encryption_Standard
[59] http://de.wikipedia.org/wiki/Advanced_Encryption_Standard
[60] http://freeworld.thc.org/thc-hydra/
[61] http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project

- Bei einem Login-Portal einer Webapplikation wird der Benutzer bei Eingabe einer falschen User-ID entsprechend informiert ("Benutzername xy ist ungültig"). Diese Information ist für einen Angreifer natürlich sehr interessant, da er nun ohne weiteres verschiedene Benutzernamen ausprobieren kann und sofort eine Antwort erhält, ob der Benutzernamen gültig war oder nicht. Auf diese Art und Weise kann sich der Angreifer eine Liste gültiger User-IDs zusammenstellen, welche wiederum z.B. für einen Password-Cracking-Versuch verwendet werden kann.
- Auf einem Webserver sind die Standard-Management-Portale von phpMyAdmin und Joomla für beliebige Benutzer erreichbar. Das ist aus dem Grunde problematisch, da ein Angreifer nun ungehindert versuchen kann, mit Password-Guessing-Methoden in das System einzudringen. Solche Management-Portale sollten deshalb speziell geschützt werden. Eine Möglichkeit, um das zu erreichen, ist zum Beispiel die Standardbezeichnungen der entsprechenden Verzeichnisse abzuändern (zum Beispiel bei Joomla von "/administrator" nach "/Xy435zu"). Weitere Ratschläge zum Schutz von Standard-Management-Portalen werden in einem Paper der "YGN Ethical Hacker Group" beschrieben [YEHG, 2008].
- Auf gewissen Webservern sind nicht unbedingt notwendige HTTP-Methoden aktiviert, was ein Sicherheitsrisiko darstellen kann. Insbesondere die TRACE-Methode sollte deaktiviert werden. Die TRACE-Methode dient im Wesentlichen zum Debuggen von Webapplikationen. Mit einem Trace wird sozusagen einfach der Input, welcher vom Client an den Webserver gesendet wurde, zurück an den Client geschickt. So kann überprüft werden, wie der Server die gesendeten Daten "sieht". Auf diese Weise können zum Beispiel Proxy-Server ausfindig gemacht werden, die sich zwischen Absender und Webserver befinden, da die Proxy-Server die Daten auf bestimmte Weise abändern. Die TRACE-Methode kann aber auch für so genannte Cross-Site-Tracing-Attacken missbraucht werden[62] [Grossman, 2003]. Mit Cross-Site-Tracing ist es für einen Angreifer zum Beispiel möglich, Cookie-Daten auszulesen, obschon die Cookies mit der httpOnly-Option gesetzt wurden (Die httpOnly-Option macht es unmöglich, Cookie-Daten programmatisch mit Scripting-Sprachen wie zum Beispiel JavaScript auszulesen).
- Auf gewissen Webservern sind so genannte "PHP Eggs" aktiviert. Beispielsweise können mit einer URL der Form "http://www.xy.com/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000" die PHP-Credits ausgelesen werden. Angreifer können auf diese Art und Weise sofort erkennen, dass das Zielsystem PHP verwendet und somit weitere Untersuchungen anstellen, um eventuelle Schwachstellen zu eruieren.
- Ein Webserver zeigt bei Eingabe ungültiger Zeichen eine detaillierte MySQL-Fehlermeldung an, inklusive Tabellennamen. Solche Fehlermeldungen geben zu viele Informationen Preis und sollten deshalb durch generische Fehlermeldungen ersetzt werden.

6.3 Ausnutzen von softwarebedingten Systemschwachstellen

Nach der Scanning-und-Enumeration-Phase (siehe Kapitel 6.2) ist der Angreifer im Besitz einer Liste mit potentiellen Schwachstellen (sowohl öffentlich bekannte, dokumentierte Schwachstellen als auch unbekannte Schwachstellen) des Systems. Diese Informationen können nun dazu verwendet werden, das System teilweise oder komplett zu kompromittieren.

6.3.1 Techniken und Ressourcen

Hat der Angreifer erst einmal einige Schwachstellen im System ausfindig gemacht, gibt es mehrere Möglichkeiten, das System zu kompromittieren:

- Gewisse Schwachstellen, die auf unsichere Softwarekonfigurationen zurückzuführen sind, können einfach ausgenutzt werden. Beispiele dazu sind Standardpasswörter, schlecht geschützte Netzwerk-Shares, schlecht geschützte Webserver-Verzeichnisse, etc…

[62] http://de.wikipedia.org/wiki/Cross-Site_Tracing

- Auf einschlägigen Webseiten mit vorgefertigten Exploits[63] nach publizierten Exploits suchen, mit denen öffentlich bekannte Schwachstellen ausgenutzt werden können (so genannte Proof-of-Concept-Exploits).
- Eigenen Exploit-Code schreiben. Das ist in den meisten Fällen allerdings sehr aufwändig und schwierig und erfordert ausgeprägte Reverse-Engineering-Fähigkeiten. Ausserdem benötigt der Angreifer dazu eine debug-fähige Version der anzugreifenden Software.
- Webapplikationen können häufig relativ einfach "von Hand" kompromittiert werden. Allerdings wird dazu ein ausgeprägtes Know-How im Bereich Web-Applikationen vorausgesetzt.

6.3.2 Ausgeführte Tests

Die Prüfungen inwiefern bereits bestehende Sicherheitsmassnahmen zum Schutz gegen softwarebedingte Schwachstellen umgesetzt sind, stützen sich auf den Aussagen aus den Interviews ab. Ausserdem werden auch einige Erkenntnisse aus den Kapiteln 2 und 6.2 miteinbezogen.

6.3.3 Folgerungen

Folgende Punkte sind uns bei den Tests speziell aufgefallen:

- Auf gewissen Systemen der Interviewpartner wird veraltete Software mit öffentlich bekannten Schwachstellen eingesetzt (siehe Kapitel 6.2.3).
- Gewisse Interviewpartner haben angegeben, dass sie keinen Malwareschutz verwenden (oder zumindest nicht auf allen Systemen). Einem potentiellen Malwarebefall sind solche Systeme also schutzlos ausgeliefert. Mindestens ein Interviewpartner aktualisiert die Malwaredefinitionen ausserdem per USB-Stick. Die Verwendung von USB-Sticks ist insofern gefährlich, als dass sich bei unsachgemässer Verwendung Malware auf dem Stick einschleichen könnten, die sich dann auf den Systemen ausbreiten, bei denen der USB-Stick eingeschoben wird.
- Mindestens ein Interviewpartner hat erwähnt, dass seine Netze schlecht segmentiert wären. Malware kann sich so einfach ausbreiten. Solche Netze könnten ausserdem anfällig auf DoS-Attacken sein.
- Mindestens ein Interviewpartner hat erwähnt, dass keine Intrusion-Detection-Systeme (IDS) verwendet werden. Potentielle Angriffsversuche können dadurch nur mässig oder überhaupt nicht nachvollzogen werden.
- Gewisse Interviewpartner setzen Shared-Accounts ein, was robuste Accounting- und Logging-Mechanismen quasi verunmöglicht (es ist schwierig nachzuvollziehen, wer was wann gemacht hat, da sich der vermeintliche Übeltäter hinter dem Gruppenaccount sozusagen "verstecken" kann).
- Auf den Internet-Portalen der Interviewpartner ist zum Teil Forced-Browsing möglich (siehe Kapitel 6.2.3).
- Bei mindestens einem Interview-Partner werden die Betriebssysteme nicht auf den neuesten Stand gebracht (Softwarestand "eingefroren").
- Nicht alle Interviewpartner verwenden Personal-Firewalls.

6.4 Passwort-Cracking

Neben dem Ausnutzen von Softwareschwachstellen (siehe Kapitel 6.3) ist Password-Cracking ein weiteres Mittel für einen Angreifer, in ein System einzudringen. Password-Cracking kann aber auch dann eingesetzt werden, wenn gewisse Systeme bereits kompromittiert wurden, um weitere User-ID/Passwort-Kombinationen zu erhalten.

[63] Zum Beispiel http://www.exploit-db.com oder http://www.metasploit.com

6.4.1 Techniken und Ressourcen

Im Prinzip gibt es zwei unterschiedliche Arten von Techniken, die gesondert betrachtet werden können: Remote-Password-Guessing und Local-Password-Guessing.

Beim Remote-Password-Guessing wird versucht, über ein Netzwerk-Protokoll, welches den Benutzer vor Gewährung des Zugriffs authentifiziert (z.B. Telnet, SSH, FTP, HTTP-BasicAuth, Windows-File-und-Print-Sharing-Service (Shared Message Block - SMB), etc…), in das System einzudringen. Das grundlegende Vorgehen dabei ist simpel: Man probiert mehrere User-ID/Passwort-Kombinationen aus, bis man eine gültige Kombination gefunden hat. Die zu testenden User-IDs und Passwörter werden dabei aus einer vordefinierten Liste gelesen (Dictionary-Attack). Dieser Prozess kann durch entsprechende Tools oder eigene Scripts einfach automatisiert werden. Im Vergleich zum Local-Password-Guessing kann Remote-Password-Guessing von jedem beliebigen Angreifer durchgeführt werden, der das Zielsystem im Netzwerk "sehen" kann. Bezüglich Password-Cracking bieten solche Remote-Systeme also im Vergleich zu "lokalen Systemen" eine ungemein grössere Angriffsfläche. Deshalb ist es von grosser Bedeutung, dass Remote-Systeme gut geschützt werden. Folgende Tools, die Remote-Password-Guessing unterstützen, sollen an dieser Stelle kurz beleuchtet werden:

- THC Hydra: Hydra ist ein mächtiges Tool für UNIX-Plattformen, das mehr als 30 Netzwerk-Protokolle unterstützt (u.a. Telnet, FTP, HTTP, HTTPS, SMB und SSH). Die Tools Brutus[64] und Bruter[65] sind Alternativen für Windows-Plattformen. Brutus scheint allerdings seit 2001 nicht mehr aktiv gewartet zu werden.
- w3af: w3af (Web Application Attack and Audit Framework) ist ein Framework, um Webapplikationen auf Sicherheitsmängel zu testen. Das Tool bietet unter Anderem ein "bruteforce-Plugin", mit welchem Passwörter für ein bestimmtes Webportal erraten werden können.

Beim Local-Password-Guessing wird versucht, lokale Systempasswörter zu knacken. Bei modernen Betriebssystemen werden lokale Passwörter nicht im Klartext abgespeichert, sondern es wird zunächst ein Hash-Wert für das Passwort berechnet, welcher schliesslich im System hinterlegt wird. Hashes sind so genannte mathematische "Einweg-Funktionen", d.h. dass die Berechnung des Hash-Wertes für einen bestimmten Wert (z.B. ein Passwort) sehr einfach ist, die Umkehroperation (also vom Hashwert auf den ursprünglichen Wert zu schliessen) ist allerdings enorm schwierig und sollte nicht innerhalb "nützlicher Frist" möglich sein. Einige Betriebssysteme fügen den Passwörtern zusätzlich einen so genannten Salt[66] bei, bevor sie gehasht werden. Durch das Beimischen von Salts erhalten zwei identische Passwörter einen unterschiedlichen Hash-Wert, wodurch vorberechnete Dictionary-Attacken unmöglich werden (vorberechnete Dictionary-Attacken arbeiten mit Listen, welche vorberechnete Hash-Werte der zu testenden Passwörter enthalten. Mit vorberechneten Dictionary-Attacken kann das Cracken von Passwörtern massiv beschleunigt werden, da die Hash-Werte der zu testenden Passwörter nur noch mit den Hash-Werten, die lokal auf dem System abgespeichert sind, verglichen und nicht für jeden Durchgang neu berechnet werden müssen). Um also lokale Systempasswörter knacken zu können, muss der Angreifer zunächst irgendwie an die Hash-Werte herankommen. Danach beginnt der eigentliche Passwort-Cracking-Prozess. Im Vergleich zum Remote-Password-Guessing kann dieser Prozess offline durchgeführt werden, das heisst das Problem der Verzögerungen beim Remote-Password-Guessing, welches sich durch die Netzwerklatenz ergibt, ist beim Local-Password-Guessing nicht vorhanden. Die Geschwindigkeit des Cracking-Prozesses ist beim Local-Password-Guessing also nur durch die vorhandene Hardwareleistung beschränkt. Es können sowohl Bruteforce- als auch Dictionary-Attacken oder falls möglich gar vorberechnete Dictionary-Attacken verwendet werden (z.B. mit Rainbow-Tables[67]). Folgende Tools unterstützen das Knacken von lokalen Systempasswörtern:

[64] http://www.hoobie.net/brutus/
[65] http://sourceforge.net/projects/worawita/
[66] http://en.wikipedia.org/wiki/Salt_%28cryptography%29
[67] http://de.wikipedia.org/wiki/Rainbow_Table

- pwdump[68]: Mit pwdump können Windows-Hashes aus der lokalen SAM (Security Account Manager) extrahiert werden, um sie danach mit einem geeigneten Tool zu cracken.
- Cain[69]: Cain ist ein Tool für Windows-Plattformen, welches das Knacken unterschiedlichster Hash-Typen (u.a. Windows LM- und NTLM-Hashes, SHA-1, SHA-2, MD5, etc.) ermöglicht. Bruteforce-, Dictionary-Attacken, sowie Rainbowtables werden unterstützt. Cain kann auch Passwort-Hashes, die über das Netzwerk übertragen werden, abfangen und anschliessend cracken. Auch Passwörter, die im Klartext in einem Netzwerk übertragen werden, können einfach gefunden werden.
- John the Ripper[70]: John the Ripper wurde hauptsächlich zum Knacken schwacher UNIX-Passwörter entwickelt. Standardmässig werden aber auch Windows-LM-Hashes unterstützt. Ausserdem kann über Patches die Unterstützung weiterer Hash-Typen (zum Beispiel Windows-NTLM-Hashes) aktiviert werden. John the Ripper kennt im Wesentlichen drei verschiedene Cracking-Modi: Single-Crack, Wordlist und Incremental (optional können eigene Cracking-Modi geschrieben und verwendet werden). Im Single-Crack-Mode findet John Passwörter, die aus einer Kombination der User-ID und Informationen aus dem GECOS-Feld[71] bestehen. Beim Wordlist-Mode wird eine vordefinierte Liste mit möglichen Passwörtern durchprobiert. John wird standardmässig mit einer solchen Liste ausgeliefert, welche allerdings nicht allzu umfangreich ist. Der Incremental-Mode ist der mächtigste Mode von John: Hier werden verschiedene Buchstaben- und Zahlenkombinationen durchprobiert. Eine von Johns Stärken sind auch die vielen verschienen "Mangling-Rules", welche auszutestende Passwortmöglichkeiten geschickt abändern, um weitere Passwortmöglichkeiten zu generieren.

Für den Erfolg von Dictionary-Attacken ist die Verwendung einer geeigneten Wordlist entscheidend. Bereits vorgefertigte Wordlists findet man z.B. bei folgenden Quellen:

- http://www.packetstormsecurity.org/Crackers/wordlists/
- ftp://coast.cs.purdue.edu/pub/dict/
- CUPP (Common User Passwords Profiler)[72]: CUPP ist ein Tool, das bei der Vorbereitung von Dictionary-Attacken behilflich ist. Im "Interactive Mode" stellt das Programm verschiedenste Fragen über die Zielperson, deren Passwort geknackt werden soll, wie z.B. Beispiel Vorname, Name, Geburtstag, Arbeitsort, etc. Aus diesen Informationen erstellt das Programm schliesslich eine Wordlist mit einigen Passwort-Kandidaten. Es ist aber auch möglich, vorgefertigte Wordlists aus einem Repository herunterzuladen.

Ein exzellentes Dokument zum Thema Password-Cracking hat J. Dravet veröffentlicht [Dravet, 2008]. Das Dokument zeigt verschiedene Möglichkeiten und Tools auf, um Windows- und Linux-Passwörter zu knacken. Die einzelnen Tools und Techniken werden dabei in Form einer Anleitung detailliert beschrieben oder es wird auf entsprechende Literatur im Internet verwiesen.

6.4.2 Ausgeführte Tests

Die Prüfungen inwiefern bereits bestehende Sicherheitsmassnahmen zum Schutz gegen Password-Cracking umgesetzt sind, stützen sich auf den Aussagen aus den Interviews ab. Ausserdem werden auch einige Erkenntnisse aus den Kapiteln 2 und 6.2 miteinbezogen.

6.4.3 Folgerungen

Folgende Punkte sind uns bei den Tests speziell aufgefallen:

[68] http://en.wikipedia.org/wiki/Pwdump
[69] http://www.oxid.it/cain.html
[70] http://www.openwall.com/john/
[71] http://en.wikipedia.org/wiki/Gecos_field
[72] http://www.remote-exploit.org/codes_cupp.html/

- Bei einem VPN-System eines Interviewpartners wird Aggressive-Mode mit PSK-Auth unterstützt. Der PSK könnte also theoretisch mit einer Offline-Attacke geknackt werden (siehe Kapitel 6.2).
- Mindestens ein Webportal der Interviewpartner verwendet HTTP-BasicAuth ohne Lock-Out-Mechanismus. Ein Angreifer kann also beliebig Passwörter ausprobieren (siehe Kapitel 6.2).
- Bei einem Webportal eines Interviewpartners sind Standard-Management-Verzeichnisse (z.B. phpMyAdmin, Joomla-Admin-Bereich) für jedermann zugänglich. Ein externer Angreifer kann so mit einem Tool wie z.B. w3af verschiedene Passwortmöglichkeiten ausprobieren, um Zugriff zum Portal zu erlangen (siehe Kapitel 6.2).
- Gemäss Interviewprotokoll wird zum Teil noch Telnet eingesetzt. Telnet überträgt die Zugangsdaten und Nutzdaten im Klartext.
- Viele Remote-Login-Verfahren (z.B. über ISDN, VPN, etc.) basieren auf Benutzernamen und Passwörter gemäss Interviewprotokoll, so dass theoretisch Password-Guessing-Attacken angewendet werden könnten.

6.5 Eindringen in das System über unsicher konfigurierte Remote-Zugänge oder Wireless-Zugänge

Unsicher konfigurierte Remote-Zugänge können die gesamte Security-Infrastruktur einer Unternehmung aushebeln. Deshalb ist es wichtig, dass vorhandene Remote-Zugänge auf ein absolutes Minimum reduziert und gut gesichert werden.

6.5.1 Techniken und Ressourcen

Im Buch "Hacking Exposed" von Stuart McClure et al. [McClure, 2009] werden u.a. folgende Techniken erwähnt, um unsicher konfigurierte Remote- bzw. Wireless-Zugänge auszunutzen:

- War-Dialers: War-Dialers sind im Wesentlichen Tools, welche eine grosse Anzahl möglicher Telefonnummern austesten, gültige Verbindungen aufzeichnen, das System "auf der anderen Seite" zu identifizieren versuchen und optional Loginversuche starten, indem häufig verwendete User-ID/Passwort-Kombinationen ausprobiert werden.
- WEP/WPA-Hacking: Auch unsicher konfigurierte Wireless-Systeme können die Sicherheit eines Systems entscheidend gefährden. Hier stellen insbesondere so genannte Rogue-Access-Points (also Access-Points, die irgendein Mitarbeiter ohne Kenntnis der IT-/Führungs-Abteilung installiert hat, um so gewisse von der IT-Policy vorgegebene Einschränkungen zu umgehen) eine grosse Gefahr dar (siehe auch Kapitel 2).
- VPN-Hacking: Auch vermeintlich sichere VPN-Architekturen sind angreifbar, wenn sie unsicher konfiguriert wurden (siehe Kapitel 6.2.3).

6.5.2 Ausgeführte Tests

Die Prüfungen inwiefern bereits bestehende Sicherheitsmassnahmen zum Schutz gegen unsicher konfigurierte Remote-Zugänge umgesetzt sind, stützen sich auf den Aussagen aus den Interviews ab. Ausserdem werden auch einige Erkenntnisse aus den Kapiteln 2 und 6.2 miteinbezogen.

6.5.3 Folgerungen

Folgende Punkte sind uns bei den Tests speziell aufgefallen:

- Bei den ISDN-Zugängen basiert die Sicherheit gemäss Interviewpartner zum Teil auf Geheimhaltung der Einwahlnummer. Mit Hilfe von War-Dialers ist es theoretisch aber trotzdem möglich, entsprechende ISDN-Zugänge ausfindig zu machen. Die Geheimhaltung der Einwahlnummer bietet also wenig bis überhaupt keine Sicherheit.

- ISDN-Zugänge werden gemäss Interviewpartner z.T. nicht geloggt oder Log-Files werden nicht ausgewertet. Potentielle Angriffsversuche und verdächtige Vorgänge können so nicht detektiert werden.
- Gewisse VPN-Systeme der Interviewpartner untersützen schwache Cipher. Ausserdem wird bei einem System IKE-Aggressive-Mode mit PSK-Auth unterstützt (siehe Kapitel 6.2.3).
- Gewisse Interviewpartner verwenden gemäss Interviewprotokoll noch Telnet. Telnet bietet überhaupt keine Sicherheit, da alle Daten (auch Zugangsdaten) im Klartext übermittelt werden. Telnet sollte deshalb nicht länger verwendet werden.
- In Kapitel 2 haben wir gesehen, dass sich viele SCADA-Organisationen gar nicht bewusst sind, wie stark sie mit dem Internet verbunden sind. Tatsächlich existieren oft aber einige Einwahlleitungen (z.B. ISDN oder VPN) zu den Systemen. Gefährlich wird das insbesondere dann, wenn die Einwahlleitungen nicht genau protokolliert sind.

6.6 Sniffing

Die folgenden Erläuterungen über "Sniffer" stützen sich im Wesentlichen auf das Buch "Hacking Exposed" von Stuart McClure et al. [McClure, 2009].

So genannte Netzwerk-Sniffer sind ursprünglich aus der Notwendigkeit entstanden, Netzwerkprobleme zu analysieren. Sniffer zeichnen im Wesentlichen den Netzwerkverkehr auf und bieten verschiedene Möglichkeiten an, den Netzwerkverkehr zu analysieren.

Wie die meisten mächtigen Tools, die von Netzwerkadministratoren verwendet werden, können auch Sniffer für arglistige Zwecke missbraucht werden. Man kann sich vorstellen, dass innerhalb eines Netzwerkes Unmengen an sensitiven Daten herumschwirren, unter Anderem Benutzernamen und Passwörter, sensitive E-Mail-Nachrichten, sensitive Dateien, etc. Werden diese Daten unverschlüsselt übertragen, können sie sehr einfach mit Hilfe eines Sniffers mitgelesen werden.

Sniffer zeichnen den gesamten Netzwerkverkehr auf, der sich "in Reichweite" der Maschine (innerhalb der lokalen Kollisionsdomäne[73]) befindet, auf welcher der Sniffer läuft. Zu diesem Zweck arbeiten Sniffer mit der Netzwerk-Karte (Network Interface Card - NIC) zusammen. Da NICs normalerweise Pakete, die nicht direkt an sie oder an die Broadcastadresse adressiert sind, verwerfen, müssen die NICs in einen speziellen Modus, den so genannten *Promiscuous Mode*[74], geschaltet werden, um jeglichen Netzwerkverkehr innerhalb der lokalen Kollisionsdomäne mitzulesen. Netzwerkverkehr ausserhalb der lokalen Kollisionsdomäne (z.B. in einem geswitchten LAN - allgemein bei Devices, die das Netzwerk segmentieren) kann nicht ohne weiteres abgehört werden. Allerdings kann z.B. mit ARP-Spoofing[75] der Verkehr so umgeleitet werden, dass er trotzdem wieder beim Host des Angreifers vorbeiführt, wodurch das Abhören des Verkehrs in einem geswitchten Netzwerk auch relativ einfach möglich ist.

Die Hauptgefahr geht hier sicherlich von den internen Mitarbeitern aus, da diese sehr einfach einen Sniffer in das lokale Netz schalten können. Für externe Angreifer ist es bereits schwieriger, einen Sniffer "zielgerecht" einzusetzen. Hat ein Hacker allerdings ein gewisses System im Zielnetz bereits kompromittiert, kann er durchaus einen Sniffer auf das entsprechende System hochladen und von dort aus den lokalen Verkehr abhören, um entweder sensitive Daten zu stehlen oder weitere Systeme zu kompromittieren.

6.6.1 Techniken und Ressourcen

Es gibt mehrere unterschiedliche Sniffer-Tools. An dieser Stelle sollen zwei Tools kurz vorgestellt werden:

[73] http://de.wikipedia.org/wiki/Kollisionsdom%C3%A4ne
[74] http://de.wikipedia.org/wiki/Promiscuous_Mode
[75] http://de.wikipedia.org/wiki/ARP-Spoofing

- Wireshark[76]: Wireshark ist wohl eines der bekanntesten Netzwerk-Analyse-Tools. Wireshark erlaubt die detaillierte Analyse von mehreren bekannten Netzwerk-Protokollen. Die abgefangenen Netzwerkdaten können dabei offline in einem GUI (Graphical-User-Interface) analysiert werden. Wireshark bietet ausserdem weitere Features, welche auf der Programm-Website erläutert werden.
- Cain: Cain ist nicht ein klassisches Sniffing-Tool an sich, sondern bietet viel mehr verschiedene Möglichkeiten, um Passwörter unterschiedlicher Art zu knacken. Das Tool wurde für Windows-Plattformen konzipiert. Cain hört den Netzwerkverkehr ab und extrahiert automatisch Passwörter im Klartext, sowie unterschiedliche Passwort-Hashes. Passwort-Hashes können anschliessend mit Bruteforce- oder Dictionary-Attacken geknackt werden. Cain erlaubt auch das Abhören des Verkehrs in einem geswitchten Netzwerk mit Hilfe von ARP-Spoofing.

6.6.2 Ausgeführte Tests

Die Prüfungen inwiefern bereits bestehende Sicherheitsmassnahmen zum Schutz gegen Sniffer umgesetzt sind, stützen sich auf den Aussagen aus den Interviews ab. Ausserdem werden auch einige Erkenntnisse aus den Kapiteln 2 und 6.2 miteinbezogen.

6.6.3 Folgerungen

Folgende Punkte sind uns bei den Tests speziell aufgefallen:

- Mindestens ein Interviewpartner hat angegeben, dass der Verkehr nicht explizit verschlüsselt wird.
- Bei den Interviewpartnern sind durchaus sensitive Daten vorhanden, insbesondere Bild- und Videodaten. Einige dieser Bild- und Videodaten haben zwar schlechte Qualität, so dass reines Abhören an sich nicht in allen Fällen eine Bedrohung darstellt (einige Interviewpartner verfügen durchaus auch über vertrauliche Daten, die nicht für jedermann einsehbar sein sollten). Allerdings gibt es auch Daten, die "korrekt" am Ziel ankommen sollten, d.h. die Integrität muss gewährleistet sein. Falls also Daten mit einem Sniffer abgehört und zu einem späteren Zeitpunkt wieder injiziert werden könnten, würde das durchaus ein gewisses Sicherheitsrisiko darstellen. Von mindestens einem Interviewpartner wurde der Ausfall der Videobilder sogar als kritisch bezeichnet.
- Gewisse Interviewpartner setzen noch Telnet ein. Telnet überträgt die Daten im Klartext, wodurch die Daten theoretisch sehr einfach mit einem Sniffer abgehört werden könnten.
- Bei gewissen Webportalen der Interviewpartner wird HTTP-Authentifizierung eingesetzt (HTTP-BasicAuth - siehe Kapitel 6.2.3). Bei reiner HTTP-Authentifizierung werden die Zugangsdaten im Klartext übermittelt, wodurch die Daten theoretisch sehr einfach mit einem Sniffer abgehört werden könnten.
- In Kapitel 2 haben wir gesehen, dass in SCADA-Netzwerken oft gar keine kryptographischen Protokolle eingesetzt werden, d.h. die Daten im Netzwerk werden nicht verschlüsselt. Oft werden auch proprietäre Protokolle mit schwachen Authentifizierungsmechanismen eingesetzt. Proprietäre Protokolle werden auch von gewissen Interviewpartnern eingesetzt.
- Bei einem VPN-System eines Interviewpartners wurden schwache Cipher unterstützt (siehe Kapitel 6.2.3). Die Daten könnten also theoretisch abgehört und eventuell entschlüsselt werden. Ausserdem wird bei den VPN-Systemen Aggressive-Mode mit PSK-Authentifizierung unterstützt. Letztere Konfiguration ist anfällig auf Offline-Brute-Force-Attacken auf das PSK.
- Bei einem System eines Interviewpartners ist geplant, die Daten u.a. mittels GSM zu übermitteln. GSM gilt mittlerweile als unsicher und sollte nicht ohne zusätzliche Si-

[76] http://www.wireshark.org/

cherheitsmechanismen verwendet werden. (siehe auch http://www.gsm-security.net/gsm-security-papers.shtml)

6.7 Social Engineering

Im Kontext der IT-Sicherheit ist das Ziel von Social Engineering-Angriffen Zugangsdaten zu Infrastrukturen und Systemen zu erhalten, als Vorbereitung für das Eindringen in Netzwerke, Systeme oder Gebäude.

Social Engineering ist eine der gefährlichsten Angriffsmethoden, da sie die Schwachstelle Mensch ausnutzt. Von Social Engineering spricht man, wenn sich ein Angreifer durch Ausnutzen von menschlichen Schwächen (oder Stärken) Zugang zu unbefugten Informationen verschafft[77]. Social Engineering ist eine sehr effektive Methode um an sensible oder geschützte Daten zu gelangen. Angreifer nutzen dabei geschickt menschliche Reaktionen oder Eigenschaften aus, wie beispielsweise Dankbarkeit, Hilfsbereitschaft, Stolz, Habgier, Unsicherheit oder Konfliktvermeidung

Ein Social-Engineering Angriff erfolgt in vier Phasen nach dem Social Engineering Angriffszyklus (Engl. Social Engineering Attack Cycle[78]):

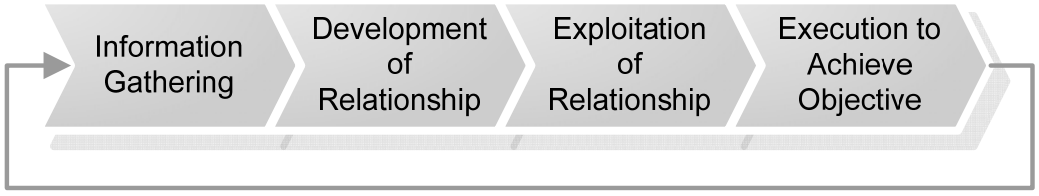


Abbildung 12: Social Engineering Angriffszyklus (Quelle Gartner)

Die erste Phase hat zum Ziel möglichst viele Hintergrundinformationen über das Angriffsziel zu erhalten um eine Beziehung mit dem Angriffsziel oder einer Person in der Umgebung aufzubauen. Dies können zum Beispiel sein: Telefonnummer, AHV-Nummer, Geburtsdatum, Organigramm- und Stellenbeschreibung, usw.

In der zweiten Phase wird die Beziehung zum Angriffsziel aufgebaut. Es liegt in der menschlichen Natur relativ unkritisch zu sein. Dies wird durch die Angreifer ausgenutzt um eine Beziehung aufzubauen. Je nachdem reicht dafür ein einmaliger Telefonanruf oder der Aufbau erstreckt sich über mehrere Wochen hinaus. Der Angreifer setzt sich damit in eine Vertrauensposition, die er dann ausnutzen kann.

In der dritten Phase wird die Vertrauensposition ausgenutzt um vom Angriffsziel vertrauliche Informationen (zum Beispiel Zugangsdaten zu Systemen) zu erhalten oder vom Angriffsziel Aktionen durchführen zu lassen (zum Beispiel Erstellen eines Accounts). Diese Informationen oder Aktivitäten können das Endziel des Angriffs sein oder können verwendet werden um eine nächste Angriffsstufe auszulösen.

Die vierte Phase ist dann die Ausführung des Angriffs um das Endziel zu erreichen. Üblicherweise umfasst ein Angriff mehrere dieser Angriffszyklen kombiniert mit traditionellen Angriffsmethoden.

6.7.1 Techniken und Ressourcen

Es gibt zahlreiche Methoden, die von einem Social Engineering Angreifer für eine Attacke angewendet werden können. Diese werden in verschiedenen Bereichen des Angriffszyklus eingesetzt. Im Folgenden werden die üblichen Methoden aufgeführt:

[77] http://www.verfassungsschutz.brandenburg.de
[78] http://www.gartner.com/gc/webletter/security/issue1/index.html

- Berufung auf Autorität: Der Angreifer gibt vor, ein IT-Mitarbeiter (oder ein anderer Kollege) zu sein und fragt den Anwender nach seinem Passwort oder anderen sensiblen Informationen.
- Hilfsbereitschaft: Menschen haben die Eigenschaft einander zu helfen, zum Beispiel Benutzer, die ihr Passwort vergessen haben. Mit ein wenig Geschick können Angreifer genügend Informationen über einen echten Benutzer sammeln um dann bei der Hotline ein neues Passwort anzufordern. Der Angreifer ruft bei der Hotline an und behauptet, ein Mitarbeiter oder Lieferant zu sein, der sein Passwort vergessen hat und darum bittet, dass sein Passwort auf einen definierten Wert zurückgesetzt wird.
- Identität stehlen: Diese Methode wird heutzutage immer beliebter. Viele Eigenschaften, die unsere Identität nachweisen sind einfach erhältlich. Es ist nicht unüblich für Angreifer genügend Informationen zu erhalten um eine Identität zu stehlen und damit neue Konten oder System-Accounts zu generieren oder auf bestehende Accounts zuzugreifen.
- Wartung und Support: Eine der einfachsten Methoden sich Zugang zu einer Organisation zu verschaffen, ist dort zu arbeiten. Werden neue Mitarbeiter noch beachtet, so gibt es nur wenige Organisationen, die dem Reinigungspersonal oder Serviceuternehmen Beachtung schenken. Diese haben jedoch meistens vollen Zugang zu den Räumlichkeiten.
- Schadsoftware: Viele der gängigen Malware wie zum Beispiel "Melissa" oder "I love you" werden heute über Social Engineering Attacken per E-Mail verbreitet. Diese Malware richtet ihren Schaden nur durch eine bewusste Aktion des Benutzers an. Die Benutzer werden dadurch getäuscht, dass entweder der Inhalt der E-Mail oder der Absender interessant oder vertrauenswürdig erscheint.
- Reverse Social Engineering: Der Angreifer vertauscht bewusst die Rollen. Dabei wird zuerst gezielt Sabotage betrieben (zum Beispiel an einem Arbeitsplatz eines Mitarbeiters). Kurz darauf bietet sich der Angreifer als helfende Person an und gibt vor, das Problem zu lösen. In dieser Phase der Betroffener-Helfer-Beziehung nutzt er das Vertrauen aus und versucht so, an Informationen heranzukommen.

6.7.2 Ausgeführte Tests

Die Prüfungen inwiefern bereits bestehende Sicherheitsmassnahmen zum Schutz gegen Social Engineering umgesetzt sind, stützen sich auf den Aussagen aus den Interviews ab.

6.7.3 Folgerungen

An den Interviews mit den Gebietseinheiten wurden folgende Eigenschaften, die beim Thema Social Engineering eine Rolle spielen, festgestellt:

- Der Zugang von Fremdpersonal zu den Systemen ist für Wartungsarbeiten die Regel. Allerdings ist zum heutigen Zeitpunkt die Anzahl der Lieferanten noch beschränkt. Die Mitarbeiter der Lieferanten, die an den Systemen eingreifen, sind dem Personal der Gebietseinheiten persönlich bekannt. Allerdings wird sich die Situation mit dem Ausbau der Vernetzung verändern, es werden weitere Lieferanten mit neuen Beteiligten dazustossen. Die Übersicht wird vermutlich in Zukunft nicht mehr so einfach bleiben wie heute.
- Ziel des Verkehrsmanagements ist ein reibungsloser und sicherer Verkehrsfluss auf dem Strassennetz zu gewährleisten. Mit dem Bestreben das Ziel zu erreichen agieren die Mitarbeiter grundsätzlich sehr aktiv und hilfsbereit. Dies hat sich auch im Verlauf des Forschgunsprojekts gezeigt, wo die Forschungsstelle diverse Kontakte gepflegt hat. Es ist nicht auszuschliessen, dass durch diese Hilfsbereitschaft bei anderen Anfragen Informationen unbewusst abgegeben werden, ohne gründliche Überprüfung der Identität der Gegenpartei.
- Damit die Aufgaben im Bereich der Verkehrstelematik wahrgenommen werden können sind diese auf die Verarbeitung von Echtzeitinformationen angewiesen. Wie das Personal auf eine etwaige vorgestäuschte "Stresssituation" (z.B. vorgetäuschter Anruf der IT oder eines Lieferanten mit Drohung eines Systemausfalls) reagiert ist nicht vorhersehbar.

- Weiterhin ist die strenge Einhaltung der Sicherheitspolicies die Voraussetzung um auch Social Engineering Angriffe abzuwehren.

6.8 Fehlmanipulation durch berechtigte Benutzer

Die Sicherheitsmechanismen, die in den Verkehrstelematiksystemen eingebaut sind verhindern das Auftreten einer Menge vom vorhersehbaren Fehler. Eine vollständige Abdeckung aller möglichen Fehler kann dadurch aber nicht garantiert werden. Die Vermeidung des Auftretens weiterer Fehler setzt eine entsprechende Ausbildung der Anwender voraus. Trotzdem gibt es immer wieder kritische Situationen in denen Fehler aufgrund von Fehlmanipulationen von berechtigten Benutzern auftreten.

6.8.1 Techniken und Ressourcen

Eine Fehlmanipulation liegt vor, wenn durch einen menschlichen Eingriff eines berechtigten Benutzers ein System in einen unerwarteten Zustand gerät und dadurch die Systemsicherheit in Frage gestellt wird. Im Zusammenhang mit Verkehrstelematiksystemen sind die Ursachen von Fehlmanipulationen:

- Fehler im laufenden Betrieb in der Bedienung von Leitsystemen: dies kann zum Beispiel der Fall sein, wenn eine neue Software-Version ohne entsprechende Einweisung der Benutzer eingeführt wird oder durch Unachtsamkeit des Benutzers.
- Das unachtsame Einstecken "fremder Komponenten" an den eigenen Systemen. Dies betrifft insbesondere die Verwendung von USB-Sticks[79] oder Notebooks, um Daten in das Netzwerk einzuspielen. Diese Komponenten können vorab, getrennt vom Betriebsleitsystem oder von der BSA, mit Malware infiziert werden, ohne dass der Benutzer dies bemerkt.
- Fehler bei Wartungsarbeiten am System die durch unsachgemässe Installation von neuen Systemkomponenten auftreten können. Dies betrifft sowohl die Aktualisierung von Hardware- als auch von Softwarekomponenten wie zum Beispiel Betriebssystem-Patches, Antimalwaresoftware, Netzwerkkonfigurationen, Fachapplikationen oder neue Konfigurationen davon. Wartungsarbeiten sind besonders kritische Aktivitäten, da diese in vielen Fällen eine hohe Berechtigungsstufe verlangen und dadurch der Zugriff auf sensible Systembereiche gegeben ist. Bekannte Fehler bei Wartungsarbeiten sind die Nichteinhaltung der Reihenfolge bei der Software-Installation grösserer Pakete (Aktualisierung Betriebsystem muss vor Aktualisierung Fachapplikation erfolgen), die Nichtbeachtung der notwendigen Hardware- und Software-Voraussetzungen vor der Installation oder fehlende Abklärungen in Bezug auf die Gesamtsystemkonfiguration.

6.8.2 Ausgeführte Tests

Die Prüfungen, inwiefern bereits bestehende Sicherheitsmassnahmen zum Schutz gegen Fehlmanipulationen berechtigter Benutzer umgesetzt sind, stützen sich auf den Aussagen aus den Interviews ab.

6.8.3 Folgerungen

Folgende Punkte sind bei den Interviews besonders aufgefallen:

- Eine der wesentlichen Schwachstellen betrifft den ganzen Bereich der Dokumentation. Eine vollständige, aktuelle und richtige Dokumentation stellt die Grundlage dar, damit das Wissen den Benutzern vermittelt werden kann. Besonders zu erwähnen sind die fehlenden Richtlinien (Security-Policies), Handbücher, Anweisungen und Prozessbeschreibungen.
- Der Bereich der Wartungsarbeiten ist insofern kritisch, als die zur Verfügung stehenden Umgebungen in der Regel keine Testsysteme umfassen. Beim Einspielen neuer Software wird auf den Lieferanten vertraut. Systematische Beschreibungen der Pro-

[79] http://bazonline.ch/ausland/asien-und-ozeanien/Neuartiges-Computervirus-soll-im-Iran-Atommeiler-beschaedigt-haben-/story/18099206

zesse für die Wartungsarbeiten sind nicht vorhanden. Teilweise werden auch Ad-Hoc Anpassungen vor Ort, ohne vorherige Tests auf einem Testsystem vorgenommen.

- Sind Fehlmanipulationen einmal erfolgt, stehen keine systematischen Notfallpläne zur Verfügung. Diese sollten die Prozesse (Aktivitäten, Anweisungen, Sofortmassnahmen, Verantwortliche) für die Wiederherstellung der Systeme in einen operativen Betrieb beschreiben. Erschwerend bei einem Notfall ist die Tatsache, dass zum Teil keine systematischen Backups der Systeme in den Zentralen zur Verfügung stehen oder diese sogar verteilt bei den Lieferanten vorgehalten werden.
- Die Ausbildung der Benutzer erfolgt weitgehend direkt am Arbeitsplatz. Es wird das "Learning by Doing" Prinzip angewendet. Dies hat auch zur Folge, dass keine systematische Einführung in die kritischen Bereiche erfolgt. Die Schwerpunkte liegen in den Abläufen unter normalen Bedingungen und nicht in den Abläufen bei Fehlersituationen.
- Die Zugangsrechte zu den Systemen werden i.d.R. über Gruppen verteilt und auch gepflegt. Dies entspricht einer üblichen, adäquaten Lösung.
- Für gewisse Wartungsarbeiten werden USB-Sticks eingesetzt. Die Gefahren, die sich beim Umgang mit diesem Medium verbergen, sind den Benutzern häufig nicht umfänglich bekannt.

6.9 Unmotivierte oder verärgerte Mitarbeiter

Der Faktor Mensch ist und bleibt ein schwaches Glied, wenn es um IT-Sicherheit geht. Umsomehr stellen unmotivierte oder verärgerte Mitarbeiter eine Gefahr für die Sicherheit von Verkehrstelematiksystemen dar. Diese Personen verfügen über sehr gute Kenntnisse der Systemumgebung und auch deren Schwachstellen und können somit dort angreifen, wo ein hohes Schadenspotential vorhanden ist.

6.9.1 Techniken und Ressourcen

Die Angriffe, die ein unmotivierter oder verärgerter Mitarbeiter durchführen kann, sind breit gefächert. Voraussetzung für einen erfolgreichen Angriff ist der Besitz der notwendigen Zugangsberechtigungen in ein System. Ist diese Voraussetzung gegeben, stehen folgende Techniken und Ressourcen zur Verfügung:

- Diebstahl von sensiblen Daten: dieser Aspekt gewinnt heutzutage immer mehr an Bedeutung. Eines der bekanntesten Beispiele ist der Datendiebstahl von Schweizer Bankverbindungen von Steuersündern aus Deutschland[80]. Im Bereich der Verkehrstelematik sind Zugangsdaten zu Systemen, Videos oder Daten von AGK-Systemen sensibel und somit für potentielle Angreifer wertvoll.
- Datenkorruption: bei der Datenkorruption werden in den Systemen Daten verfälscht mit der Absicht, dass darauf Fehlentscheide erfolgen. Ein Angreifer könnte zum Beispiel reale Ereignismeldungen verfälschen mit der Absicht, ein Verkehrschaos zu produzieren oder korrupte Messwerte in ein System einschleusen mit dem Ziel einer Leitzentrale bewusst falsche Grundlagen zur Verfügung zu stellen.
- Sensible Daten löschen: die in den Verkehrstelematiksystemen verfügbaren Videobilder oder die Messwerte von AGK-Anlagen sind als sensibel zu betrachten. Ein Angreifer, mit entsprechenden Rechten, kann diese Daten unwiderruflich löschen und somit die für die Fachprozesse notwendige Beweispflicht beeinträchtigen.
- Systeme umkonfigurieren: bei der Umkonfiguration von Systemen werden Leit- oder Steuerfunktionen ausgelöst so dass das das Verkehrsmanagement "fremdgesteuert" wird und die Leitzentralen die Situation nicht mehr beherrschen. Als Beispiele können genannt werden: Sperren aller Spuren, sehr niedrige Geschwindigkeitsbeschränkung auf Hochleistungsstrassen an Spitzenzeiten, Anzeigen von falschen Informationen auf WTAs, usw.
- Systeme mit Schadsoftware (Malware) "infizieren": das Infizieren von Systemen mit Schadsoftware wird sowohl für die Übernahme der Herrschaft über Systeme oder Teile davon als auch für die Störung von einzelnen Komponenten eingesetzt. Die willentliche Infizierung durch einen Mitarbeiter stellt eine hohe Gefahr dar, da je nach Sys-

[80] http://www.spiegel.de/netzwelt/web/0,1518,722327,00.html

temkenntnissen und Fähigkeiten des Mitarbeiters - ein Mitarbeiter kann in diesem Falle auch ein Lieferant sein - die Infizierung nicht sofort detektiert werden kann.

6.9.2 Ausgeführte Tests

Die Prüfungen inwiefern bereits bestehende Sicherheitsmassnahmen zum Schutz gegen unmotivierte oder verärgerte Mitarbeiter umgesetzt sind, stützen sich auf den Aussagen aus den Interviews ab.

6.9.3 Folgerungen

Folgende Punkte sind bei den Interviews besonders aufgefallen:

- Die Zugriffsrechte werden auf Gruppenebene vergeben und gepflegt. Dies entspricht einer sinnvollen Regelung.
- Die Verfolgung der Aktivitäten, insbesondere bei den Lieferanten, ist nicht gewährleistet. Dadurch, dass für die Lieferanten keine "persönlichen" Accounts definiert sind kann nicht zurückverfolgt werden wer hat was wann gemacht. Dies ist für die Nachvollziehbarkeit der Aktivitäten ungenügend.
- Die Zutrittskontrollen zu den einzelnen Systemen sind nicht einheitlich geregelt. Zum heutigen Zeitpunkt wird nicht systematisch aufgezeichnet wer sich wie lange wo aufgehalten hat.
- Generell fehlt eine systematische Verwaltung der Lieferanten und der Wartungszugänge (z.B. ISDN), was eine Übersicht über die Zugangsrechte zu den Systemen erschwert.

6.10 Physische Attacken/Unfälle

Bei physischen Attacken versucht ein Angreifer sich vor Ort Zugang zu einer oder mehrerer BSA zu verschaffen. Von dort aus wird versucht, einen möglichst grossen Schaden anzurichten. Der Schaden kann sich einerseits auf die physischen Ressourcen wie zum Beispiel die Gebäude, das Kommunikationsnetz, die Rechneranlagen der Leitzentrale oder die Sensoren und Aktoren auf der Feldebene beziehen. Andererseits kann eine physische Attacke auch dazu dienen vertrauliche Informationen zu sammeln: Zugangsdaten, Systemkonfigurationen, Telefonverzeichnisse oder andere vertrauliche Dokumente, welche offen zugänglich sind. Diese dienen als Grundlage für weitere Angriffe.

Neben physischen Attacken können auch Unfälle zur Korrumpierung von Systemen führen. Unfälle sind ausserordentliche Ereignisse, die zum Ausfall oder zur Zerstörung der Anlagen führen. Unfälle können menschlicher (z.B. eine Fehlmanipulation) oder technischer Natur (Stromausfall) sein.

6.10.1 Techniken und Ressourcen

Die Techniken und Ressourcen für die physischen Attacken/Unfälle sind in den Angriffsvektoren im Kapitel 5.3.10 aufgeführt. Es geht in der Regel um die physische Zerstörung von Anlagen mittels Feuer, Wasser, Gas oder mit Gewalt. Bei physischen Attacken kann es auch vorkommen, dass die Anlagen "nur" ausser Betrieb gesetzt werden in dem diese abgestellt, vom Kommunikationsnetz getrennt oder manipuliert werden. Bei elektronisch gesicherten Zugängen (wie Badge-Systeme) versucht ein Angreifer, sich entweder einen entsprechenden Schlüssel zu beschaffen oder aber sich Zugang über andere Wege (zum Beispiel gleichzeitiger Eintritt mit anderen Mitarbeitern) zu schaffen.

6.10.2 Ausgeführte Tests

Die Prüfungen inwiefern bereits bestehende Sicherheitsmassnahmen zum Schutz gegen physische Attacken umgesetzt sind, stützen sich auf den Aussagen aus den Interviews ab. Es wurden keine weiteren Tests durchgeführt.

6.10.3 Folgerungen

Folgende Punkte sind bei den Interviews besonders aufgefallen:

- Die Standorte der BSA und deren Zugang sind zur Zeit unterschiedlich gesichert. In der Regel stehen die Systeme in abgeschlossenen Räumen. Der Zugang ist dann über ein dokumentiertes Schliesskonzept geregelt. In Einzelfällen existieren Badge-Systeme und Videoüberwachung, die zusätzlich eine Zugangsregistrierung beim Eingang vornehmen. Einzelne Standorte besitzen einen höheren Sicherheitsstandard, da diese im Rechenzentrum bei der Polizei angesiedelt sind.
- Der Zugang für externe Personen erfolgt über vorherige Anmeldung. Externe werden dann persönlich an die Arbeitsstationen begleitet. Eine Überwachung der durchgeführten Arbeiten erfolgt nicht. Der Zugang für externe beruht jedoch nicht auf einem sehr hohen Sicherheitsstandard: keine Registrierung des Ein-/Ausgangs, keine Überprüfung der Identität, usw.
- Die Anlagen auf der Strecke sind in der Regel Zugriffsgesichert. Die Zugänge zu den Räumlichkeiten und Schaltschränken sind schlüsselgesichert. Es erfolgt jedoch keine Registrierung des Zugangs.
- Für den Schutz der Anlagen gegen Feuer und Wasser werden unterschiedliche Systeme eingesetzt: Brandabschottungen, Rauchmelder, Sprinkler, Gaslöschanlagen. Die Sprinkleranlagen entsprechen nicht mehr dem aktuellen Standard und können beim Einsatz erheblichen Schaden an IT-Systemen anrichten.
- In einigen BSA sind die Systeme redundant ausgelegt und stehen an unterschiedlichen Standorten.

6.11 Praktische Untersuchung eines Servicelaptops

Im Rahmen dieses Forschungsprojekts wollten wir auch untersuchen, wie sicher dass die Servicelaptops sind, welche von gewissen Interviewpartnern im Piket-Dienst eingesetzt werden. Dabei interessierten wir uns insbesondere für folgende Aspekte:

- Welche Möglichkeiten ergeben sich für einen externen Angreifer, der einen Servicelaptop stiehlt? - Dazu gehören u.a. folgende Punkte:
  - Können sensitive Daten eingesehen werden?
  - Kann man sich an das Betriebssystem anmelden?
  - Kann man sich über einen Remotezugang in das Firmennetzwerk einloggen?
- Kann ein vertrauenswürdiger Benutzer durch Fehlmanipulation die Systeme gefährden oder Daten korrumpieren? - Dazu gehören u.a. folgende Punkte:
  - Welche Rechte hat ein eingeloggter Benutzer?
  - Auf welche Funktionen hat ein eingeloggter Benutzer Zugriff?
  - Welche Sicherheitsmassnahmen sind auf den Laptops installiert und wie aktuell ist die entsprechende Software? (Betriebssystemversionen, Personal Firewall, Antimalwaresoftware, etc.)

Um uns ein genaueres Bild über die obigen Punkte machen zu können, haben wir einen Service-Laptop eines Interviewpartners konkret auf Schwachstellen untersucht. Es handelte sich dabei um einen IBM Thinkpad T43 2668-C16. Der Interviewpartner verwendet ausserdem für die Anmeldung am Laptop ein spezielles USB-Dongle-System. Ohne die entsprechende Hardware sollte der Laptop gemäss Interviewpartner gar nicht erst aufstarten. Für den Test haben wir weder den USB-Dongle, noch das BIOS-Passwort erhalten. Wir konnten auf diese Weise also relativ gut nachvollziehen, welche Möglichkeiten einem externen Angreiber beim Diebstahl eines solchen Laptops offen stehen.

6.11.1 Techniken und Ressourcen

In diesem Unterkapitel sollen einige Techniken beleuchtet werden, welche von externen Angreifern, die einen Laptop gestohlen haben, eingesetzt werden können, um das Gerät zu übernehmen.

Wurde der Laptop mit einem Power-On-Passwort konfiguriert, muss dieses zunächst irgendwie umgangen werden, um überhaupt von einem Device (z.B. CD-ROM, USB-Stick, etc.) booten und somit weitere Angriffe starten zu können. Power-On-Passwörter werden im BIOS konfiguriert. Diesen Mechanismus zu umgehen, ist gerade bei Laptops nicht immer ganz einfach, wie ein Artikel der Firma Password Crackers bestätigt[81]. So werden bei Laptops die BIOS-Passwörter oft in einem speziellen Security-Chip gespeichert. Es ist somit nutzlos, die CMOS-Batterie für eine gewisse Zeit lang auszubauen, da die BIOS-Passwörter so nicht verloren gehen. Es existieren auch keine "einfachen" Password-Recovery-Tools, mit welchen das Passwort ausgelesen werden könnte. Trotzdem scheint es immer wieder Wege zu geben, um BIOS-Passwörter auch bei Laptops zurücksetzen zu können. Die Firma Password Crackers selbst bietet eigene Security-Chips an, welche mit den Chips auf den Laptops ausgetauscht werden können, um BIOS-Passwörter zu umgehen (u.a. auch für IBM Thinkpad Laptops)[82]. Allerdings erfordert das Austauschen dieser Chips ausgeprägte technische Hardwarekenntnisse. Je nach Modell und Hersteller können weitere Anleitungen im Internet existieren, die das Aushebeln von BIOS-Passwörtern behandeln. Im Falle von IBM Thinkpad Laptops existiert gar eine ganze Website, welche sich ausschliesslich mit dem Cracken entsprechender BIOS-Passwörter beschäftigt[83].

Neben Power-On-Passwörtern bieten einige Laptops auch die Möglichkeit, die Harddisk (HD) mit Passwörtern vor unbefugten Zugriffen zu schützen. Die Passwörter werden auf der Harddisk (in der Festplattenfirmware) gespeichert, so dass man auch dann nicht auf die Daten zugreifen kann, wenn die Harddisk in ein anderes System eingebaut wird. Es handelt sich hierbei um das so genannte "Security Feature Set" der ATA-Spezifikation[84] [Bögeholz, 2005][Hatfield, 2006]. Das Security Feature Set erlaubt das Setzen zweier Kennwörter: das "User Password" und das "Master Password". Letzteres kann dazu verwendet werden, um den Festplattenzugriff wiederherzustellen, auch wenn das "User Password" abhanden gekommen ist. Mit dem Setzen eines "User Password" wird der Zugriff auf die Nutzdaten auf der Harddisk gänzlich verhindert. Harddisk-Passwörter haben mit BIOS-Passwörter nichts zu tun (obschon HD-Passwörter im BIOS konfiguriert werden), d.h. die Techniken, um BIOS-Passwörter zu knacken, können zum Knacken von Harddisk-Passwörtern nicht eingesetzt werden. Für IBM Thinkpad Laptops scheint es zurzeit auch tatsächlich keinen "günstigen" Weg zu geben, um Harddisk-Passwörter zu umgehen, gemäss der weiter oben erwähnten Website, welche sich mit dem Cracken von IBM Thinkpad Passwörtern beschäftigt. Gemäss anderen Quellen ist es aber durchaus möglich, ATA-Harddisk-Passwörter zurückzusetzen[85] [Bosen, 2007][Bögeholz, 2005]. So existieren zum Beispiel Datenrettungsunternehmen, welche entsprechende Services anbieten. Allerdings kann so ein Vorhaben auch ziemlich teuer werden. Je nachdem, wie sensibel und wertvoll die Daten auf der Disk sind, lohnen sich die Investionen in so einen Datenrettungsservice aber allemal.

Eine sicherere Variante als das ATA Security Feature Set, um Festplatten vor unbefugten Zugriffen zu schützen, ist den Inhalt auf der Festplatte zu verschlüsseln. Wurde die Festplattenverschlüsselung sicher konfiguriert, hat ein Angreifer praktisch keine Chancen, an sensible Daten heranzukommen. Es existieren verschiedene Möglichkeiten zur Festplattenverschlüsselung: So gibt es zum Beispiel Softwarelösungen, welche nur bestimmte Dateien oder Verzeichnisse verschlüsseln oder aber auch ganze Festplatten. Softwarelösungen, welche ganze Festplatten verschlüsseln (Software-based-Full-Disk-Encryption), verlangen vom Benutzer einmal ein Passwort - danach werden die Daten für den Benutzer transparent verschlüsselt, bzw. entschlüsselt. Das Trusted Platform Module (TPM)[86] [87] enthält einen sicheren Kryptoprozessor, welcher auf dem Mainboard angebracht wird. Die Schlüssel, welche von den Full-Disk-Encryption-Programmen zur Ver- und Entschlüsselung verwendet werden, lassen sich dann an ein bestimmtes TPM binden (Bin-

[81] http://www.pwcrack.com/bios.shtml
[82] http://www.pwcrack.com/security_chips.shtml
[83] http://www.ja.axxs.net/unlock/
[84] http://de.wikipedia.org/wiki/ATA/ATAPI
[85] http://www.hardwareanalysis.com/content/topic/34045/
[86] http://de.wikipedia.org/wiki/Trusted_Platform_Module
[87] http://en.wikipedia.org/wiki/Full_disk_encryption

ding/Wrapping - Sealing), d.h. wenn die Festplatte in ein anderes System eingebaut wird, schlägt die Entschlüsselung der Daten fehl. Allerdings bieten nicht alle Softwarelösungen eine Unterstützung für TPM an. Ein Wikipedia-Artikel gibt einen guten Überblick über verschiedene Softwarelösungen für Festplattenverschlüsselung[88]. Ausserdem existieren auch Hardwarelösungen, beispielsweise Festplatten, bei denen Festplattenverschlüsselung direkt in die Laufwerke eingebaut ist (Hardware-based-Full-Disk-Encryption)[89]. Grundsätzlich kann man sagen, dass Hardware-based-Full-Disk-Encryption performanter abläuft als die Software-Variante. Softwaresysteme sind ausserdem grundsätzlich durch Malware angreifbar (z.B. Stehlen von Encryption-Keys, etc.). Hardware-basierte Festplattenverschlüsselung gilt als sehr sicher, wenn sichere Passwörter verwendet werden (oder alternative, als sicher geltende Authentifizierungsmechanismen) [Benz, 2005][Bosen, 2007].

Hat man die ersten Hürden (BIOS-Passwörter, HD-Passwort) erst einmal überwunden, sind die weiteren Schritte zur Kompromittierung meistens nicht mehr allzu schwierig. Die nächsten Schritte, welche ein Angreifer nun höchst wahrscheinlich unternehmen würde, wären das Auslesen sensitiver Daten und das Anmelden am Betriebssystem. Wenn wir davon ausgehen, dass wir nun von einem beliebigen Device booten können, ist es einfach, sensitive Daten auszulesen (angenommen die Festplatte sei nicht sicher verschlüsselt). Sensitive Daten lassen sich zum Beispiel mit einer Linux-LiveCD (z.B. Backtrack[90]) auslesen. Dazu bootet man ganz einfach von der LiveCD und mountet dann das Laufwerk, auf welchem sich die sensitiven Daten befinden. Um also sensitive Daten auszulesen, ist es nicht einmal nötig, sich korrekt am Betriebssystem, das auf dem Notebook installiert wurde, anzumelden. Letzteres dürfte in einigen Fällen aber auch nicht allzu schwierig sein. Der Zugriff auf das Betriebssystem ist für Angreifer insbesondere dann interessant, wenn dort zum Beispiel Programme für den Zugriff auf das interne Firmennetz installiert wurden. Angreifer könnten dann versuchen, sich über diese Programme irgendwie in das Firmennetz einzuschleusen, um weiteren Schaden anzurichten. Je nachdem, welches Betriebssystem auf dem Laptop installiert wurde, gibt es unterschiedliche Techniken, um Systempasswörter zu knacken. Wir wollen zunächst einige Techniken für Windows-Systeme beleuchten und uns dann Linux-Systemen zuwenden. Weitere Informationen zum Thema Passwort-Cracking befinden sich auch im Kapitel 6.4.1.

Eine der einfachsten Methoden, Systempasswörter eines Windows-System zu knacken, ist die Ophcrack-LiveCD. Ophcrack[91] ist ein Windows-Passwort-Cracker. Das Tool kann LM- und NTLM-Hashes knacken. Der Cracking-Vorgang mit der LiveCD ist enorm simpel: Man muss nichts weiter tun, als ganz einfach von der CD zu booten. Der Cracking-Vorgang wird sodann automatisch gestartet. Hat das Opfer ein einfach zu erratendes Passwort gewählt, kann das Passwort mit einer hohen Wahrscheinlichkeit geknackt werden. Windows-Passwörter können auch mit einer Backtrack-LiveCD geknackt werden. Backtrack ist eine Linux-Distribution, welche speziell für Penetration-Tester konzipiert wurde und somit bereits viele nützliche Penetration-Testing-Tools enthält. Das Vorgehen zum Knacken von Windows-Passwörtern mit Backtrack ist etwas komplizierter als mit einer Ophcrack-LiveCD, aber auch nicht allzu schwierig. Ein Artikel von J. Dravet enthält entsprechende Anleitungen [Dravet, 2008]. Das Vorgehen kann wie folgt zusammengefasst werden: Zunächst bootet man von der Backtrack-LiveCD. Danach wird die Windows-Systempartition gemountet. Mit den Linux-Tools bkhive und samdump2 können sodann die Passwort-Hashes extrahiert werden. Schliesslich kann man versuchen, mit john die Hashwerte zu knacken. Die Backtrack-LiveCD enthält ausserdem ein Tool, mit welchem das Passwort eines Windows-Benutzers ganz einfach zurückgesetzt werden kann. Unter Umständen ist es also gar nicht unbedingt nötig, das Passwort zu cracken, sondern es genügt, das Passwort schlicht abzuändern oder zurückzusetzen. Das entsprechende Tool, um Windows-Passwörter zurückzusetzen, nennt sich chntpw. Eine einfache Anleitung für chntpw findet man ebenfalls im Text von Dravet [Dravet, 2008].

Linux-Passwörter können ebenfalls relativ einfach mit der Backtrack-LiveCD geknackt

[88] http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software
[89] http://en.wikipedia.org/wiki/Hardware-based_full_disk_encryption
[90] http://www.backtrack-linux.org/
[91] http://ophcrack.sourceforge.net/

werden. Das Vorgehen dabei unterscheidet sich allerdings ein bisschen von dem bei Windows-Passwörtern. Eine einfache Anleitung findet sich wiederum im Text von Dravet [Dravet, 2008]. Zunächst bootet man wie gewohnt mit der Backtrack-LiveCD und mountet dann das Linux-Systemlaufwerk. Der Unterschied liegt nun im Wesentlichen darin, wie man an die Passwort-Hashes herankommt. Bei modernen Linux-Systemen befinden sich die Nutzerdaten und die eigentlichen Passwort-Hashes in zwei unterschiedlichen Dateien (/etc/passwd und /etc/shadow[92]). Damit Linux-Passwörter geknackt werden können, müssen diese beiden Dateien zuerst wieder "zusammengeführt" werden. Zu diesem Zweck verwendet man den unshadow Befehl, welcher Teil des john-Tools ist. Die mit unshadow erzeugte Datei kann nun schliesslich als Input für john verwendet werden, um schliesslich die Passwörter zu knacken.

Natürlich können nicht alle Passwörter ohne weiteres geknackt werden. Hat das Opfer starke Passwörter gewählt und wurden sichere Hashalgorithmen gewählt (als unsicher gelten zum Beispiel Windows LM-Hashes, welche deshalb unter keinen Umständen mehr verwendet werden sollten, so dürften Passwort-Cracking-Versuche aussichtslos sein. Will man aber "nur" sensitive Dateien auslesen, muss man sich die Mühe, Passwörter zu knacken, sowieso erst gar nicht machen.

6.11.2 Ausgeführte Tests

Wie bereits weiter oben erwähnt, handelte es sich beim Test-Laptop um einen IBM Thinkpad T43 2668-C16. Die Festplatte war mit einem Harddisk-Password (HDP) versehen. Ausserdem benötigte man zum Starten des Laptops ein spezielles USB-Dongle-System.

Zunächst haben wir versucht, irgendwie von einem Device zu booten, was allerdings aussichtslos war. Ohne den USB-Dongle und das entsprechende Passwort bootet die Maschine nicht. Linux-LiveCDs können somit nicht eingesetzt werden. Es ist auch nicht möglich, von einem anderen USB-Stick zu booten. Die Festplatte in ein anderes System einzubauen brachte uns auch nicht viel weiter, da die Festplatte wie bereits angetönt mit einem Harddisk-Passwort versehen war.

Parallel dazu haben wir eine Internet-Recherche durchgeführt, um zu schauen, wie die eingesetzten Sicherheitsmassnahmen umgangen werden könnten. Dabei sind wir auf zwei potentielle Lücken gestossen: Harddisk-Passwörter (ATA Security Feature Set) und IBM Thinkpad BIOS Passwörter. Leider konnten wir die Lücken allerdings nicht praktisch verifizieren.

Ebenfalls konnten wir nicht austesten, was für Software und welche Softwareversionen auf dem Laptop installiert waren.

6.11.3 Folgerungen

Auf den ersten Blick muss man sagen, dass das System relativ gut gesichert ist. Mit den implementierten Massnahmen sollten zumindest Script Kiddies und einfache Angreifer abgewehrt werden können. Schaut man allerdings etwas genauer hin und recherchiert ein bisschen im Internet, so taucht doch der eine oder andere Schwachpunkt auf. So bieten zum Beispiel Harddisk-Passwörter mit dem ATA Security Feature Set wenig Sicherheit. Zumindest scheint es einige Firmen zu geben, welche entsprechende Passwörter wiederherstellen können. Harddisk-Passwörter haben aber noch ein ganz anderes Problem: So hat es scheinbar schon Vorfälle gegeben, dass Angreifer über Malware bei Opfern ein Harddisk-Passwort setzten, so dass die betroffenen Personen nicht mehr auf ihre Daten zugreifen konnten [Bögeholz, 2005]. Ein weiteres Problem ist, dass IBM Thinkpad BIOS Passwörter scheinbar relativ einfach umgangen werden können. Inwiefern man damit auch das USB-Dongle-System aushebeln kann, konnten wir allerdings nicht nachvollziehen.

[92] http://de.wikipedia.org/wiki/Shadow-Passwort

7 Risikoanalyse

In Kapitel 5 (Bedrohungsanalyse) haben wir mögliche Angriffsvektoren für die VT-Systeme eruiert (sozusagen eine Risikolandkarte) und diese Angriffsvektoren in Angriffsgruppen, welche ein ganz bestimmtes Angriffsziel beschreiben, gruppiert. In Kapitel 6 (Verifikation bereits umgesetzter Sicherheitsmassnahmen) wurde dann untersucht, inwiefern die aktuell umgesetzten Sicherheitsmassnahmen gegen die in Kapitel 5 identifizierten Angriffsgruppen schützen. Gestützt auf den Resultaten aus den Kapiteln 5 und 6 geht es in diesem Kapitel nun darum, eine Risikoanalyse durchzuführen. Dabei stützen wir uns wieder auf den "elementaren" Angriffsvektoren aus Kapitel 5 und nicht auf den "Angriffsgruppen" und aus zwar aus dem Grunde, dass in einer Risikoanalyse das Gesamtspektrum an möglichen Risiken/Angriffsvektoren betrachtet werden sollte [Gleissner, 2008]. Die Gruppierung logisch zusammengehöriger Angriffsvektoren in Angriffsgruppen spielt für die Risikoanalyse in diesem Sinne eine untergeordnete Rolle.

"Die Risikoanalyse beinhaltet eine Beurteilung der Tragweite der erkannten Risiken in Bezug auf Eintrittswahrscheinlichkeit und quantitative Auswirkungen"[93]. Für die Quantifizierung dieser Eintrittswahrscheinlichkeiten und Konsequenzen (Auswirkungen) der einzelnen Risiken stützen wir uns dabei auf qualitative Methoden und zwar deswegen, weil es im Kontext von VT-Systemen extrem schwierig oder gar unmöglich wäre, die genauen Kosten (Konsequenzen) beim Eintritt eines bestimmten Angriffsvektors zu benennen. Genauso schwierig wäre es zu sagen, mit welcher genauen Wahrscheinlichkeit ein gewisser Angriffsvektor eintritt. Um dennoch eine Möglichkeit zu erhalten, die einzelnen Angriffsvektoren miteinander zu vergleichen, bieten qualitative Methoden einen guten Kompromiss. Bei qualitativen Methoden werden für die Eintrittswahrscheinlichkeiten und die Konsequenzen eines Risikos keine "scharfen" Werte, wie z.B. "ein erwartetes Ereignis pro Jahr" oder "CHF 100'000 Schaden pro Ereignis", ermittelt, sondern es werden die Eintrittswahrscheinlichkeiten und Konsequenzen in Kategorien eingeteilt: So können die Konsequenzen "hoch", "spürbar" oder aber "unbedeutend" sein. Gleichermassen kann die Wahrscheinlichkeit in Kategorien wie "häufig", "gelegentlich" oder "selten" eingeteilt werden.

Die Kapitel 7.2 bzw. 7.3 diskutieren die verschiedenen Kategorien, welche wir für diese Risikoanalyse für die Konsequenzen bzw. Eintrittswahrscheinlichkeiten ausgewählt haben. Durch die Einteilung der Eintrittswahrscheinlichkeiten und Konsequenzen entsteht eine so genannte Risikomatrix.

Abbildung 13: Beispiel Risikomatrix zeigt ein Beispiel einer solchen Risikomatrix. Es ist deutlich zu sehen, wie durch die Einteilung der Konsequenzen und Eintrittswahrscheinlichkeiten von Risiken in verschiedene Kategorien so genannte Risikoklassen entstehen. Die identifizierten Risiken (Angriffsvektoren) können somit einzelnen Risikoklassen zugeordnet werden. Dadurch wird sofort ersichtlich, welche Risiken genauer betrachtet werden müssen und welche Risiken vernachlässigt, d.h. akzeptiert werden können (Risiken, welche zum Beispiel in die Klasse mit Eintrittswahrscheinlichkeit "Häufig" und Konsequenzen "Katastrophal" eingeteilt wurden, gilt es irgendwie zu bewältigen. Als Option kann zum Beispiel versucht werden, die Eintrittswahrscheinlichkeit zu verringern. Kapitel 7.4 diskutiert die Einteilung der von uns identifizierten Angriffsvektoren in die Risikoklassen der Risikomatrix. In Kapitel 7.5 wird die Einteilung der Angriffsvektoren in Risikoklassen in einer Risikomatrix grafisch dargestellt und es werden die "kritischsten" Angriffsvektoren herausgehoben.

[93] Institut der Wirtschaftsprüfer (IDW) Prüfungsstandard 340, S.3., zitiert durch [Gleissner, 2008]

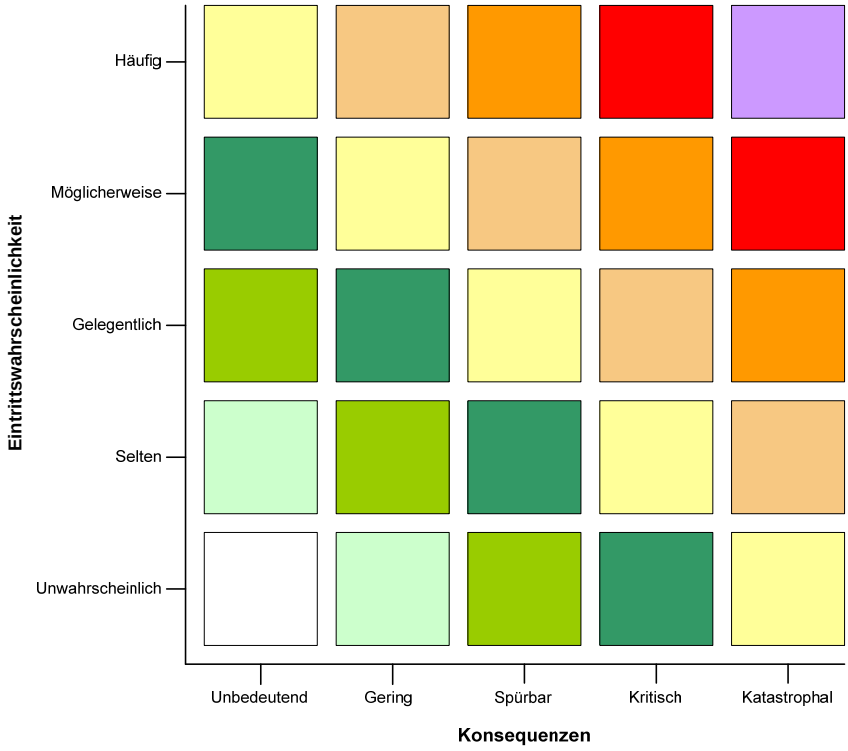


Abbildung 13: Beispiel Risikomatrix

7.1 Abschliessende Attacken und vorbereitende Angriffsvektoren

In Kapitel 5 wurde eine Vielzahl von Angriffsvektoren aufgeführt, u.a. auch solche, welche den VT-Betrieb zwar nicht direkt stören, aber als Vorbereitung für einen entsprechenden Angriff dienen (z.B. Angriffsvektoren der Angriffsgruppe "Information Gathering" oder "Scanning"). Für die Einteilung in Risikoklassen in diesem Kapitel wollen wir allerdings nur jene Angriffsvektoren betrachten, welche wirklich eine abschliessende Attacke (z.B. Daten korrumpieren/löschen) darstellen, die den VT-Betrieb direkt stören können. Die anderen Angriffsvektoren werden dabei aber nicht ganz ausser Acht gelassen, sondern sind behilflich bei der Zuordnung einer "abschliessenden Attacke" in eine bestimmte Wahrscheinlichkeitskategorie. So kann zum Beispiel argumentiert werden, dass Attacken, die kaum eine Vorbereitung benötigen (d.h. nur ein wenig Information Gathering und Scanning, kein Social Engineering, etc.) relativ gesehen häufiger zum Erfolg führen (also eine höhere Eintrittswahrscheinlichkeit aufweisen) als Attacken, die eine intensive Vorbereitung (d.h. es ist ein detailliertes Information Gathering nötig, Systeme müssen akribisch gescannt und auf Schwachstellen untersucht werden, Social Engineering muss angewendet werden, etc.) für eine erfolgreiche Durchführung benötigen.

Folgende Angriffsvektoren aus Kapitel 5 können als "abschliessende Attacken" bezeichnet werden (damit diese "abschliessenden Attacken" später besser in Risikoklassen eingeteilt werden können, werden sie hier noch etwas genauer spezifiziert als in Kapitel 5):

Nr.	Name	Beschreibung/Beispiel
1.	DoS	Eine einfache DoS-Attacke, die von einem externen Angreifer ausgeführt wird, z.B. auf einen Webserver oder eine Komponente des BLS, so dass der entsprechende Service/die entsprechende Komponente kurzzeitig unerreichbar ist.
2.	DDoS	Eine koordinierte DDoS-Attacke, wobei ein ganzes Bot-Netz ein bestimmtes System eines VT-Betreibers mit einer sehr grossen Anzahl von Anfragen eventuell längerfristig lahm legen kann.

Nr.	Name	Beschreibung/Beispiel
3.	Malware auf Webserver installieren	Die Malware soll dabei Browserschwachstellen ausnutzen und so die Besucher von Webseiten der VT-Betreiber angreifen.
4.	Webseiten verunstalten	z.B. ein Online-Portal eines VT-Betreibers.
5.	Daten lö-schen/korrumpieren	z.B. Beweisbilder, sodass die Beweisbilder vor Gericht keinen Be-stand mehr haben.
6.	Sensitive Daten stehlen	z.B. vertrauliche Bilddaten, wodurch datenschutzrechtliche Probleme für die Betreiber der VT-Systeme entstehen könnten.
7.	Patches/OS-Updates/Malwareupdates	Patches und Updates, welche sich aus verschiedenen Gründen nicht mit dem System vertragen, können ein System lahm legen.
8.	Logische/physische Bedi-enfehler	z.B. aus Versehen ein Signal falsch stellen oder eine "falsche" Wech-seltextanzeige ausgeben, was zu Verkehrsproblemen führen könnte, aber auch Ziehen eines Steckers aus Versehen, wodurch eine Kom-ponente ausfallen würde.
9.	Einstecken eines mit Malware verseuchten Geräts	Ein Mitarbeiter steckt unabsichtlich und unwissend einen mit Malware verseuchten Laptop oder USB-Stick in ein System ein, wodurch sich die Malware ausbreiten und das System lahm legen könnte.
10.	Allgemeine Wartungsar-beiten am System	Mitarbeiter oder Lieferanten könnten beispielsweise durch unsach-gemässe Installation einer neuen Systemkomponente das System lahm legen.
11.	Strassenanlagen bedienen für arglistige Zwecke	Die Bedienung erfolgt dabei über das BLS. Das arglistige Bedienen der Strassenanlagen könnte zu einem Verkehrschaos führen. Als Beispiel für eine arglistige Bedienung könnte ein absichtliches Auslö-sen eines Tunnelrots oder die Schliessung eines Tunnels angeführt werden.
12.	Absichtliche Verbreitung von Malware	z.B. absichtliches Einstecken eines verseuchten Laptops oder USB-Sticks durch verärgerte Mitarbeiter. Die dadurch verbreitete Malware könnte das BLS lahm legen.
13.	Feldkomponenten umpro-grammieren	z.B. so, dass sie nicht mehr auf Befehle des BLS reagieren oder falsche Informationen ans BLS liefern.
14.	Feuer legen	z.B. in BLZ, Tunnels, etc. Das Feuer gefährdet entsprechende Kom-ponenten des Kommunikationsnetzes.
15.	Physische Beschädigung von Feldkomponenten	Physische Beschädigung von Sensoren/Aktoren auf der Feldebene, wie z.B. Kameras, Wechseltextanzeigen, etc.
16.	Rechner mit Gewalt zer-stören	z.B. Tunnelrechner und Gruppenrechner
17.	Rechner herunterfah-ren/ausstecken	z.B. Tunnelrechner und Gruppenrechner
18.	Kabel durchtren-nen/ausstecken	Auf diese Weise kann die Kommunikationsverbindung zu gewissen Komponenten komplett ausfallen.
19.	Brandmeldesensor mani-pulieren	z.B. in Tunnel, BLZ, etc. Das könnte beispielsweise zu einer unnöti-gen Evakuierung eines Gebäudes führen, was auch mit entsprechen-dem Aufwand verbunden ist. Ferner könnten dadurch Sprinkleranla-gen aktiviert werden, sodass zusätzlich auch noch physischer Scha-den entsteht.
20.	Videokameras ausstecken	-
21.	Unfall in BLZ Gebäude	z.B. eine Gasexplosion oder eine defekte Wasserleitung, wodurch die Komponenten der BLZ gefährdet/physisch beschädigt werden könn-ten.
22.	Server vom Netz tren-nen/herunterfahren	Einen Server in der BLZ vom Netzwerk trennen oder den Server herunterfahren, so dass entsprechende Services nicht mehr abgeru-fen werden können.
23.	Backup-Tapes zerstören	-
24.	Eine E-Mail versenden, die schädlichen Code enthält	Die Malware kann sich dabei im Anhang befinden (z.B. eine präpa-rierte PDF-Datei, welche eine Schwachstelle im Adobe Acrobat Rea-der ausnützt oder ausführbare Dateien). Nachrichten, die im HTML-Format gesendet werden, können direkt schädlichen Script-Code enthalten. Die Malware soll dazu dienen, das BLS lahm zu legen.

Folgende Angriffsvektoren aus Kapitel 5 dienen zur Vorbereitung von "abschliessenden Attacken":

- Google Hacking (filetype:pcf site:example.com; Index of /password; etc.)
- Webcrawling (Firmenwebseiten auf lokalen Computer kopieren und mit speziellen Tools nach interessanten Informationen durchsuchen. Möglicherweise sind auskommentierte "Testpasswörter" im HTML-Code vorhanden etc.)
- Facebook, Jobwebseiten (evtl. geben Jobausschreibungen Informationen über den momentanen Security-Standard einer Firma Preis), Internetarchive (archive.org, thememoryhole.org), Internetforen (z.B. publizierte Firewallkonfigurationen etc.)
- WHOIS & DNS Enumeration (IP-Adressen und Domainnamen herausfinden)
- DNS Interrogation (zone transfer)
- Network Reconnaissance (Komplettes Profil der Netzarchitektur des Opfers zusammenstellen: traceroute, automatisierte Programme, etc.)
- Nach offenen Ports scannen
- Ping Sweeps
- ICMP Queries
- Betriebssystem bestimmen
- Enumeration (Banner Grabbing, etc.)
- Nach Schwachstellen scannen (Nessus, Nikto, OpenVAS)
- Web-Cyberattacken (Session Hijacking, SQLi, Unvalidated Redirects and Forwards, CSRF, SSI, XSS)
- Manual Webapplication Assessment (Mit Browser Plug-ins, Web Proxies (z.B. Webscarab), Directory-Listing, Source Code Disclosure, Sample Files, Canonicalization Attacks)
- Brute Forcing
- Dictionary PW Guessing/Rainbowtables
- VPN-Hacking (z.B. IKE-Aggressive-Mode hacken, etc.)
- Wardialing (einen Bereich möglicher Telefonnummern durchtesten mit spezieller Wardialing-Software - evtl. mit einem gestohlenen Laptop. Die ISDN-Zugänge beruhen ja zum Teil auf "Geheimhaltung der Telefonnummern")
- WEP-/WPA-Hacking
- GSM-/GPRS-Hacking (AGK will für mobile Stationen auch GSM-Zugang einbauen)
- Sniffing (z.B. PW Exchange, etc.)
- Physischen Zugang als verkleideter Lieferant/Mitarbeiter erhalten
- Phishing (Mitarbeiter werden über E-Mail z.B. auf eine gefälschte Seite gelockt, wo sie gebeten werden, ihr Passwort zu übermitteln auf Grund von "irgendwelchen Sicherheitsvorkehrungen")
- E-Mail mit vertrauenswürdiger Absender-Adresse versenden (z.B. Adresse eines Lieferanten/Administrators/Mitarbeiters) um an interne Informationen (IP-Adressen, Domainnamen, Telefonnummern, Passwörter, etc.) ranzukommen
- Sich am Telefon als Lieferant/Mitarbeiter ausgeben, um sich einen Remotezugang freischalten zu lassen
- Insiderkenntnisse (z.B. veröffentlichen sensibler Daten in einem öffentlichen Forum, aber auch ausnutzen der Kenntnisse für arglistige Zwecke)
- Zugang zum System über nicht entfernte Benutzerkonten
- Zugang zum System über Schlüssel, die dem Benützer nicht entzogen worden sind
- Einbruch (z.B. in ein BLZ-Gebäude oder in eine Tunnelanlage)
- Backdoors installieren
- Keyloggers installieren
- Malware installieren, die Schwachstellen im Browser ausnutzen können

7.2 Kategorien für Konsequenzen

Die Konsequenzen werden in folgende Kategorien aufgeteilt:

- Unbedeutend
- Gering
- Spürbar
- Kritisch
- Katastrophal

Die Einteilung in die unterschiedlichen Kategorien für Konsequenzen erfolgt anhand dessen, wie stark der VT-Betrieb durch einen entsprechenden Vorfall/Angriffsvektor eingeschränkt wird.

7.2.1 Unbedeutend

Unbedeutend sind z.B. jene Konsequenzen eines erfolgreichen Angriffs, welche den operativen Betrieb der VT-Systeme in keiner Art und Weise beeinträchtigen. Ein Beispiel wäre die Verunstaltung des Webportals eines VT-Betreibers. Verunstaltete Webseiten sind zwar durchaus mühsam, der operative Betrieb der VT-Systeme wird dadurch aber nicht im Geringsten gefährdet. Da eine verunstaltete Website für den Betrieb nicht kritisch ist, müssen auch nicht sofortige Massnahmen eingeleitet werden. Der Aufwand, um eine verunstaltete Seite zu "reparieren", hält sich in Grenzen.

7.2.2 Gering

Gering ist eine Konsequenz dann, wenn der operative Betrieb der VT-Systeme nur geringfügig gestört wird, d.h., dass höchstens ein paar nicht kritische Funktionen auf BLZ-Ebene kurzzeitig ausfallen. Als Beispiel könnte man sich eine DoS-Attacke auf ein Verwaltungsportal der Betreiber (z.B. Webviewer für Verkehrsüberwachung) oder einen VPN-Gateway vorstellen. Dadurch sind gewisse Funktionen zwar zwischenzeitlich nicht mehr erreichbar, der operative VT-Betrieb wird dadurch aber nicht gross gefährdet. Die Komponenten können mit überschaubarem Aufwand wieder in Betrieb gesetzt werden.

7.2.3 Spürbar

Spürbare Konsequenzen stören den VT-Betrieb bereits so, dass vereinzelte, wichtige Komponenten des VT-Betriebs ausfallen. Beispiele könnten der Ausfall von Videokameras oder der Ausstieg gewisser Tunnelrechner sein. Auch die Konsequenzen einer organisierten Cyberattacke (beispielsweise eine DDoS-Attacke) auf einen VPN-Gateway oder ein Verwaltungsportal, sodass der entsprechende Dienst während einigen Tagen nicht mehr erreichbar ist oder nicht mehr kontrolliert werden kann, können als spürbar bezeichnet werden. Der Ausfall ist allerdings "nur" temporär und lokal begrenzt und die betroffenen Komponenten lassen sich innert "nützlicher Frist" ersetzen oder reparieren.

7.2.4 Kritisch

Kritische Konsequenzen haben zur Folge, dass keine "übergeordnete Steuerung" mehr möglich ist - die Systeme lassen sich also nicht mehr verlässlich von der BLZ aus kontrollieren. Ein Beispiel wäre ein Ausbruch einer Malware, welche das gesamte Kommunikationsnetz lahm legt oder ein Angreifer, welcher die Kontrolle über einen Grossteil der Steuerungsmechanismen erlangt hat. Vor Ort, auf der Feldebene, lassen sich die Geräte aber noch bedienen. Dadurch kann zwar temporär ein Verkehrschaos entstehen, allerdings ist durch die Möglichkeit, dass die VT-Systeme lokal noch bedient werden können, gegeben, dass das Problem innert einer gewissen Frist zumindest etwas entschärft werden kann.

7.2.5 Katastrophal

Bei katastrophalen Konsequenzen gerät der VT-Betrieb völlig ausser Kontrolle. Die Sys-

teme lassen sich dann überhaupt nicht mehr kontrollieren, weder von der BLZ aus noch vor Ort. Ein Angreifer hat die vollständige Kontrolle über BLZ erlangt. Neben immensen Kosten für den Wiederaufbau der Systeme ist auch mit grossen Reputationsschäden für die VT-Betreiber und damit auch für Bund und Kantone zu rechnen.

7.3 Kategorien für Eintrittswahrscheinlichkeiten

Die Eintrittswahrscheinlichkeiten werden in folgende Kategorien aufgeteilt:

- Unwahrscheinlich
- Selten
- Gelegentlich
- Möglich
- Häufig

Für die Einteilung der Eintrittswahrscheinlichkeiten in unterschiedliche Kategorien nehmen wir uns den Attack-Tree aus Kapitel 5.1 zur Hilfe. Wie wir im Attack-Tree gesehen haben, durchläuft ein Angriff in seiner allgemeinsten Form folgende Stufen:

- (im Falle von Cyberattacken) Angreifbare Systeme identifizieren als:
  - Berechtigter Benutzer (interne/externe Mitarbeiter, Insider, ehemalige Benutzer, Lieferanten)
  - Externer Angreifer mittels:
    - Social Engineering
    - Analysemethoden (Information Gathering und Scanning)
- Zugang zu den Systemen (physisch oder logisch) erhalten als:
  - Berechtigter Benutzer (interne/externe Mitarbeiter, Insider, ehemalige Benutzer, Lieferanten)
  - Externer Angreifer mittels:
    - Social Engineering
    - Cyberattacke
- Attacke ausführen

Gewisse Angriffe durchlaufen allerdings nicht alle Stufen, die oben abgebildet wurden. Beispielsweise muss man sich nicht unbedingt Zugang zu einem System verschaffen, um eine einfache DoS-Attacke ausführen zu können. Bei physischen Attacken müssen die anzugreifenden Systeme nicht zuerst mittels Analysemethoden identifiziert werden.

Parallel zu den oben abgebildeten Stufen eines Angriffs können für eine Klassifizierung der Eintrittswahrscheinlichkeiten auch Aspekte wie Erreichbarkeit des anzugreifenden Systems, benötigtes Know-how für die gesamte Ausführung der Attacke, benötigte Ressourcen, vorhandene Sicherheitsmassnahmen und der "Wert eines Angriffs" (wie viel Schaden man mit einem entsprechenden Angriff anrichten kann) betrachtet werden. So werden zum Beispiel Systeme, welche direkt am Internet angeschlossen und schlecht geschützt sind (z.B. veraltete Software etc.), sodass deren Schwachstellen mittels einfachen Analysemethoden identifiziert werden können, eher angegriffen als Systeme, deren Schwachstellen nur mittels Insiderkenntnissen analysiert werden können. Ausserdem werden Angriffe, welche sich mit einfachen Mitteln, z.B. öffentlich verfügbaren Exploits, ausführen lassen eher durchgeführt als Angriffe, die nur mit sehr spezifischem Know-how durchgeführt werden können. Die Wahrscheinlichkeit eines erfolgreichen Angriffs kann ausserdem entscheidend reduziert werden, wenn starke und robuste Sicherheitspraktiken im Einsatz sind (z.B. möglichst wenig Informationen öffentlich verfügbar machen, Einsatz von restriktiven Firewalls, etc.) und die Systeme gut gehärtet sind (aktuelle Patches, sichere Softwarekonfiguration, etc.). Schliesslich spielt der Wert des Angriffs eine entscheidende Rolle. Der Aspekt des "Wertes eines Angriffs" kann jedoch nicht für sich alleine betrachtet werden, sondern muss im Zusammenhang mit den anderen besprochenen Aspekten verstanden werden. Lässt sich beispielsweise mit einem bestimmten

Angriff viel Schaden anrichten oder ein grosser Gewinn erzielen und kann dieser Angriff mit geringem Aufwand und wenig Know-how durchgeführt werden, so wird der entsprechende Angriff eher ausgeführt als ein Angriff, durch dessen Konsequenzen ein vernachlässigbarer Aufwand für die VT-Betreiber entsteht und dessen Ausführung erst noch viel Ressourcen benötigt und ein hohes Know-how voraussetzt.

An dieser Stelle soll auch nochmals explizit erwähnt werden, dass wir unter Eintrittswahrscheinlichkeit die Wahrscheinlichkeit verstehen, dass ein bestimmter Angriff erfolgreich ausgeführt werden kann (sodass die entsprechenden Konsequenzen des Angriffs eintreten). Grundsätzlich kann man also nicht sagen, dass exponierte Systeme (also Systeme, die direkt über das Internet erreichbar sind) automatisch mit einer hohen Wahrscheinlichkeit kompromittiert werden können. Wenn ein exponiertes System entsprechend gut gesichert wurde, kann die Eintrittswahrscheinlichkeit für einen bestimmten Angriff durchaus auch sehr tief sein. Was man aber sagen kann, ist, dass exponierte Systeme grundsätzlich eher Angriffsversuchen ausgesetzt sind als isolierte Systeme. Das bedeutet dann aber, wie bereits erwähnt, nicht automatisch, dass der Angriff dann auch bei jedem Angriffsversuch zum Erfolg führt. Des Weiteren soll noch erwähnt werden, dass die folgenden Wahrscheinlichkeitskategorien auf den aktuell implementierten Schutzmechanismen der Interviewpartner beruhen (gemäss Kapitel 6).

7.3.1 Unwahrscheinlich

Angriffe, deren Eintrittswahrscheinlichkeiten als "unwahrscheinlich" einzustufen sind, benötigen für eine erfolgreiche Ausführung einen physischen Zugang zu Feldsystemen. Die dazu nötigen Vorbereitungen für einen externen Angreifer sind derart hoch, dass sich ein solcher Angriff kaum noch lohnt. Einerseits muss ein externer Angreifer herausfinden, wo sich die entsprechenden Systeme überhaupt befinden (die entsprechenden Informationen herauszufinden dürfte schwierig sein, da kaum Informationen zu Standorten von Feldsystemen öffentlich verfügbar sind, gemäss unseren Erkenntnissen aus dem Information Gathering - siehe Abschnitt 6.1). Dann benötigt ein externer Angreifer auch entsprechende Mittel, um sich Zugang zu den Systemen beschaffen zu können. In den meisten Fällen dürfte ein externer Angreifer nicht um die Anwendung physischer Gewalt herumkommen, um zum Ziel zu gelangen. Beispiele für solche Angriffe sind das Herunterfahren/Zerstören von Tunnelrechnern, Ausstecken von Tunnelrechnern, Legen von Feuern in Tunnels, etc.

7.3.2 Selten

Angriffe, welche selten erfolgreich ausgeführt werden, zielen einerseits auf Systeme ab, bei welchen der Zugang nicht mehr über den "logischen Weg" erlangt werden kann. Es wird mindestens physischer Zugang zum BLS-Gebäude vorausgesetzt, d.h. ein berechtigter Benutzer kann die Attacke auf Stufe BLS ausführen. Ein externer Angreifer kann versuchen, mit einer entsprechenden Verkleidung Zugang zum System zu erhalten - allenfalls müssen dann aber auch noch die benötigten Schlüssel beschafft werden. Auch ein Einbruch durch einen externen Angreifer könnte zum Ziel führen. Schliesslich könnte ein externer Angreifer auch noch versuchen, einen Feueralarm auszulösen, um Zugang zum Gebäude zu erlangen. Ein Beispiel für einen Angriff dieses Typs wäre zum Beispiel das Bedienen der VT-Systeme für arglistige Zwecke. Andererseits können selten eintretende Angriffe auch auf Systeme abzielen, die zwar öffentlich erreichbar aber so gut "gehärtet" sind, dass Aufwand und Ertrag ("Wert" des Angriffs) in einem ungünstigen Verhältnis stehen.

7.3.3 Gelegentlich

Bei Angriffen, die "gelegentlich" eintreten, lässt sich der Zugang zu verwundbaren Systemen nur schwer mittels Analysemethoden beschaffen, insbesondere deshalb, weil die entsprechenden Systeme nur während klar definierten Zeitfenstern, die vom VT-Betreiber kontrolliert werden, über das Internet erreichbar sind. Als berechtigter Benutzer kann eine entsprechende Attacke aber von aussen ausgeführt werden, d.h. es ist für die schlussendliche Ausführung der Attacke nicht unbedingt notwendig, physisch vor Ort zu sein. Externe Angreifer müssen also mindestens Social-Engineering-Techniken anwenden, um sich einen Remotezugang freischalten zu lassen (z.B. Phishing-E-Mails, sich per Telefon

einen Zugang freischalten lassen, etc.), was natürlich eine intensive Vorbereitung voraussetzt - die nötigen Informationen lassen sich aber mittels Information Gathering ermitteln. Ausserdem müssen sie über die nötigen Credentials verfügen, um sich am System anmelden zu können. In diese Kategorie fallen zum Beispiel allgemeine Wartungsarbeiten am System oder Patches/Malwareupdates.

7.3.4 Möglicherweise

Angriffe, welche "möglicherweise" erfolgreich ausgeführt werden, zielen ebenfalls auf Systeme ab, die von aussen (über das Internet) erreichbar sind, allerdings muss man sich hier zunächst "logisch Zugang" verschaffen, damit man die Attacke ausführen kann. Die dazu benötigten Informationen lassen sich aber mittels Analysemethoden innert nützlicher Frist besorgen (mittels Information Gathering, Portscanning, Vulnerability Scanning etc.). Um Zugang zu erhalten, können öffentlich verfügbare Tools (z.B. Password Cracker, VPN-Footprinting-Tools, Sniffer, etc.) oder publizierte Exploits verwendet werden. Ein Beispiel für einen solchen Angriff wäre die Verbreitung von Malware über eine öffentlich bekannte Softwareschwachstelle. Auch die Verbreitung von Malware per E-Mail dürfte als möglich eingestuft werden: Hierzu muss man sich zwar nicht logisch Zugang verschaffen, allerdings müssen zusätzliche Informationen wie E-Mail-Adressen von möglichen Opfern beschafft werden. Ausserdem kann es sein, dass einfache Social-Engineering-Techniken (z.B. Fälschen der Absenderadresse) angewandt werden müssen, um das Opfer dazu zu bewegen, ein verseuchtes E-Mail-Attachment eher zu öffnen.

7.3.5 Häufig

Angriffe mit einer als "häufig" einzustufenden Eintrittswahrscheinlichkeit zielen auf Systeme ab, die direkt am Internet angeschlossen sind und somit ohne weiteres "von aussen" erreicht werden können. Angreifbare Systeme lassen sich innert kurzer Zeit (ein bis zwei Tage Aufwand für eine einzelne Person) mittels einfacher Analysemethoden (Portscanning, Vulnerability Scanning) identifizieren (die entsprechenden Systeme verfügen also beispielsweise über veraltete Software mit publizierten Schwachstellen und sind entsprechend schlecht geschützt). Solche Attacken können ausgeführt werden, ohne dass man sich zunächst Zugang beschaffen muss. Die Attacke selbst kann mittels einfachen, öffentlich verfügbaren Tools durchgeführt werden (z.B. Metasploit). Ein Beispiel für einen solchen Typ von Angriffen wäre eine einfache DoS-Attacke auf einen Webserver oder einen VPN-Gateway.

7.4 Einteilung der Angriffsvektoren in Risikoklassen

7.4.1 DoS

Die Konsequenzen einer einfachen DoS-Attacke auf einen Webserver oder einen VPN-Gateway eines Betreibers, sodass der entsprechende Service kurzzeitig unerreichbar ist, können als "gering" eingeschätzt werden.

Während der Scanning-Phase, welche wir im Rahmen dieses Forschungsprojekts bei gewissen Interview-Partnern durchgeführt haben (siehe Abschnitt 6.2), stellten wir fest, dass mindestens ein System anfällig auf DoS-Attacken ist (aufgrund teilweise veralteter Software mit entsprechenden, öffentlich publizierten Schwachstellen). Die angreifbaren Systeme lassen sich also mittels einfachen Analysemethoden (Scanning, Information Gathering) identifizieren. Bei mindestens einem System wäre es ausserdem sehr wahrscheinlich möglich, die Attacke mittels öffentlich verfügbarer Exploits durchzuführen. Die Eintrittswahrscheinlichkeit solcher Attacken ist demnach als "häufig" einzustufen.

Folgerungen:

- Konsequenzen: gering
- Wahrscheinlichkeit: häufig

7.4.2 DDoS

Auch bei einer DDoS-Attacke können realistischerweise nur Systeme angegriffen wer-

den, welche direkt "von aussen" erreichbar sind, also Webportale und evtl. Router und FTP-Server etc. Allerdings sind DDoS-Attacken schwieriger zu "stoppen" als "einfache" DoS-Attacken, wo das betroffene System üblicherweise einfach neu gestartet werden kann, um den Service wieder verfügbar zu machen. Der Angreifer kann bei DDoS-Attacken "steuern", wie lange ein entsprechendes System unerreichbar sein soll. Die Konsequenzen können deshalb als "spürbar" angesehen werden.

Im Vergleich zu einfachen DoS-Attacken benötigen DDoS-Attacken mehr Ressourcen. DDoS-Attacken werden typischerweise mit einem so genannten Botnet ausgeführt[94]. Dabei handelt es sich um eine grosse Anzahl vernetzter Rechner, die sich unter der Kontrolle eines Angreifers befinden. Um eine DDoS-Attacke auszuführen, können solche Botnetze beispielsweise bei kriminellen Organisationen gemietet werden (gegen ein entsprechendes Entgelt). Hier stellt sich allerdings die Frage, wie "lukrativ" so ein Angriff wirklich sein kann, insbesondere wenn man bedenkt, dass man relativ wenig Schaden anrichten kann. Die Eintrittswahrscheinlichkeit dürfte daher als "selten" eingestuft werden.

Folgerungen:

- Konsequenzen: spürbar
- Wahrscheinlichkeit: selten

7.4.3 Malware auf Webserver installieren

Malware, welche Besucher von Webportalen der VT-Betreiber angreift, dürfte für die VT-Betreiber vor allem einen gewissen Image-Schaden verursachen. Für den Betrieb der VT-Systeme dürften die entsprechenden Konsequenzen aber eher "unbedeutend" sein.

Gemäss dem Melani-Halbjahres-Bericht 2010 für das erste Halbjahr [MELANI, 2010] gibt es mehrere Möglichkeiten, um Malware auf einem Webserver zu installieren: Einerseits kann man die FTP-Logindaten stehlen, um an den Content der Webseite zu gelangen und diesen entsprechend zu modifizieren. Ausserdem können Schwachstellen im CMS oder von installierten Webapplikationen ausgenützt werden. Schliesslich kann man über Cross-Site Scripting in Foren und Gästebüchern den Besuchern schadhaften Code unterjubeln. Während der Scanning- und Information-Gathering-Phase (siehe Abschnitt 6.2) haben wir bei mindestens einem Webportal ein CMS-System gefunden. Dieses Webportal hatte ausserdem auch einen offenen FTP-Port. Uns ist es zwar nicht gelungen, mittels Password-Guessing die Passwörter für das CMS-Management-Portal und den FTP-Zugang herauszufinden, durch den Einsatz von mehr Ressourcen wäre das jedoch eventuell möglich. Allerdings stellt sich auch hier wieder die Frage, wie "lukrativ" so ein Angriff ist. Da die Seiten der VT-Betreiber verhältnismässig selten besucht werden, dürfte sich ein entsprechender Angriff nicht wirklich lohnen. Die Wahrscheinlichkeit kann daher als "selten" eingeschätzt werden.

Folgerungen:

- Konsequenzen: unbedeutend
- Wahrscheinlichkeit: selten

7.4.4 Webseiten verunstalten

Die Konsequenzen einer verunstalteten Website sind tendenziell als gering einzuschätzen.

Um eine Website verunstalten zu können, gibt es grundsätzlich verschiedene Möglichkeiten. Beispielsweise könnte man die ganze Domain "stehlen" und auf einen Host umleiten lassen, welcher unter der Kontrolle des Angreifers steht[95]. Eine andere Möglichkeit besteht darin, direkt den Hosting-Provider anzugreifen: Vielleicht wurden ja schwache

[94] http://de.wikipedia.org/wiki/Botnet
[95] http://www.darknet.org.uk/2006/09/domain-stealing-or-how-to-hijack-a-domain/

Passwörter gewählt etc. Je nachdem, wie gut die Systeme gesichert sind, kann der Angriff sehr schwierig auszuführen zu sein. Ausserdem muss auch beachtet werden, dass es für einen Angreifer kaum attraktiv sein dürfte, die Website eines VT-Betreibers zu verunstalten, da durch eine verunstaltete Website kein grosser Schaden entsteht und sich auch nicht viel Ruhm dafür ernten lässt (die Webseiten der VT-Betreiber dürften im Volk eher unbekannt und daher eher auch "schwach" frequentiert sein im Vergleich zu offiziellen Webseiten des Bundes (beispielsweise admin.ch oder bit.ch)). Deshalb ist davon auszugehen, dass solche Angriffe eher selten statt finden.

Folgerungen:

- Konsequenzen: gering
- Wahrscheinlichkeit: selten

7.4.5 Daten löschen/korrumpieren

Die Konsequenzen gelöschter bzw. korrumpierter Daten können durchaus als kritisch angesehen werden. Gemäss Interviewprotokoll sind die VT-Betreiber darauf angewiesen, dass die Daten unverfälscht beim BLS ankommen, da man sich ansonsten kein genaues Bild über die Verkehrssituation mehr machen kann und sich der Betrieb somit nicht mehr zuverlässig steuern lässt. Ausserdem kann es sein, dass Daten vor Gericht als Beweismittel verwendet werden müssen. Korrumpierte Daten können jedoch nicht mehr als rechtlich handfeste Beweismittel dienen.

Im Rahmen dieses Forschungsprojekts haben wir selbst ein Information Gathering und ein Scanning durchgeführt (siehe Abschnitte 6.1 und 6.2). Dabei ist es uns allerdings nicht gelungen, Systeme mittels Analysemethoden zu identifizieren, die potenziell sensitive Daten enthalten könnten. Auch konnten wir mittels Analysemethoden keine Systeme identifizieren, mit denen sich sensitive Daten für die VT-Systeme manipulieren liessen. Es ist daher davon auszugehen, dass die Systeme, wo die entsprechenden Daten abgespeichert werden, resp. wo die Daten erzeugt werden (z.B. Kameras, etc.), kaum "von aussen" erreichbar sind. Um die Attacke ausführen zu können, ist also mindestens physischer Zugang zum BLS nötig, evtl. sogar zu Feldsystemen. Wie "einfach" Daten gelöscht, bzw. korrumpiert werden können, hängt auch damit zusammen, ob eine Veränderung/Abfälschung der Daten detektiert werden kann (Integritätsschutz). Hier wissen wir aus Kapitel 2, dass die Protokolle, die im SCADA-Umfeld verwendet werden, kaum über Authentifizierung und Integritätsschutz verfügen. Gemäss Interviewprotokoll sind die Netze, wo solche Protokolle eingesetzt werden, jedoch immer autonom und gegen aussen abgeschottet. Es kann daher davon ausgegangen werden, dass solche Angriffe eher selten bis unwahrscheinlich sind.

Folgerungen:

- Konsequenzen: kritisch
- Wahrscheinlichkeit: selten

7.4.6 Sensitive Daten stehlen

Wenn sensitive Daten gestohlen werden, so kann das für die VT-Betreiber insbesondere datenschutzrechtliche Konsequenzen haben. Ausserdem dürfte auch mit einem gewissen Image-Schaden zu rechnen sein. Die Konsequenzen dürften also als "kritisch" eingeschätzt werden.

Im Rahmen der von uns durchgeführten Scanning-Phase konnten wir keine Systeme entdecken, welche sensitive Videodaten enthalten könnten. Es ist also eher davon auszugehen, dass solche Systeme nicht einfach "von aussen" zu erreichen sind. Um eine solche Attacke ausführen zu können ist also mindestens physischer Zugang zum BLS-Gebäude nötig. Hier könnte man noch argumentieren, dass ein verärgerter Mitarbeiter sich die entsprechenden Daten evtl. einfach besorgen könnte. Allerdings haben wir in Abschnitt 2.3 auch gesehen, dass Angriffe "von innen" nicht mehr allzu oft statt finden.

Die Eintrittswahrscheinlichkeit dürfte daher als "selten" eingeschätzt werden.

Folgerungen:

- Konsequenzen: kritisch
- Wahrscheinlichkeit: selten

7.4.7 Patches/OS-Updates/Malwareupdates

Patches, OS-Updates oder Malwareupdates könnten schlimmstenfalls die ganze Kommunikationsinfrastruktur lahm legen, wenn sich die neu eingespielte Software nicht gut mit dem System verträgt (siehe auch Abschnitt 2.2). Die Konsequenzen dürfen also durchaus als "kritisch" eingeschätzt werden.

Um Patches etc. einspielen zu können, benötigt man mindestens logisch Zugang zum System. Patches etc. werden meistens von internen Mitarbeitern oder externen Lieferanten etc. eingespielt. Gemäss Interviewprotokoll bieten einige Interviewpartner Remote-Zugänge für Lieferanten zur Wartung an (z.T. auch noch über "schlecht kontrollierbare" ISDN-Leitungen, die entweder nicht geloggt werden oder deren Logs noch nie überprüft wurden). Ein Interviewpartner hat explizit erwähnt, dass als grösstes Risiko für das System die durch die Systemlieferanten eingespielten Updates/Patches betrachtet werden, da dies häufig direkt - ohne vorgängige Tests - auf dem produktiven System erfolge. Dass kleinere Anpassungen der Software oft direkt vor Ort vorgenommen werden, ohne vorgängige Prüfungen, wird auch von einem zweiten Interviewpartner bestätigt. Ein weiterer Interviewpartner erwähnt, dass der Software-Updateprozess nicht einheitlich geregelt sei und die Lieferanten einiges an Spielraum hätten. Die Eintrittswahrscheinlichkeit dürfte daher als "gelegentlich" eingestuft werden.

Folgerungen:

- Konsequenzen: kritisch
- Wahrscheinlichkeit: gelegentlich

7.4.8 Logische/physische Bedienfehler

Logische oder physische Bedienfehler treten oft durch Unachtsamkeit bei der Arbeit mit den Systemen auf. Häufige Ursachen sind die Einführung neuer Funktionen ohne dass das Personal genügend geschult wurde oder Handlungen in Stresssituationen beim Eintreten von mehreren gleichzeitigen Ereignissen auf dem Strassennetz.

Die Fehler erfolgen durch Bedienung der Systeme vor Ort sei es in einer Betriebsleitzentrale oder einer Tunnelleitzentrale. Die Auswirkungen können den Normalbetrieb stören, jedoch sollten die Fehler rasch erkannt und behoben werden können, weshalb wir die Konsequenzen als "spürbar" einstufen. Weiterhin gehen wir davon aus, dass die Systeme das "Einstellen von Extremsituationen" durch entsprechende Sicherheitsmechanismen in der Systemlogik verhindern. Die Wahrscheinlichkeit stufen wir als "selten" ein da in den Interviews keine massgebenden Defizite in der Schulung der Anwender für die Bedienung der Systeme festgestellt werden konnten.

Folgerungen:

- Konsequenzen: spürbar
- Wahrscheinlichkeit: selten

7.4.9 Einstecken eines mit Malware verseuchten Geräts

Wenn ein Mitarbeiter ein verseuchtes Gerät bei einem System des BLS einsteckt, dürften die entstehenden Konsequenzen als "kritisch" einzuschätzen sein. Die Malware könnte das gesamte BLS lahm legen, so dass eine übergeordnete Steuerung kaum noch möglich wäre.

Vorfälle, dass Mitarbeiter durch Einstecken eines verseuchten Geräts ein ganzes Netz lahm legten, hat es in der Vergangenheit durchaus schon gegeben. Insbesondere wird auch gemunkelt, dass sich die Stuxnet-Malware beim Iranischen Atomkraftwerk Buschehr über einen USB-Stick ausgebreitet hat (siehe Abschnitt 2.3.1). Ein Interviewpartner hat angegeben, dass der Malwareschutz bei einem Netz, das nicht am Internet angeschlossen ist, alle zwei Wochen mittels USB-Stick aktualisiert wird. Die Gefahr, hier eine Malware unbemerkt einzuschleppen, ist relativ gross. In den BSA-Netzen wird ausserdem z.T. überhaupt kein Malwareschutz verwendet und die Betriebssystem-Software wurde eingefroren. Die eingesetzten Servicelaptops scheinen jedoch in den meisten Fällen einen Malwareschutz installiert zu haben. Mindestens ein Interviewpartner hat jedoch als potenzielle Schwachstelle den Zugriff von externen mobilen Geräten genannt. Die Gefahr liege hier in der nicht kontrollierbaren Nutzung der dafür vorgesehenen Laptops für andere Zwecke oder in der Verwendung von nicht vorgesehenen Endgeräten und der damit verbundenen Gefahr des Einschleusens von Malware in das System. Insgesamt kann die Wahrscheinlichkeit als "gelegentlich" eingeschätzt werden.

Folgerungen:

- Konsequenzen: kritisch
- Wahrscheinlichkeit: gelegentlich

7.4.10 Allgemeine Wartungsarbeiten am System

Bei den allgemeinen Wartungsarbeiten kann es vorkommen, dass neue Releases direkt auf einem Produktionssystem eingespielt werden. Dies ist in vielen Situationen notwendig, da keine Testsysteme zur Verfügung stehen. Die Auswirkungen auf die laufenden Systeme können nicht vorhergesagt werden. Im schlimmsten Fall können das Netzwerk oder zentrale Rechner lahmgelegt werden.

Diese Fehler treten beim direkten Zugriff auf die Systeme vor Ort oder Remote auf und können den laufenden Betrieb massiv beeinträchtigen. Die Auswirkungen werden rasch erkannt. Die Behebung solcher Fehler kann aber eine gewisse Zeit beanspruchen, weshalb wir die Konsequenzen als "kritisch" beurteilen. Die Eintrittswahrscheinlichkeit stufen wir als "gelegentlich" ein, insbesondere deshalb weil während den Interviews eine heterogene Situation in Bezug auf vorhandene Testsysteme identifiziert werden konnte.

Folgerungen:

- Konsequenzen: kritisch
- Wahrscheinlichkeit: gelegentlich

7.4.11 Strassenanlagen bedienen für arglistige Zwecke

Die Konsequenzen eines solchen Angriffs wären durchaus als "kritisch" einzustufen. Durch das Anzeigen falscher Verkehrssignale könnte ein vorübergehendes Verkehrschaos entstehen.

Während der Scanning-und-Enumeration-Phase, die wir im Rahmen dieses Forschungsprojektes durchgeführt haben, konnten wir keine Systeme entdecken, von welchen aus man VT-Systeme steuern könnte. Mindestens zwei Interviewpartner haben allerdings angegeben, dass es für den Pikett-Dienst einen Fernzugriff gibt: Vertrauenswürdige Personen können also per Remotezugang auf die entsprechenden Systeme zugreifen. Ein weiterer Interviewpartner plant eine DMZ, so dass sich die Pikett-Leute auch von zu Hause aus einloggen können. Verärgerte, entlassene Mitarbeiter, denen die Zugriffsberechtigungen nicht entzogen wurden, könnten sich theoretisch somit relativ einfach Zugang zu den Systemen verschaffen. Für externe Angreifer dürfte der Zugriff etwas schwieriger sein. Es ist uns während der Scanning-und-Enumeration-Phase nicht gelungen, per VPN in ein System einzudringen, wobei wir gesehen haben, dass bei einem Interviewpartner durchaus gewisse Schwachstellen vorhanden sind (siehe Abschnitt 6.2.3). Ein Interviewpartner hat ausserdem angegeben, dass die verwendeten ISDN-Zugänge nur

schlecht kontrolliert werden können. In Kombination mit mehr Ressourcen und Social Engineering könnte es theoretisch möglich sein, entsprechende Schwachstellen auszunutzen. Insgesamt dürfte die Eintrittswahrscheinlichkeit als "gelegentlich" eingeschätzt werden.

Folgerungen:

- Konsequenzen: kritisch
- Wahrscheinlichkeit: gelegentlich

7.4.12 Absichtliche Verbreitung von Malware

Die Konsequenzen sind als "kritisch" einzustufen, da die Malware theoretisch das ganze BLS lahm legen könnte.

IT-Vorfälle im Zusammenhang mit verärgerten Mitarbeitern hat es in der Vergangenheit durchaus schon gegeben. Wir haben allerdings auch gesehen, dass Angriffe heutzutage vermehrt von externer Seite statt finden (siehe Abschnitt 2.3). Verärgerte Mitarbeiter könnten die Malware beispielsweise über Remotezugänge verbreiten und ein verseuchtes Gerät lokal im BLS einstecken. Insgesamt dürfte die Eintrittswahrscheinlichkeit als "selten" einzuschätzen sein.

Folgerungen:

- Konsequenzen: kritisch
- Wahrscheinlichkeit: selten

7.4.13 Feldkomponenten umprogrammieren

Das Umprogrammieren von Feldkomponenten beansprucht eine gewisse Vorbereitung des Angriffs, da man sich Zugang auf die Systeme verschaffen muss. Sind diese Vorbedingungen erfüllt, kann man durch gezielte Angriffe Sensoren oder Aktoren so beeinflussen, dass die Systeme falsch reagieren (z.B. Falsche WTA-Texte oder Geschwindigkeitsanzeigen oder Fahrbahnnutzung) oder falsche Informationen (falsche Messwerte an Querschnitten) liefern. Die Konsequenzen stufen wir als "spürbar" ein, da der Einfluss auf den Betrieb bei solchen Angriffen in der Regel lokal begrenzt bleibt.

Die in den Interviews gesammelten Informationen zeigen, dass die Zugänge zu den Systemen mindestens schlüsselgesichert sind und das, aufgrund der hierarchischen Systemarchitektur, der vorliegende Angriff auf den unteren Ebenen nur geringen Schaden verursacht. Deshalb stufen wir die Eintrittswahrscheinlichkeit als "selten" ein.

Folgerungen:

- Konsequenzen: spürbar
- Wahrscheinlichkeit: selten

7.4.14 Feuer legen

Ein Angriff durch bewusstes Feuerlegen in einem Tunnel oder in einer Betriebsleitzentrale kann Systemkomponenten (z.B. Kommunikationsnetz) physisch zerstören und den Betrieb dadurch beträchtlich behindern (z.B. Sperrung Tunnel). Der Aufwand für solche Angriffe bleibt aber relativ hoch, da man sich vorab Zugang zu den Systemen verschaffen muss. Generell resultieren aus solchen Angriffen erhebliche Materielle Schäden sowie längere Betriebsunterbrüche. Aus diesen Gründen beurteilen wir die Konsequenzen als "kritisch".

Die Interviews haben gezeigt, dass die vorhandenen physischen Schutzmechanismen gegen den Brand einen hohen Standard aufweisen, so dass ein solcher Angriff als höchst unwahrscheinlich eingestuft wird. Falls sich die Brandschutzanlagen in einem ersten

Schritt desaktivieren lassen müsste die Eintrittswahrscheinlichkeit erhöht werden.

Folgerungen:

- Konsequenzen: kritisch
- Wahrscheinlichkeit: unwahrscheinlich

7.4.15 Physische Beschädigung von Feldkomponenten

Die physische Beschädigung von Feldkomponenten kann ohne grosse Vorbereitung in Form von Vandalismus vorgenommen werden. Dabei werden Sensoren und/oder Aktoren auf der Feldebene physisch zerstört. Der Einfluss auf den Betrieb bleibt lokal d.h. es sind davon vereinzelte Streckenabschnitte betroffen. Das Gesamtsystem oder das übergeordnete Verkehrsmanagement werden nur geringfügig tangiert. Die Wiederherstellung des Normalbetriebs kann eine gewisse Zeit in Anspruch nehmen, weshalb wir die Konsequenzen als "spürbar" beurteilen.

Aus den Interviews ist ersichtlich, dass sensible Feldkomponenten über entsprechende Massnahmen von physischen Zerstörungen geschützt sind (z.B. Komponenten der AGK), weniger sensible Komponenten eher nicht. Die Attraktivität eines Angriffs bleibt aber durch den relativ lokalen Einfluss auf den Betrieb beschränkt, daher stufen wir die Eintrittswahrscheinlichkeit als "selten" ein.

Folgerungen:

- Konsequenzen: spürbar
- Wahrscheinlichkeit: selten

7.4.16 Rechner mit Gewalt zerstören

Das bewusste Zerstören von Rechnern auf der Prozessleitebene oder auf der Gruppenleitebene ist mit einem gewissen Aufwand verbunden, da der Angreifer sich zuerst Zugang zu den Systemen vor Ort verschaffen muss. Der Einfluss einer physischen Zerstörung der Rechner kann, im Fall eines Prozessleitrechners, eine relativ grosse Auswirkung auf den Betrieb aufweisen und die Sicherheit der Verkehrsteilnehmer gefährden. Die Wiederherstellung des Normalbetriebs kann eine gewisse Zeit in Anspruch nehmen, da ganze Systeme ersetzt werden müssen. Aus diesen Gründen beurteilen wir die Konsequenzen als "kritisch" ein.

Die Informationen aus den Interviews zeigen, dass die Zugänge zu den Systemen in den Zentralen und auf der Gruppenleitebene schlüsselgesichert sind und das Schlüsselmanagement in der Regel systematisch gehandhabt wird. Dadurch sinkt die Wahrscheinlichkeit eines solchen Angriffs und wird von uns als "selten" eingestuft.

Folgerungen:

- Konsequenzen: kritisch
- Wahrscheinlichkeit: selten

7.4.17 Rechner herunterfahren/ausstecken

Ein Angriff, bei dem Rechner ausgeschaltet oder heruntergefahren werden, wirkt sich auf den Betrieb aus, da einzelne Steuerfunktionen nicht mehr lauffähig sind. Die Ursachen sollten in der Regel rasch erkannt werden können. Die Wiederherstellung des Normalbetriebs ist in einen vernünftigen Zeitraum möglich, weshalb wir die Konsequenzen als "spürbar" einstufen.

Für diesen Angriff ist wiederum eine Präsenz vor Ort notwendig. Die Eintrittswahrscheinlichkeit stufen wir als "selten" ein, insbesondere deshalb weil während den Interviews festgestellt wurde, dass die Zugänge mindestens schlüsselgesichert sind und eine rest-

riktive Schlüsselvergabe stattfindet. Die macht den vorliegenden Angriff eher unattraktiv.

Folgerungen:

- Konsequenzen: spürbar
- Wahrscheinlichkeit: selten

7.4.18 Kabel durchtrennen/ausstecken

Das Durchtrennen oder Ausstecken von Netzwerkkomponenten kann dazu führen, dass die Kommunikationsverbindung zu gewissen Anlagenkomponenten nicht mehr gewährleistet ist. Der Betrieb kann dadurch temporär gestört werden. Die Auswirkungen eines solchen Angriffs bleiben jedoch beschränkt, da eine Behebung in einem angemessenen Zeitraum erfolgen kann. Die Konsequenzen beurteilen wir deshalb als "spürbar".

Wie beim vorhergehenden Angriff ist auch hier der Zugang vor Ort eine Voraussetzung. Dieser ist jedoch, aufgrund der vorhandenen Zutrittsregelungen nicht ohne entsprechenden Aufwand zu erhalten, wodurch wir die Eintrittswahrscheinlichkeit als "selten" einstufen.

Folgerungen:

- Konsequenzen: spürbar
- Wahrscheinlichkeit: selten

7.4.19 Brandmeldesensor manipulieren

Die Manipulation eines Brandmeldesensors kann dazu führen, dass der Betrieb in einer Zentrale gestört wird in dem das Gebäude evakuiert wird oder dass ein Tunnel gesperrt wird. Weiterhin könnte durch das Auslösen von Sprinkleranlagen physischer Schaden bei den Rechnern entstehen. Der Aufwand für einen solchen Angriff bleibt jedoch relativ hoch, da man sich Zugang zu den Gebäuden verschaffen muss und wir deshalb die Konsequenzen als "spürbar" beurteilen.

Aus den geführten Interviews ist ersichtlich, dass der Zutritt zu den Anlagen mindestens schlüsselgesichert ist und entsprechende organisatorische Vorkehrungen beim Schlüsselmanagement existieren. Dadurch sinkt die Angriffswahrscheinlichkeit und wird von uns als "selten" eingestuft.

Folgerungen:

- Konsequenzen: spürbar
- Wahrscheinlichkeit: selten

7.4.20 Videokameras ausstecken

Bei einem Angriff vor Ort in einer Tunnelleitzentrale, wo der Angreifer Videokameras aussteckt, geht es darum, eine Informationsquelle zur Überwachung und Beurteilung der Verkehrssituation lahm zu legen. Wir beurteilen die Konsequenzen als "spürbar", da bei solchen Angriffen nur einzelne Anlagen resp. Standorte betroffen sind. Der Betrieb wird dabei nur mässig gestört.

Dadurch, dass der Angreifer sich zuerst Zugang zu den Anlagen vor Ort verschaffen muss, ist ein gewisser Aufwand in der Vorbereitung notwendig. Die Interviews haben gezeigt, dass die aktuellen Anlagen über eine relativ gute physische Zugangssicherheit verfügen und somit der Zugang erschwert wird, weshalb wir die Eintrittswahrscheinlichkeit als "selten" einstufen.

Folgerungen:

- Konsequenzen: spürbar

- Wahrscheinlichkeit: selten

7.4.21 Unfall in BLZ-Gebäude

Bei einem Unfall in einer Betriebsleitzentrale (z.B. Wasserschaden) können Kernkomponenten auf der Prozesssteuerebene physisch zerstört werden. Dies kann den Betrieb der zentrale massiv über mehrere Tage resp. Wochen lahm legen, da dann keine übergeordnete Steuerung des Verkehrssystems mehr möglich ist. Nebst Image-Schaden ist auch mit kritischen Sicherheitslücken für die Verkehrsteilnehmer zu rechnen, weshalb wir die Konsequenzen als "kritisch" beurteilen.

Die heute existierenden Massnahmen zur Gewährleistung der physischen Sicherheit sind auf die möglichen Unfallszenarien (Brandschutz, Wasserschutz, Notstromaggregat) ausgelegt. Die Eintrittswahrscheinlichkeit wird deshalb als selten eingestuft.

Folgerungen:

- Konsequenzen: kritisch
- Wahrscheinlichkeit: selten

7.4.22 Server ausstecken/herunterfahren in Zentrale

Das bewusste Ausstecken oder Herunterfahren von Servern in einer Betriebsleitzentrale kann ohne weiteres zu punktuell katastrophalen Zuständen führen. So würde zum Beispiel ein solcher Angriff an einem hoch belasteten Feiertag oder Ferienwochenende zu massiven Störungen auf dem Verkehrsnetz führen. Auch in diesem Fall sind der Image-Schaden und die entstehenden Sicherheitslücken für den Verkehrsteilnehmer nicht zu unterschätzen. Aus diesen Gründen beurteilen wir die Konsequenzen als "kritisch".

Der Aufwand für einen solchen Angriff bleibt aber relativ hoch, da ein Zutritt vor Ort vorausgesetzt wird. Die Eintrittswahrscheinlichkeit stufen wir als "selten" ein, insbesondere auch weil aus den geführten Interviews hervorgeht, dass die Zutritte zu den Zentralen schlüsselgesichert und teilweise mit elektronischer Zutrittsregelung versehen sind.

Folgerungen:

- Konsequenzen: kritisch
- Wahrscheinlichkeit: selten

7.4.23 Backup-Tapes zerstören

Das Zerstören von Backup-Tapes durch einen Angreifer hat auf den täglichen Betrieb der BSA keinen Einfluss. Ein solcher Angriff erhält aber in Kombination mit anderen Angriffsvektoren, z.B. physische Zerstörung von Servern oder bei einem notwendigen Restore aufgrund einer Malwareattacke, eine höhere Bedeutung. Weiterhin sind die betroffenen Systeme eher von statischer Natur, mit wenigen Veränderungen über die Zeit. In den Interviews konnten diese Eigenschaften erkannt werden, welche sich auf das Operating auswirken: es werden nicht systematisch regelmässige Backups durchgeführt. Falls dann die Backup-Tapes nicht vorhanden sind, kann der Betrieb gestört werden, bis der Lieferant die Situation beheben kann, weshalb wir die Konsequenzen als "spürbar" einstufen.

Der Aufwand für einen solchen Angriff bleibt hoch, da ein Zutritt vor Ort vorausgesetzt wird. Die Eintrittswahrscheinlichkeit stufen wir als "selten" ein, da aus den geführten Interviews hervorgeht, dass die Zutritte zu den Zentralen schlüsselgesichert und teilweise mit elektronischer Zutrittsregelung versehen sind.

Folgerungen:

- Konsequenzen: spürbar
- Wahrscheinlichkeit: selten

7.4.24 Eine E-Mail versenden, die schädlichen Code enthält

Da die Malware theoretisch das ganze BLS lahm legen könnte, sind die Konsequenzen als "kritisch" einzustufen.

Die Vorbereitung für solche Attacken ist nicht allzu aufwändig: Alles was man braucht, sind ein paar E-Mail-Adressen. Wie wir in Kapitel 6.1 gesehen haben, ist es für einen Angreifer relativ einfach, sich die entsprechenden E-Mail-Adressen zu besorgen. Evtl. ist noch ein bisschen Social-Engineering nötig, um das Opfer dazu zu bringen, das verseuchte E-Mail-Attachment zu öffnen. Um die E-Mail vertrauenswürdiger aussehen zu lassen, könnte man beispielsweise noch die Absenderadresse fälschen (z.B. als Absenderadresse des zuständigen Administrators). Entsprechende Tools hierzu sind öffentlich verfügbar (z.B. Metasploit). Aus den Interviewprotokollen können wir entnehmen, dass zumindest gewisse Interviewpartner nicht auf allen Systemen des BLS einen Malwareschutz installiert und den Stand der Betriebssystemsoftware eingefroren haben. Ausserdem hat mindestens ein Interviewpartner angegeben, dass sich aufgrund der aktuell mangelhaften Separierung der Netze eine Malware schnell ausbreiten könnte. Allerdings haben die meisten Interviewpartner auch angegeben, dass die Betriebsnetze gut von den Firmennetzen getrennt seien. Es ist also fraglich, ob sich eine Malware wirklich bis zum BLS ausbreiten könnte. Die Eintrittswahrscheinlichkeit ist daher als "selten" einzustufen.

Folgerungen:

- Konsequenzen: kritisch
- Wahrscheinlichkeit: selten

7.5 Fazit

In den Kapiteln 7.4.1 bis 7.4.24 wurde die Zuteilung der "abschliessenden Angriffsvektoren" in verschiedene Risikoklassen diskutiert. Die Risikomatrix in Abbildung 14 stellt die entsprechenden Resultate visuell dar. Die Nummern in der Matrix referenzieren dabei jeweils die einzelnen "abschliessenden Angriffsvektoren" gemäss Kapitel 7.4.1 bis 7.4.24 (also 1 für DoS, 2 für DDoS, etc.).

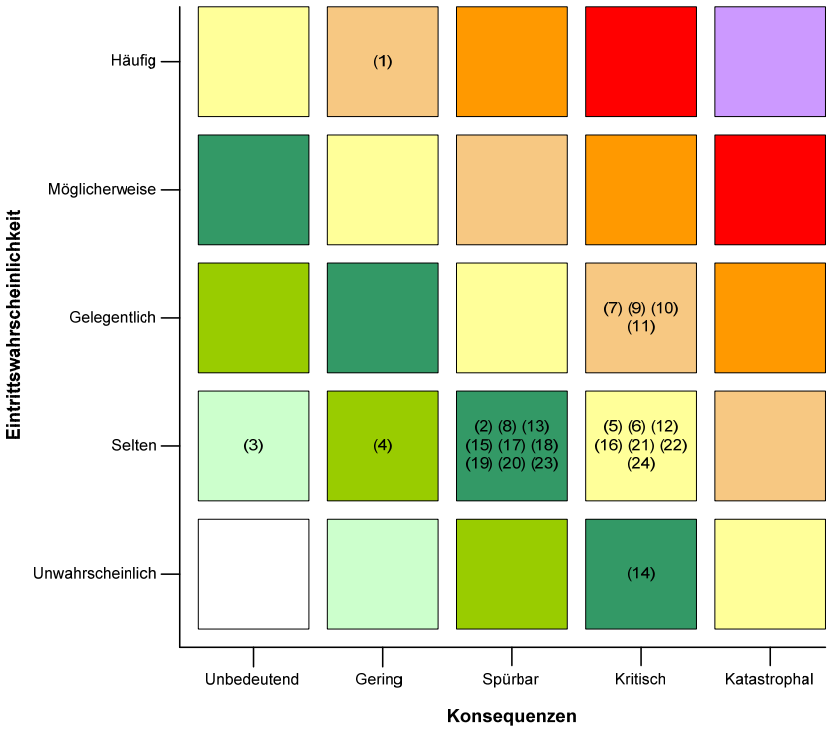


Abbildung 14: Risikomatrix

In der obenstehenden Risikomatrix ist deutlich zu erkennen, dass keine Angriffsvektoren mit katastrophalen Konsequenzen und hohen Eintrittswahrscheinlichkeiten vorhanden sind.

Allerdings sind doch einige Angriffsvektoren vorhanden, die sicherlich näher betrachtet werden müssen. Beispielsweise gibt es Angriffsvektoren, die kritische Konsequenzen haben und gelegentlich eintreten könnten:

- 7: Patches/OS-Updates/Malwareupdates
- 9: Einstecken eines mit Malware verseuchten Geräts
- 10: Allgemeine Wartungsarbeiten am System
- 11: Strassenanlagen bedienen für arglistige Zwecke

DoS Attacken (1) haben zwar nur geringe Konsequenzen, könnten theoretisch aber häufig auftreten.

Es sind ausserdem auch einige Angriffsvektoren vorhanden, die kritische Auswirkungen haben, jedoch selten vorkommen:

- 5: Daten löschen/korrumpieren
- 6: Sensitive Daten stehlen
- 12: Absichtliche Verbreitung von Malware
- 16: Rechner mit Gewalt zerstören
- 21: Unfall in BLZ-Gebäude
- 22: Server ausstecken/herunterfahren in Zentrale
- 24: Eine E-Mail versenden, die schädlichen Code enthält

Für die oben aufgelisteten Angriffsvektoren sollte untersucht werden, ob irgendwie die Eintrittswahrscheinlichkeiten oder gar die Konsequenzen verringert werden können. In den Kapiteln 8 und 10 werden Konzepte und Empfehlungen aufgezeigt, die für einen sichereren IT-Einsatz behilflich sein können.

8 Massnahmen zur Reduktion der erhöhten Risiken

In Kapitel 7 haben wir eine Risikoanalyse durchgeführt, wobei wir die Konsequenzen und Eintrittswahrscheinlichkeiten von jedem "abschliessenden Angriffsvektor" (siehe Kapitel 7.1) analysiert und beurteilt haben. Mit Hilfe der aus der Risikoanalyse entstandenen Risikomatrix in Kapitel 7.5 konnten wir dann einige "abschliessende Angriffsvektoren" identifizieren, deren Risiken erhöht sind und deshalb reduziert werden sollten (Angriffsvektoren, die "oberhalb" des grünen Bereichs in der Matrix zu liegen gekommen sind). In diesem Kapitel wollen wir für genau diese "erhöhten Risiken" einige Massnahmen auflisten, mit welchen die entsprechenden Risiken reduziert werden können. Dabei handelt es sich einerseits um Massnahmen, mit denen die Eintrittswahrscheinlichkeit eines Angriffsvektors reduziert werden kann, und, falls möglich, auch um Massnahmen, mit denen die Konsequenz eines Angriffsvektors reduziert werden kann[96]. Jeder "abschliessende Angriffsvektor", welcher gemäss Kapitel 7.5 genauer betrachtet werden sollte, wird dabei gesondert in einem Unterkapitel untersucht.

Als generelle Bemerkung sei hier noch erwähnt, dass wir hier bewusst von "erhöhten Risiken" sprechen und damit diejenigen Risiken bezeichnen, die in der Risikomatrix oberhalb des grünen Bereichs liegen und für welche wir entsprechend im Folgenden reduzierende Massnahmen vorschlagen. Wir vermeiden hier bewusst den Begriff "nicht tragbare" oder "nicht akzeptable Risiken", weil wir dem ASTRA bzw. den Gebietseinheiten den Entscheid, welche Risiken im konkreten Fall nun nicht tragbar sind, nicht abnehmen können.

8.1 Patches/OS-Updates/Malwareupdates

8.1.1 Einleitung

Dieser Angriffsvektor beschreibt Szenarien, in denen Patches und Malwareupdates durch Lieferenaten oder Mitarbeiter in produktive Systeme ohne vorgängige Tests eingespielt werden. Dadurch könnte theoretisch das ganze System lahm gelegt werden, wenn sich die neu eingespielte Software nicht gut mit dem System verträgt, weshalb die Konsequenzen dieses Angriffsvektors von uns als "kritisch" eingeschätzt wurden. Wir haben ausserdem gesehen, dass einige Interviewpartner Remote-Zugänge für Lieferanten zur Wartung anbieten. Zum Teil handelt es sich dabei auch noch um schlecht kontrollierbare ISDN-Zugänge, die entweder nicht geloggt werden oder deren Logs nie überprüft wurden. Ausserdem spielen Systemlieferanten Patches und Updates häufig direkt vor Ort, ohne vorgängige Tests, auf dem produktiven System ein. Des Weiteren sei der Softwareupdateprozess nicht einheitlich geregelt, was den Lieferanten einiges an Spielraum lasse. Wir haben daher die Eintrittswahrscheinlichkeit als "gelegentlich" eingeschätzt.

8.1.2 Massnahmen zur Verringerung des Risikos

Die folgenden Massnahmen basieren im Wesentlichen auf Dokumenten des National Infrastructure Co-Ordination Centre (NISCC) [NISCC, 2006], des National Institute of Standards and Technology (NIST) [NIST, 2005] [NIST, 2008], des Österreichischen Zentrums für sichere Informationstechnologie [A-SIT, 2007] und des US Department of Homeland Security [DHS, 2009].

- Einführen eines systematischen, dokumentierten Patch-Management-Prozesses. Ein Patch-Management-Pozess soll einer Unternehmung die Kontrolle darüber geben, wann und wie Patches, bzw. neue Software-Releases in eine produktive Umgebung

[96] Die Konsequenzen eines Angriffsvektors sind häufig fest vorgegeben und lassen sich daher kaum verändern, im Vergleich zur Eintrittswahrscheinlichkeit. So können zum Beispiel die Folgen eines Datendiebstahls nicht wirklich "reduziert" werden. Die Eintrittswahrscheinlichkeit für einen Datendiebstahl kann jedoch mit entsprechenden Sicherheitsmassnahmen (z.B. Verschlüsselung der Daten) sehr wohl reduziert werden.

eingespielt werden. Der Prozess sollte dabei folgende Elemente umfassen (Details sind der Literatur zu entnehmen [NISCC, 2006]):

- o Assessment and Inventory: Erfassen der Softwarekomponenten des operativen Systems, Erfassung möglicher Bedrohungen und Schwachstellen und Bestimmung, ob die Unternehmung darauf vorbereitet ist, neue Patches und Updates einzuspielen.
- o Patch Identification: Neue Patches und Softwareupdates untersuchen, bestimmen, ob sie für die Organisation relevant sind und feststellen, ob die Einspielung des Patches einem "normalen" Softwareupdate entspricht oder als Massnahme für einen Notfall dient.
- o Evaluation, Planning and Testing: Für jeden Patch soll bestimmt werden, ob er in das produktive System eingespielt werden soll, wie und wann der Patch eingespielt werden soll und ausserdem muss sichergestellt werden, dass der Patch vorgängig in einer realistischen Testumgebung geprüft wird um zu bestätigen, dass durch den Patch keine Systeme kompromittiert werden.
- o Deployment: Den Patch erfolgreich anwenden, wobei die Benutzer des Systems so wenig wie möglich gestört werden sollten.

- Es ist unbedingt notwendig zu überprüfen, ob sich der Patch gut mit dem System verträgt. Gerade bei SCADA-Systemen kann es sein, dass zum Teil ältere Software eingesetzt, welche von einem Patch gar nicht erst unterstützt wird.
- Patches sollten wenn möglich zu Randzeiten eingespielt werden.
- Patches sollten nur aus vertrauenswürdigen Quellen bezogen werden.
- Massnahmen zum Schutz von Remote-Zugängen:
  - o Jegliche Zugriffe sollten authentifiziert (am besten 2-Factor-Authentication) und authorisiert werden
  - o Alle möglichen Remote-Zugriffe auf das System sollten sauber dokumentiert werden.
  - o Remote-Zugriff sollte nur zu ganz bestimmten Zeitpunkten möglich sein und wenn es ausdrücklich vom Betreiber erlaubt wurde.
  - o Es sollten kryptographische Massnahmen verwendet werden, damit die Integrität und Vertraulichkeit der Daten sichergestellt sind.
  - o Die Remote-Zugänge sollten geloggt werden, um unerlaubte Zugriffe aufzudecken.

8.1.3 Einfluss der Massnahmen auf das Risiko, Kosten und operationelle Abläufe

Mit den obenstehenden Massnahmen dürfte die Eintrittswahrscheinlichkeit auf "selten" reduziert werden. Wichtig ist hier vor allem, dass die Unternehmung die volle Kontrolle darüber besitzt, wann durch wen welcher Patch eingespielt werden soll. Dadurch wird verhindert, dass Patches "willkürlich" von Lieferanten oder Mitarbeitern eingespielt werden. Wenn ausserdem alle Patches vor dem Einspielen in das produktive System vorgängig auf einem Testsystem überprüft werden, so dürfte es kaum mehr möglich sein, dass ein Patch ein System lahm legt. Die Konsequenzen können mit den obenstehenden Massnahmen nicht reduziert werden. Die Kosten dürften nicht allzu hoch sein. Das Aufziehen eines ganzen Patch-Management-Prozesses dürfte vor allem zu Beginn ein paar Kosten verursachen. Wenn der Prozess jedoch erst einmal etabliert ist, dürften kaum mehr Kosten anfallen. Die operationellen Abläufe müssen entsprechend an den Patch-Management-Prozess angepasst werden.

Folgerungen:

- Konsequenzen: kritisch (unverändert)
- Wahrscheinlichkeit: vorher: gelegentlich → neu: selten

8.2 Einstecken eines mit Malware verseuchten Geräts

8.2.1 Einleitung

Dieser Angriffsvektor beschreibt Szenarien, in denen interne Mitarbeiter unwissend eine

mit Malware verseuchten Laptop oder USB-Stick in ein System einstecken, wobei sich die Malware ausbreiten und theoretisch das ganze System lahm legen könnte. Die Konsequenzen dieses Angriffsvektors haben wir in Kapitel 7 deshalb auch als "kritisch" eingeschätzt. In Kapitel 2 haben wir ausserdem gesehen, dass es in der Vergangenheit durchaus schon Vorfälle gegeben hat, wo Mitarbeiter aus Versehen oder Unachtsamkeit Systeme lahm gelegt haben, weil sie ein verseuchtes Gerät in ein System eingeführt haben. Die Eintrittswahrscheinlichkeit wurde daher als "gelegentlich" festgelegt.

8.2.2 Massnahmen zur Verringerung des Risikos

Die folgenden Massnahmen basieren grösstenteils auf Dokumenten des BITKOM [BITKOM b], des US Department of Homeland Security [DHS, 2009], des Österreichischen Zentrums für sichere Informationstechnologie [A-SIT, 2007] und des National Institute of Standards and Technology [NIST, 2008].

- Sensibilisieren der Mitarbeiter: Die Mitarbeiter müssen auf das Problem sensibilisiert werden um mögliche Gefahren zu erkennen.
- Installation eines Malwareschutzes und einer Personal Firewall auf Laptops. Der Malwareschutz sollte dabei laufend, am besten täglich, aktualisiert werden.
- "Fremde" Dateien und Datenträger, die in ein System eingeführt werden, sollten vor der Einführung mit einem Malwareschutz überprüft werden.
- Eine Unternehmensrichtlinie sollte Regeln zur Nutzung der Antimalwaresoftware festlegen und vorschreiben, was zu tun ist, wenn eine Malware gefunden wurde.
- Separierung verschiedener Netzwerkebenen, so dass eine ausgebrochene Malware zumindest nicht das gesamte Netz lahm legen kann. Details, wie eine sichere Netzwerk-Architektur (Defense-in-Depth-Architektur) aufgebaut werden kann, finden sich in der Literatur [NIST, 2008].
- Wo überall möglich, sollte auch im BLS ein Malwareschutz eingesetzt werden. Am besten werden die Malwareupdates dabei von einem zentralen Server aus administriert.

8.2.3 Einfluss der Massnahmen auf das Risiko, Kosten und operationelle Abläufe

Mit den obenstehenden Massnahmen dürfte die Eintrittswahrscheinlichkeit deutlich reduziert werden (auf "selten"). Wichtig ist insbesondere, dass sich alle Mitarbeiter der "Gefahr des Einschleusens von Malware" bewusst sind. Wenn die Malwaredefinitionen ständig aktuell gehalten werden und Daten vor dem Einführen in ein System mit einem Malwarescanner analysiert werden, dürfte es kaum noch möglich sein, dass Malware durch Einstecken mobiler Datenträger oder Laptops in das System eingeschleust wird. Die Kosten für die Massnahmen dürften ziemlich geringfügig sein. Die meisten Interviewpartner verwenden bereits Antimalwaresoftware gemäss Interviewprotokoll. Sicherlich muss ein gewisser Aufwand betrieben werden, um die Mitarbeiter zu sensibilisieren. Eventuell braucht es auch noch eine Anpassung der operationellen Abläufe, so dass sichergestellt wird, dass die Malwaredefinitionen täglich aktualisiert werden. Die Konsequenzen bleiben durch die obenstehenden Massnahmen unverändert.

Folgerungen:

- Konsequenzen: kritisch (unverändert)
- Wahrscheinlichkeit: vorher: gelegentlich → neu: selten

8.3 Allgemeine Wartungsarbeiten am System

8.3.1 Einleitung

Dieser Angriffsvektor beschreibt Szenarien, in denen an einem produktiven System Wartungsarbeiten durch eigenes oder Fremdpersonal durchgeführt werden, die zu einem Ausfall des Systems führen. Solche Angriffe können den Betrieb massiv beeinträchtigen, da man meist ungenügend auf die Ereignisse vorbereitet ist. Die Konsequenzen dieses Angriffsvektors haben wir in Kapitel 7 deshalb als "kritisch" eingeschätzt. Dadurch, dass

an einigen Standorten zurzeit keine Testsysteme vorhanden sind haben wir die Eintrittswahrscheinlichkeit als "gelegentlich" eingestuft.

8.3.2 Massnahmen zur Verringerung des Risikos

Die folgenden Massnahmen basieren zum Teil auf dem Dokument der BSG [BSG, 2008].

- Klare Trennung zwischen Produktivsystem und Test-/Entwicklungssystem realisieren.
- Definieren von klaren Verfahren beim Einsatz neuer Software, insbesondere:
  - Jede neue Software wird einem Softwarefreigabeverfahren unterzogen
  - Jedes Produkt wird einer Eingangskontrolle unterzogen
  - Es dürfen nur freigegebene Software auf den Systemen laufen
- Einbinden der Wartungsarbeiten in das Qualitätsmanagement. Es ist darauf zu achten, dass die Wartungsaktivitäten als Teil der Qualitätssicherungsverfahren der Betriebsleitzentralen dokumentiert und gelebt werden.
- Erfolgsfaktoren für die Sicherstellung einer hohen Qualität bei der Softwareentwicklung definieren, insbesondere:
  - Klare und messbare Anforderungen definieren
  - Software laufend auf Vollständigkeit und Korrektheit testen
  - Erstellen von Testplänen und Prioritäten auf geschäftskritische Komponenten setzen
- Definieren von klaren Verfahren beim Patch-Management: Sicherheitsupdates oder Patches unterstehen den gleichen Verfahren, wie für neue Software und müssen vor dem Einspielen in das Produktivsystem getestet und freigegeben sein.
- Bei Soft- und Hardwareänderungen ist ein umfassendes Changemanagement zu führen in dem alle Änderungen auf kontrollierte Weise erfolgen. Dabei ist auf eine vollständige und korrekte Dokumentation der Änderungen zu achten.

8.3.3 Einfluss der Massnahmen auf das Risiko, Kosten und operationelle Abläufe

Mit den obenstehenden Massnahmen dürfte die Wahrscheinlichkeit auf "selten" reduziert werden. Die Kosten sind, je nach Massnahme, unterschiedlich. Für die organisatorischen Massnahmen wie diejenigen der Qualitätssicherung oder des Patch-Managements sind geringe Kosten zu erwarten. Jedoch sind für den Aufbau von Testsystemen in den Betriebsleitzentralen eher hohe Kosten zu erwarten. Auf die operationellen Abläufe haben die organisatorischen Massnahmen einen mässigen Einfluss, da in der Regel bereits ähnliche Verfahren im Einsatz sind. Die Konsequenzen bleiben mit den oben stehenden Massnahmen unverändert.

Folgerungen:

- Konsequenzen: kritisch (unverändert)
- Wahrscheinlichkeit: gelegentlich → neu: selten

8.4 Strassenanlagen bedienen für arglistige Zwecke

8.4.1 Einleitung

Dieser Angriffsvektor umschreibt Szenarien, bei denen Strassenanlagen für arglistige Zwecke bedient werden. Beispielsweise könnte absichtlich ein Tunnelrot ausgelöst oder "falsche" Wechseltextanzeigen eingespiesen werden, was zu einem kurzfristigen Verkehrschaos führen könnte. Wir haben die Konsequenzen deshalb als "kritisch" eingestuft. Wir haben ausserdem gesehen, dass für Pikett-Leute bereits Fernzugriffe möglich oder geplant sind, wodurch verärgerte, entlassene Mitarbeiter relativ einfach Zugang verschaffen könnten, wenn ihnen der Zugriff nicht richtig entzogen wurde. Während dem Scanning haben wir ausserdem festgestellt, dass bei einem Interviewparter gewisse Schwachstellen im VPN-System vorhanden sind. Des Weiteren sind zum Teil noch ISDN-Zugänge vorhanden, die nur schlecht kontrollierbar seien. Wir haben die Eintrittswahrscheinlichkeit deshalb als "gelegentlich" eingeschätzt.

8.4.2 Massnahmen zur Verringerung des Risikos

Die folgenden Massnahmen basieren auf einem Dokument des US Department of Homeland Security (DHS) [DHS, 2009], auf einem Dokument des Zentrums für sichere Informationstechnologie (A-SIT) [A-SIT, 2007] und einem Dokument des CPNI [CPNI, 2007].

- Um Risiken mit Mitarbeitern zu vermindern, sollte ein aktives "Personnel-Security-Management" betrieben werden. Dazu müssen alle Phasen der Anstellung eines Mitarbeiters betrachtet werden, inkl. Einstellung in das Unternehmen und Verlassen des Unternehmens.
  - Vor der Anstellung sollte ein Personen-Screening durchgeführt werden für alle Personen, die Zugang zu kritischen Anlagen erhalten sollen (beispielsweise frühere Anstellungen, Leumund, Qualifikationen, etc.).
  - Mitarbeiter sollen dazu verpflichtet werden (durch eine Unterschrift), sich an bestehende Gesetze und Sicherheitsrichtlinien des Unternehmens zu halten.
  - Für die verschiedenen Stellen in einem Unternehmen sollten detaillierte Stellenbeschreibungen existieren mit einer entsprechenden Einschätzung des "Risikogehalts" der Stelle.
  - Auch während der Anstellung sollten Mitarbeiter "im Auge behalten" werden. Allerdings gilt es dabei bestehende Gesetze (z.B. Datenschutz) und Normen (moralische Grundsätze) zu beachten.
  - Jeder Angestellte soll nur jene Zugangsrechte erhalten (logisch und physisch), die er absolut benötigt, um seine Arbeit gemäss Stellenbeschreibung auszuführen (Principle of Least Privilege).
  - Wenn ein Mitarbeiter das Unternehmen verlässt, sollten die entsprechenden Zugangsrechte (sowohl physisch und logisch), Passwörter, Schlüssel, Badges, etc. entfernt/dem Mitarbeiter abgenommen werden.
  - Wenn ein Mitarbeiter einen neuen Posten in der Unternehmung antritt, sollten die Zugangsberechtigungen entsprechend angepasst werden.
- Sicherheitsmassnahmen bezüglich Remote-Zugänge (siehe 8.1.2)

8.4.3 Einfluss der Massnahmen auf das Risiko, Kosten und operationelle Abläufe

Mit den obenstehenden Massnahmen dürfte die Eintrittswahrscheinlichkeit auf "selten" reduziert werden. Wichtig ist hier insbesondere, dass ein solides Personnel-Management betrieben wird. So genannte Insider (Mitarbeiter, die ihre legitimen Zugriffsrechte im Unternehmen für arglistige Zwecke ausnützen) stellen nun Mal eine grosse Gefahr für die Unternehmen dar (siehe auch Kapitel 2). Die Unternehmen müssen sich daher vor den entsprechenden Gefahren durch Insider schützen. Die Konsequenzen werden durch die obenstehenden Massnahmen nicht beeinflusst. Die Kosten für die Personnel-Management-Massnahmen dürften sich in einem vertretbaren Rahmen bewegen. Die operationellen Abläufe bei der Einstellung und Entlassung eines Mitarbeiters oder bei internen Mutationen müssen entsprechend überprüft und bei Bedarf gemäss obenstehenden Massnahmen angepasst werden.

Folgerungen:

- Konsequenzen: kritisch (unverändert)
- Wahrscheinlichkeit: vorher: gelegentlich → neu: selten

8.5 DoS-Attacken

8.5.1 Einleitung

Dieser Angriffsvektor beschreibt Szenarien, in denen externe Angreifer mittels DoS-Attacken einen Webserver oder VPN-Gateway kurzzeitig zum Erliegen bringen. Da die Komponenten, welche durch solche Angriffe betroffen sein können, nicht kritisch sind für den Betrieb der VT-Anlagen und die betroffenen Komponenten ausserdem mit geringem Aufwand wiederhergestellt werden können, haben wir die Konsequenzen als "gering"

eingeschätzt. Andererseits haben wir bei mindestens einem Interviewpartner auch gewisse Schwachstellen aufgrund teilweise veralteter Software in einem VPN-Gateway entdeckt, die sehr wahrscheinlich mittels öffentlich verfügbarer Exploits ausgenützt werden könnten. Die Eintrittswahrscheinlichkeit wurde daher auf "häufig" eingeschätzt.

8.5.2 Massnahmen zur Verringerung des Risikos

Die folgenden Massnahmen basieren grösstenteils auf Dokumenten des US Department of Homeland Security [DHS, 2009] und des National Institute of Standards and Technology [NIST, 2008].

- Die Softwareversionen der eingesetzten Software immer auf dem aktuellsten Stand halten, insbesondere bei nach aussen exponierten Systemen.
- Einsatz geeigneter Netzwerkdevices, um verdächtige Pakete, die für einen DoS-Angriff verwendet werden könnten, herauszufiltern (Beispielsweise Firewalls, IDS, IPS, etc.).

8.5.3 Einfluss der Massnahmen auf das Risiko, Kosten und operationelle Abläufe

Mit den oben eingesetzten Massnahmen dürfte die Eintrittswahrscheinlichkeit auf "selten" reduziert werden. Die Konsequenzen sind weiterhin unverändert als "gering" einzustufen. Die Kosten dürften ziemlich gering sein. Operationelle Abläufe dürften kaum beeinflusst werden. Als mögliches Risiko könnte man aufführen, dass sich evtl. neu eingespielte Software nicht gut mit der bestehenden Software verträgt. Um entsprechende Risiken zu minimieren, sollten die Massnahmen, die in Abschnitt 8.1.2 zum Thema Patch-Management aufgeführt werden, beachtet werden.

Folgerungen:

- Konsequenzen: gering (unverändert)
- Wahrscheinlichkeit: vorher: häufig → neu: selten

8.6 Daten löschen/korrumpieren

8.6.1 Einleitung

Dieser Angriffsvektor beschreibt Szenarien, in denen sensitive Daten, beispielsweise Beweisbilder oder -videos, gelöscht werden. Die Interviewpartner sind darauf angewiesen, dass die Daten unverfälscht beim BLS ankommen (da man sich ansonsten kein genaues Bild über die Verkehrssituation mehr machen kann und sich der Betrieb nicht mehr zuverlässig steuern lässt). Ausserdem können korrumpierte Beweisbilder/-videos vor Gericht nicht mehr als handfeste Beweismittel verwendet werden. Die Konsequenzen wurden daher als "kritisch" eingestuft. Wir sind ausserdem zum Schluss gekommen, dass solche Angriffe "selten" zum Erfolg führen dürften, u.a. auch deshalb, weil wir während unserer Scanning-Phase keine Rechner ausfindig machen konnten, die wirklich sensitive Daten enthalten könnten.

8.6.2 Massnahmen zur Verringerung des Risikos

Die folgenden Massnahmen basieren im Wesentlichen auf Dokumenten des US Department of Homeland Security [DHS, 2009], des National Institute of Technology [NIST, 2008] und des Österreichischen Zentrums für sichere Informationstechnologie [A-SIT, 2007]

- Kritische Daten wie Beweisbilder und -videos, die vor Gericht verwendet werden sollen, sollten doppelt gesichert werden. Am besten erstellt man regelmässig Backups und lagert diese an einem gesicherten Ort (mit physischem Zugangsschutz) ausserhalb des Standortes. Eine Verschlüsselung der Daten ergibt zusätzliche Sicherheit.
- Nur ausgewähltes Personal sollte Zugang zu sensitiven Daten haben. Das soll durch entsprechende Authentisierungsmechansimen sichergestellt werden.

- Massnahmen bezüglich Personnel-Security-Management (siehe 8.4.2).
- Malwareschutz. Die Malwaredefinitionen sollten dabei regelmässig (am besten täglich) aktualisiert werden. Wechseldatenträger sollten dabei mit besonderer Vorsicht gehandhabt werden (siehe auch 8.2.2)
- Verwendung von IDS/IPS (Intrusion Detection/Prevention Systemen), um Angriffe zu erkennen, bzw. zu vermeiden.
- Sensitive Daten sollten wenn immer möglich über verschlüsselte, integritätsgesicherte Kanäle übertragen werden.
- Ein gutes Patch-Management sollte gehandhabt werden (siehe auch 8.1.2)

8.6.3 Einfluss der Massnahmen auf das Risiko, Kosten und operationelle Abläufe

Auch mit den obenstehenden Massnahmen kann die Wahrscheinlichkeit eines erfolgreichen Angriffs nicht vollständig ausgeräumt werden. Allerdings dürften die Konsequenzen auf "spürbar" reduziert werden. Wichtig ist hier sicher, dass Daten, die korrekt beim BLS ankommen sollten, über integritätsgesicherte Kanäle übertragen werden. Ausserdem sollten sensitive Beweisdaten doppelt gesichert werden. So bleiben die Daten mit grosser Wahrscheinlichkeit auch im Falle eines Angriffs erhalten. Die Kosten dürften in einem überschaubaren Rahmen bleiben. Gemäss Interviewprotokoll werden Backups teilweise bereits eingesetzt, ebenso wie Antimalwaresoftware.

Folgerungen:

- Konsequenzen: vorher: kritisch → neu: spürbar
- Wahrscheinlichkeit: selten (unverändert)

8.7 Sensitive Daten stehlen

8.7.1 Einleitung

Dieser Angriffsvektor beschreibt Szenarien, in denen den VT-Betreiber sensitive Daten entwendet werden. Gestohlene, sensitive Daten können für die VT-Betreiber insbesondere datenschutzrechtliche Konsequenzen haben und ausserdem Image-Schäden verursachen. Deshalb haben wir die Konsequenzen dieses Angriffsvektors auch als "kritisch" eingeschätzt. Die Wahrscheinlichkeit eines erfolgreichen Angriffs wurde als "selten" eingestuft, u.a. auch deshalb, weil man "von Aussen" kaum an wirklich sensitive Daten herankommen dürfte (was wir auch während unserer Scanning-Phase gesehen haben).

8.7.2 Massnahmen zur Verringerung des Risikos

Die folgenden Massnahmen basieren hauptsächlich auf einem Dokument des US Department of Homeland Security (DHS) [DHS, 2009].

- Personnel-Security-Management-Massnahmen (siehe 8.4.2).
- Zugangsschutz (siehe 8.6.2)
- Bei Wechseldatenträgern, die sensitive Daten enthalten (beispielsweise CDs/DVDs), ist spezielle Vorsicht geboten. Die Daten sollten auf jeden Fall verschlüsselt werden. Es muss auf jeden Fall sichergestellt werden, dass die Daten nicht in die Hände Unbefugter gelangen.
- Vor dem Entsorgen von Datenträgern, auf denen sensitive Daten geführt wurden, müssen die Datenträger zuerst "sicher" gelöscht werden. Dazu sollten spezielle Löschalgorithmen verwendet werden (ein Wikipediaartikel gibt hier einen guten Überblick[97]).
- Informationslecks sollten auf jeden Fall vermieden werden. Es muss sichergestellt werden, dass nur die allernötigsten Informationen an die Öffentlichkeit gelangen. Besondere Aufmerksamkeit gilt:
  - Wechseldatenträgern

[97] http://en.wikipedia.org/wiki/Data_remanence

- o Offizielle Dokumente
- o Remote Access

8.7.3 Einfluss der Massnahmen auf das Risiko, Kosten und operationelle Abläufe

Eine gewisse Restwahrscheinlichkeit, dass sensitive Daten gestohlen werden können, bleibt leider immer - auch die obenstehenden Massnahmen können die Eintrittswahrscheinlichkeiten nicht weiter reduzieren. Auch die Konsequenzen dürften mit den obenstehenden Massnahmen kaum verändert werden. Trotzdem lohnt es sich, obenstehende Massnahmen zur Kenntnis zu nehmen als Good-Practice-Guidelines im Umgang mit sensitiven Daten. Die Kosten dürften gering sein. Die operationellen Abläufe für die Entsorgung von Datenträgern sollten überprüft und bei Bedarf angepasst werden.

Folgerungen:

- Konsequenzen: kritisch (unverändert)
- Wahrscheinlichkeit: selten (unverändert)

8.8 Absichtliche Verbreitung von Malware

8.8.1 Einleitung

Dieser Angriffsvektor beschreibt Szenarien, in denen verärgerte Mitarbeiter absichtlich Malware im System verbreiten, beispielsweise durch das Einstecken versäuchter Laptops oder USB-Sticks. Die dadurch verbreitete Malware könnte theoretisch das ganze BLS lahm legen, weshalb wir die Konsequenzen dieses Angriffsvektors auch als "kritisch" eingestuft haben. Die Eintrittswahrscheinlichkeit wurde von uns als "selten" eingestuft (IT-Vorfälle mit verärgerten Mitarbeitern hat es in der Vergangenheit zwar durchaus schon gegeben, allerdings werden externe Angriffe heutzutage vermehrt "von aussen" ausgeführt).

8.8.2 Massnahmen zur Verringerung des Risikos

- Personnel-Security-Management (siehe 8.4.2)
- Einsatz von Antimalwaresoftware (siehe 8.2.2)
- Separierung verschiedener Netzbereiche (siehe 8.2.2)

8.8.3 Einfluss der Massnahmen auf das Risiko, Kosten und operationelle Abläufe

Die Eintrittswahrscheinlichkeit bleibt mit den obenstehenden Massnahmen unverändert auf "selten". Die Konsequenzen können jedoch auf "spürbar" reduziert werden, wenn entsprechende Massnahmen bezüglich Einsatz von Antimalwaresoftware und Separierung der Netze ins Auge gefasst werden. Die Kosten dürften dabei nicht allzu hoch sein.

Folgerungen:

- Konsequenzen: vorher: kritisch → neu: spürbar
- Wahrscheinlichkeit: selten (unverändert)

8.9 Rechner mit Gewalt zerstören

8.9.1 Einleitung

Dieser Angriffsvektor beschreibt Szenarien, in denen Angreifer in eine Betriebsleitzentrale oder eine Tunnelleitzentrale eindringen um dort bewusst Rechner physisch zu zerstören. Solche Angriffe können das ganze System lahm legen. Die Konsequenzen dieses Angriffsvektors haben wir in Kapitel 7 deshalb als "kritisch" eingeschätzt. Dadurch dass die Zugänge zu den Systemen schlüsselgesichert oder zum Teil überwacht sind haben wir die Eintrittswahrscheinlichkeit als "selten" festgelegt.

8.9.2 Massnahmen zur Verringerung des Risikos

Die folgenden Massnahmen basieren zum Teil auf dem Dokument der BSG [BSG, 2008].

- Einhalten der Vorgaben des Bundesamtes für Bauten und Logistik und des Bundessicherheitsdienstes für den physischen Schutz.
- Redundante Auslegung kritischer Systemkomponenten wie das Kommunikationsnetzwerk, die Server oder die Backups der Systeme und Daten. Dabei kann bei einem physischen Angriff der Betrieb auf die redundanten Komponenten umgestellt werden. Es ist dabei zu achten, dass diese geographisch getrennt vorgehalten werden.
- Erstellen eines Disaster-Recovery-Plans für die Wiederherstellung der Systeme und der Einrichtungen. Dieser umfasst insbesondere die Vermeidung von Single Point of Failure in der Stromversorgung, der Hardware, der Telekommunikation und dem Gebäude.
- In den Wartungsverträgen mit den Systemlieferanten immer darauf achten, dass der Lieferant im Ernstfall Ersatzteile oder ganze Systeme liefern kann.
- Sensibilisieren der Mitarbeiter bezüglich Social-Engineering Angriffe. Dies kann über gezielte Schulungen und die Herausgabe einer entsprechenden Policy erreicht werden.
- Ab dem Zeitpunkt einer Kündigung eines Mitarbeiters einer Betriebsleitzentrale oder eines Lieferanten ist dieser beim Zugang zu den Systemen zu überwachen. Gleichzeitig sollten die Passwörter, zu denen der gekündigte Mitarbeiter Zugang gehabt hat geändert werden.

8.9.3 Einfluss der Massnahmen auf das Risiko, Kosten und operationelle Abläufe

Mit den obenstehenden Massnahmen dürften die Konsequenzen auf "spürbar" reduziert werden. Dadurch dass aus Wirtschaftlichkeitsüberlegungen nicht alle Komponenten redundant vorgehalten werden können, kann es trotzdem bei einem Angriff zu vereinzelten Ausfällen kommen. Die Kosten für die Massnahmen sind unterschiedlich. Für die organisatorischen Massnahmen wie der Disaster-Recovery-Plan oder die Schulungen der Mitarbeiter sind geringe Kosten zu erwarten. Weit höher belaufen sich die Kosten für evtl. erforderliche bauliche Massnahmen, die redundante Auslegung von Systemkomponenten oder die Wartungsverträge mit den Lieferanten. Auf die operationellen Abläufe haben die Massnahmen lediglich bei der Einhaltung der Policy betreffend Social-Engineering und bei Kündigung einen Mitarbeiters einen Einfluss. Es muss sichergestellt sein dass diese Vorgaben im täglichen Betrieb eingehalten werden. Die Eintrittswahrscheinlichkeit bleibt durch die obenstehenden Massnahmen unverändert.

Folgerungen:

- Konsequenzen: vorher: kritisch → neu: spürbar
- Wahrscheinlichkeit: selten (unverändert)

8.10 Unfall in BLZ-Gebäude

8.10.1 Einleitung

Dieser Angriffsvektor umfasst die Szenarien, in denen die Systeme einer Betriebsleitzentrale durch einen Brand, einen Wasserschaden o.ä. zerstört werden. Solche Ereignisse können den Betrieb über einen längeren Zeitraum lahm legen. Die Konsequenzen dieses Angriffsvektors haben wir in Kapitel 7 deshalb als "kritisch" eingeschätzt. Dadurch dass die Betriebsleitzentralen bereits heute in der Mehrheit über entsprechende Schutzmassnahmen verfügen haben wir die Eintrittswahrscheinlichkeit als "selten" beurteilt.

8.10.2 Massnahmen zur Verringerung des Risikos

Zur Verringerung des Risikos werden folgende Massnahmen vorgeschlagen. Diese basieren teilweise auf dem Dokument der BSG [BSG, 2008].

- Einhalten der Vorgaben des Bundesamtes für Bauten und Logistik und den Bundessicherheitsdienstes für den physischen Schutz.
- Aufbauen eines "IT-Service Continuity Management" (ITSCM) mit dem Ziel nach einem Schadensereignis eine unterbruchsfreie Weiterführung des IT-Betriebs zu gewährleisten. Dies beinhaltet:
  - die Erstellung eines IT Continuity Plan mit präventiven Vorbereitungen und Schutzvorkehrungen sowie Bildung von Redundanzen
  - ein Contingency Plan mit der Beschreibung, wie die Zeit mit reduzierten Ressourcen überbrückt wird
  - ein Disaster-Recovery-Plan für die Wiederherstellung der Systeme und der Einrichtungen (siehe dazu 8.9.2)
- Erstellen von Hilfsmittel für eine erfolgreiche Kommunikation in Notfällen. Diese bestehen aus einem Notfallplan der beschreibt in welcher Situation wer Verantwortlich ist, aus Formularen auf denen wichtige Informationen rasch zugänglich sind, aus fest geschalteten Rufnummern, aus vorbereitete Aussagen zu verschiedenen Situationen und aus einer Prioritätenliste in dem festgehalten wird, wer in welcher Situation zuerst informiert wird.
- Aufbauen und Nachführen einer vollständigen Systemdokumentation, damit ein Administrator sich rasch einen Überblick über das System verschaffen kann. Diese beinhaltet:
  - die Dokumentation aller vorhandenen IT-Systeme und deren Konfiguration
  - die Dokumentation der Benutzer, Gruppen und Rechte
  - die physikalische und logische Netzwerkkonfiguration
  - die Datensicherung der Systeme
  - die vorhandenen Applikationen und deren Konfiguration
- Die Dokumentation ist so aufzubewahren, dass sie im Notfall jederzeit verfügbar ist. Der Zugriff auf die Dokumentation ist auf die Administratoren zu beschränken.

8.10.3 Einfluss der Massnahmen auf das Risiko, Kosten und operationelle Abläufe

Mit den obenstehenden Massnahmen dürften die Konsequenzen auf "spürbar" reduziert werden. Die Mehrheit der Massnahmen ist organisatorischer Natur, da wir in diesem Bereich in den Interviews grössere Defizite festgestellt haben. Weiterhin sind organisatorische Massnahmen kurzfristiger umzusetzen, als wenn die IT-Infrastruktur selbst angepasst werden muss. Die Kosten für die Massnahmen erachten wir deshalb als akzeptabel. Die Massnahmen haben einen Einfluss auf die operationellen Abläufe, da die notwendigen Prozesse für das ITSCM eingeführt und gelebt werden müssen. Die Eintrittswahrscheinlichkeit bleibt durch die obenstehenden Massnahmen unverändert.

Folgerungen:

- Konsequenzen: vorher: kritisch → neu: spürbar
- Wahrscheinlichkeit: selten (unverändert)

8.11 Server ausstecken/herunterfahren in Zentrale

8.11.1 Einleitung

Dieser Angriffsvektor beschreibt Szenarien, in denen Angreifer in eine Betriebsleitzentrale eindringen um dort bewusst Störungen an den Servern oder dem Netzwerk zu verursachen. Solche Angriffe können den Betrieb stark beeinträchtigen. Die Konsequenzen dieses Angriffsvektors haben wir in Kapitel 7 deshalb als "kritisch" eingeschätzt. Dadurch dass die Zugänge zu den Systemen schlüsselgesichert oder zum Teil überwacht sind haben wir die Eintrittswahrscheinlichkeit als "selten" festgelegt.

8.11.2 Massnahmen zur Verringerung des Risikos

Die folgenden Massnahmen basieren zum Teil auf dem Dokument der BSG [BSG, 2008].

- Einhalten der Vorgaben des Bundesamtes für Bauten und Logistik und den Bundessicherheitsdienstes für den physischen Schutz.
- Redundante Auslegung kritischer Systemkomponenten wie das Kommunikationsnetzwerk, die Server oder die Backups der Systeme und Daten (siehe 8.9.2).
- Sensibilisieren der Mitarbeiter bezüglich Social-Engineering Angriffe (siehe 8.9.2).
- Überwachen ab dem Zeitpunkt einer Kündigung eines Mitarbeiters (siehe 8.9.2).

8.11.3 Einfluss der Massnahmen auf das Risiko, Kosten und operationelle Abläufe

Mit den obenstehenden Massnahmen dürften die Konsequenzen auf "spürbar" reduziert werden. Dadurch dass aus Wirtschaftlichkeitsüberlegungen nicht alle Komponenten redundant vorgehalten werden können, kann es trotzdem zu vereinzelten Ausfällen kommen. Die Kosten für die organisatorischen Massnahmen sind eher gering. Für bauliche Massnahmen oder die Beschaffung von Systemkomponenten sind eher hohe Kosten zu erwarten. Auf die operationellen Abläufe haben die Massnahmen lediglich bei der Einhaltung der Policy betreffend Social-Engineering und bei Kündigung einen Mitarbeiters einen Einfluss. Diese müssen eingeführt und deren Einhaltung periodisch überprüft werden. Die Eintrittswahrscheinlichkeit bleibt durch die obenstehenden Massnahmen unverändert.

Folgerungen:

- Konsequenzen: vorher: kritisch → neu: spürbar
- Wahrscheinlichkeit: selten (unverändert)

8.12 Eine E-Mail versenden, die schädlichen Code enthält

8.12.1 Einleitung

Dieser Angriffsvektor beschreibt Szenarien, in denen externe Angreifer gezielt eine E-Mail mit schädlichem Code an Mitarbeiter von VT-Betreibern senden. Die Malware soll dazu dienen die VT-Systeme lahm zu legen. Die Konsequenzen wurden von uns daher als "kritisch" eingestuft. Da die Interviewpartner die Betriebsnetze von den Business-Netzen gut separiert haben, dürften solche Angriffe eher "selten" zum Erfolg führen.

8.12.2 Massnahmen zur Verringerung des Risikos

Die folgenden Massnahmen basieren zum Teil auf einem Dokument des Österreichischen Zentrums für sichere Informationstechnologie [A-SIT, 2007]:

- Vermeiden von Informationslecks.
- Einsatz von Antimalwaresoftware (siehe 8.2.2)
- Betriebs- und Kommunikationsnetze sauber voneinander trennen (siehe 8.2.2).
- Mitarbeiter bezüglich Gefahren von E-Mail-Nachrichten sensibilisieren:
  - Vorsicht bei Mails von unbekannten Absendern.
  - Dateianhänge vorsichtig behandeln. Im Zweifelsfall die Dateien nicht öffnen.
  - Bei Verdacht auf Malware die zuständigen Stellen innerhalb der Unternehmung alarmieren.
  - Auch Nachrichten, die im HTML-Format gesendet werden, können im Hintergrund Schadcode ausführen. Nachrichten sollten deshalb grundsätzlich nur im Textmodus angezeigt werden.

8.12.3 Einfluss der Massnahmen auf das Risiko, Kosten und operationelle Abläufe

Die Konsequenzen dürften mit den obenstehenden Massnahmen auf "spürbar" reduziert werden. Die Kosten dürften gering sein: Die meisten Interviewpartner setzen bereits Anti-Malwaresoftware ein und die Netze sind grösstenteils auch bereits sauber voneinander getrennt. Wichtig ist hier, dass die Mitarbeiter sensibilisiert werden.

Folgerungen:

- Konsequenzen: vorher: kritisch → neu: spürbar
- Wahrscheinlichkeit: selten (unverändert)

8.13 Auswirkung der Massnahmen auf die Risikomatrix

Mit den in diesem Kapitel vorgeschlagenen Massnahmen ergibt sich folgende neue Risikomatrix:

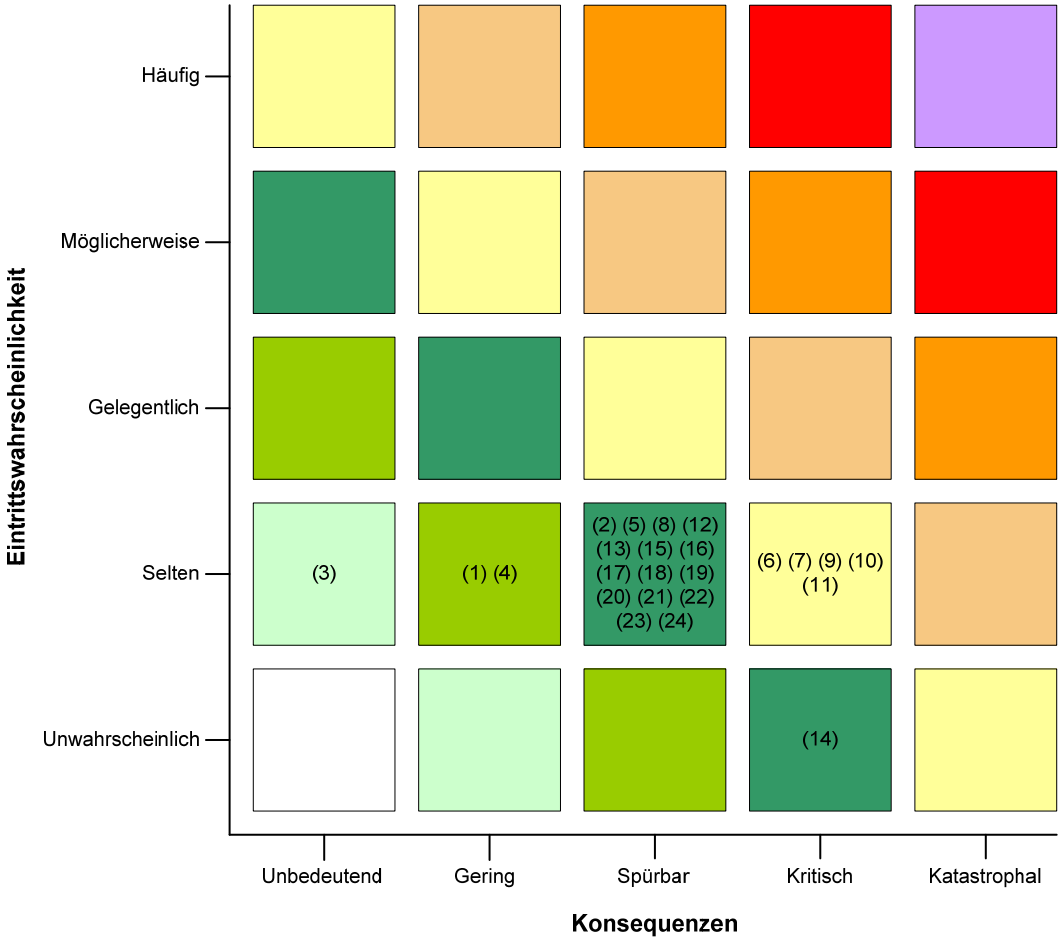


Abbildung 15: Risikomatrix, nach den Massnahmen

In der Matrix ist ersichtlich, dass auch nach Durchführung von geeigneten Massnahmen die Konsequenzen bei einzelnen Angriffsvektoren kritisch bleiben. Diese sind, im Rahmen einer kontinuierlichen Sicherheitsstrategie im Auge zu behalten und bei Bedarf - insbesondere wenn sich deren Eintrittswahrscheinlichkeiten durch neuartige Bedrohungsszenarien erhöhen sollten – erneut über Massnahmen zu entscheiden, mit welchen deren Risiken reduziert werden können.

An dieser Stelle möchten wir nochmals explizit darauf hinweisen, dass es sich bei der von uns durchgeführten Risikoanalyse und den daraus resultierenden Massnahmen zur Reduktion der Risiken um eine summarische Betrachtung über alle untersuchten Gebietseinheiten und Systeme handelt. Die Beurteilung der Risiken entspricht dabei im Wesentlichen unserer Aussensicht, obschon wir auch einige Informationen aus den Interviews, die wir mit verschiedenen Gebietseinheiten durchgeführt haben, in der Bewertung einfliessen liessen. Schlussendlich muss jede Gebietseinheit selbst darüber entscheiden, welche Risiken akzeptiert werden können und welche Risiken mit Hilfe der in diesem Kapitel definierten Massnahmen reduziert werden müssen.

9 Sicherheitskonzept

9.1 Einleitung

Dieses Kapitel enthält einen Überblick mit einer sinnvollen Menge von Massnahmen, die für die IT-Sicherheit in der Verkehrstelematik relevant sind. Das Kapitel enthält sowohl Massnahmen, die bereits in den Gebietseinheiten und in der Verkehrsmanagementzentrale Schweiz umgesetzt sind, als auch Massnahmen zur Reduzierung der im Kapitel 7 erkannten Risiken. Jede Massnahme wird mit einer Beschreibung sowie einer Begründung dokumentiert.

Das Ziel des Kapitels ist es, einer Gebietseinheit oder einer VM-Zentrale ein Hilfsmittel zur Verfügung zu stellen, das die Massnahmen beschreibt und die Gründe dafür verständlich darlegt.

Die Massnahmen werden in die Bereiche:

- organisatorische Sicherheitsmassnahmen
- technische Sicherheitsmassnahmen
- physische Sicherheitsmassnahmen

unterteilt. Innerhalb dieser Gruppierung wird noch zwischen grundlegenden und weiterführenden Massnahmen unterschieden. Mit den grundlegenden Massnahmen wird bereits eine gute Sicherheit erreicht. Die weiterführenden Massnahmen sollen einzelnen Gebietseinheiten oder VM-Zentralen dazu dienen, noch eine erhöhte Sicherheit einzuführen. Die Beurteilung des Nutzens einer erhöhten Sicherheit muss dabei fallweise erfolgen.

9.2 Organisatorische Sicherheitsmassnahmen

9.2.1 Grundlegend

Dokumentation

➡	Für jedes System wird eine vollständige, aktuelle und richtige Systemdokumentation gepflegt.	Der Zugriff auf eine qualitativ hochwertige Dokumentation spart im Notfall enorm Zeit. Die Erhaltung des Wissens wird durch die Dokumentation sichergestellt.
➡	Pro Betriebsorganisation ist ein Disaster-Recovery-Plan für die Wiederherstellung der Systeme und der Einrichtungen zu führen.	Der Plan definiert die notwendigen Massnahmen, die zur Rückkehr zum Normalbetrieb nach einem Systemausfall notwendig sind. Es sind darin insbesondere folgende Fragen zu beantworten: – Wie viel Ausfallzeit ist zu verkraften? – Wie hoch darf der Datenverlust maximal sein? – Wie ist die Reihenfolge bei der Wiederher-

		stellung der Systeme und der Daten? – Was sind die personellen Verantwortlichkeiten im Notfall?
➡	Pro Betriebsorganisation ist eine Sicherheitsrichtlinie mit Beschreibung der Regeln und der Verfahren für sicherheitskritische Bereiche zu führen.	Mit der Richtlinie werden allgemeine Regeln definiert, die bei Einhaltung bereits grundlegende Risiken auf ein Minimum reduzieren. Die Richtlinie beinhaltet Angaben zur Organisation (Rollen und Verantwortungen), zu erlaubten und verbotenen Prozessen (Verfahren zum Malwareschutz, Umgang mit externen Datenträgern, …) und zu den Konsequenzen bei Nicht-Einhaltung der Richtlinie. Die Richtlinie ist regelmässig zu überprüfen und ggf. an neue Bedrohungen anzupassen.

Administration

➡	Die Systemadministratoren betreiben ein aktives Zugangsmanagement: – Benutzerscharfe Logins (keine "shared accounts") – Zugriffsrechte nur dort wo nötig – Regelung bei Austritt eines Mitarbeiters und bei betriebsinternen Mutationen – Überwachen der Aktivitäten durch Protokollierung – Forcieren sicherer Passwörter	Ein formelles und dokumentiertes Benutzermanagement inklusive Überwachung sowohl für interne Mitarbeiter als auch bei den Lieferanten bildet die Basis für eine sichere Zugriffskontrolle und unterstützt die Nachvollziehbarkeit im Falle einer Störung oder eines Unfalls.
➡	Die Software ist möglichst immer auf dem aktuellsten Stand zu halten (besonders bei exponierten Systemen wie z.B. Remote-Zugängen).	Dadurch wird sichergestellt, dass keine Sicherheitslücken aufgrund von veralteter Software entstehen. Dabei sollte aber darauf geachtet werden, dass sich die aufdatierte Software auch problemlos mit der bestehenden Software des Systems verträgt (siehe auch "Verfahren beim Einsatz neuer Software" und "Patch-Management-Prozess einführen").

➡	Software muss "sicher" konfiguriert (gehärtet) werden.	Durch eine unsichere Konfiguration der Softwarekomponenten können Sicherheitslücken entstehen, die sich sehr einfach ausnutzen lassen können (z.B. nicht geänderte Standardpasswörter).
➡	Firewallregeln sind zu warten	Die Firewallregeln sollten regelmässig überprüft und bei Bedarf angepasst werden. Auf diese Weise wird sichergestellt, dass keine "veralteten" Regeln aktiviert sind oder die Firewall "zu offen" ist.
➡	Fernwartungszugänge sind abzusichern – Remote-Zugänge zeitlich begrenzen – Remote-Zugänge kontrolliert freischalten: Wartungsarbeiten sind anzumelden – Mitarbeiter, die Wartungsaufgaben erfüllen sind registriert und besitzen benutzerspezifische Logins – Zugriffe protokollieren und Log-Dateien regelmässig prüfen – Sichere Authentisierungsmechanismen anwenden – Sichere Protokolle mit sicheren kryptografischen Verfahren verwenden	Schlecht gesicherte Remote-Zugänge können die gesamten Sicherheitsmechanismen einer Unternehmung aushebeln. Deshalb ist es von entscheidender Bedeutung, die Fernwartungszugänge angemessen zu sichern.
➡	Backup und Recovery systematisch betreiben: – Erarbeiten eines Backup-Konzepts – Regelmässige Backups der Systeme und der Daten – Gelegentliches Testen der Recovery-Prozeduren	Bei einer Wiederherstellung des Betriebs nach einem Notfall ist der Zugriff auf aktuelle Systemkonfigurationen und Daten extrem wichtig. Regelmässige Backups alleine genügen nicht. Es muss auch periodisch der Recovery-Prozess durchgespielt werden um die Systemwiederherstellung zu testen.
➡	Sicherung kritischer Daten (Backups an verschiedenen geographischen Orten ab-	Die doppelte Sicherung der Daten schützt vor Datenverlust (beispielsweise durch Malware, externe Angreifer, etc.). Die Backups sollten

	legen).	deshalb ausserhalb des Standortes aufbewahrt werden, damit sie bei "physischen Ereignissen" am Standort (z.B. Brand) nicht beschädigt werden.

Führung

➡	In Wartungsverträgen sind Klauseln für Ersatzteillieferungen zu berücksichtigen.	Beim Abschluss eines Vertrags ist darauf zu achten, dass der Lieferant im Notfall Ersatzteile oder ganze Systeme liefern kann.
➡	Die Verfahren beim Einsatz neuer Software sind zu regeln: – Erarbeiten und einsetzen eines Softwarefreigabeverfahrens – Strikte Eingangskontrolle für jedes neue Produkt – Nur freigegebene Software installieren – Kopien der Software an einem anderen Standort lagern – Sicherstellen des Quell-Codes	Beim Einsatz von neuer Software sind einige Grundregeln festzulegen, die helfen die Sicherheit zu erhöhen.
➡	Ein Patch-Management-Prozess ist einzuführen.	Der Patch-Management-Prozess stellt dabei sicher, dass neue Patches zunächst genau analysiert und getestet werden. Patches werden nur dann in das produktive System eingespielt, wenn sie (z.B. aus Gründen der Sicherheit) absolut notwendig sind und wenn keine Schwierigkeiten bezüglich der Zusammenarbeit mit der bestehenden Software aufgedeckt werden konnten.
➡	Richtlinien für die Sicherstellung einer hohen Qualität bei der Software-Entwicklung sind festzulegen.	Durch den Einsatz robuster und einfach wartbarer Software ergeben sich während der Einsatzzeit weniger Probleme. Es sollte auch darauf geachtet werden, dass bei der Softwareentwicklung keine unsicheren Programmkonstrukte verwendet werden. Die Software muss ausserdem vor Inbetriebnahme auf Sicherheitslücken

		getestet werden.
➡	Rolle des IT-Sicherheitsbeauftragten ist sicherzustellen.	Je Organisationseinheit (VM-Zentrale oder Gebietseinheit) ist eine Person in der Rolle des IT-Sicherheitsbeauftragten zu bestimmen. Der IT-Sicherheitsbeauftragte ist für die Erarbeitung und die Durchsetzung der Sicherheitsrichtlinien zuständig.
➡	"IT-Service Continuity Management (ITSCM)" aufbauen.	Das ITSCM stellt sicher, dass die Risiken für die IT-Prozesse identifiziert und bewertet sind, dass Notfallmassnahmen vorhanden sind und dass nach einem Schaden der Betrieb geordnet wieder aufgenommen werden kann. Die Elemente eines ITSCM beinhalten organisatorische, technische und personelle Massnahmen.

9.2.2 Weiterführend

Dokumentation

➡	Verfahren für die Notfallvorsorge sind zu erarbeiten.	Für den Notfall sind die wesentlichsten Massnahmen zu definieren. Die Verfügbarkeitsanforderungen und die Kapazitätsanforderungen (CPU, Speicher, Netzwerk, …) sind zu dokumentieren. Es ist ein Datensicherungskonzept zu erstellen und periodisch zu testen. Die Mindestanforderungen an den Betrieb sind zu definieren. Für verschiedene Ereignisse sind Notfallpläne vorzuhalten.
➡	Hilfsmittel für die Kommunikation in Notfällen sind zu erarbeiten.	Eine erfolgreiche externe Kommunikation ist für die VM-Zentralen von hoher Bedeutung. Deshalb sollten verschiedene Hilfsmittel dafür bereitgestellt werden. Dazu gehören der Notfallplan, vorbereitete Aussagen zu definierten Situationen, Formulare für die Aufnahme und Weitergabe von Informationen sowie eine Prioritätenliste für die Information von beteiligten

		Stellen.
➡	Ratschläge zur Beseitigung von Informationslecks sind zu erarbeiten.	Mit diesen Massnahmen wird sichergestellt, dass möglichst wenig sensitive Informationen über eine Firma an die Öffentlichkeit geraten. Dadurch wird das Unternehmen einerseits besser vor potenziellen Angriffen durch Aussenstehende Cracker geschützt, andererseits kann so auch ein möglicher Datendiebstahl verhindert oder erschwert werden.

Führung

➡	Die Änderungen an den Systemen (Software und Hardware) unterliegen einem Changemanagement.	Mit einem umfassenden Changemanagement wird die Nachvollziehbarkeit bezüglich "was wann von wem geändert wurde", erhöht. Diese Informationen sind im Notfall von grosser Bedeutung.
➡	Eine regelmässige Überprüfung der Informatiksicherheit durch externe Partner ist durchzuführen.	Dadurch wird sichergestellt, dass das Unternehmen angemessen vor Bedrohungen, welche zum Zeitpunkt der Überprüfung gerade aktuell sind, geschützt ist. Externe Partner sollten deshalb beigezogen werden, weil die Unternehmung selbst evtl. "zu nahe" am System dran ist und potenzielle Schwachstellen deshalb möglicherweise übersieht. Ausserdem kann es sein, dass die Unternehmung selbst nicht über die aktuellsten Tools und Techniken verfügt, um ein detailliertes und aussagekräftiges Überprüfung durchzuführen.
➡	Ausbildung in Informatiksicherheit ist zu betreiben: – Datenschutz/Datensicherheit – Malwareschutz	Der Mensch ist bekanntlich das schwächste Glied in der Kette von Sicherheits-Massnahmen. Deshalb ist es von entscheidender Bedeutung, die Mitarbeiter in einem Unternehmen für den sicheren Umgang mit Informatikmitteln zu sen-

	– Umgang mit E-Mails – Umgang mit (mobilen) Datenträgern – Sicherheit am Arbeitsplatz (physisch) – Social Engineering (Gefahren)	sibilisieren.
➡	Die Wartungsarbeiten an den Systemen sind als Prozesse gemäss den Vorgaben des Qualitätsmanagements zu definieren.	Damit soll sichergestellt werden, dass die Aktivitäten der Wartungsarbeiten gemäss Standardabläufen geplant durchgeführt und kontrolliert werden.
➡	Eine Notfallorganisation ist aufzubauen.	Die Notfallorganisation dient dazu bei einem Schaden schnell und richtig zu handeln. Folgende Punkte sind ein Bestandteil davon: – Krisenstab mit klaren Stellvertretungen – Klare Führungsgrundsätze – Kurze Meldewege – Klar strukturiertes und einfaches Notfallhandbuch – Hardware-Ersatzteile

9.3 Technische Sicherheitsmassnahmen

9.3.1 Grundlegend

➡	Klare Trennung zwischen Produktiv- und Test-/Entwicklungssystemen ist sicherzustellen.	Neue Patches oder Softwarekomponenten sollten vor dem Einspielen in das produktive System zuerst in einem "realistischen" Testumfeld geprüft werden. Dadurch kann festgestellt werden, ob sich die neue Software evtl. nicht gut mit der bestehenden Software verträgt.
➡	Sensitive Daten grundsätzlich verschlüsselt übertragen (auch USB-Sticks, CDs, DVDs, Festplattenverschlüsselung bei Service-Laptops).	Dadurch wird verhindert, dass sensitive Informationen in die falschen Hände geraten.
➡	Zugriff auf sensitive Bereiche soll erst nach einer erfolgreichen Authentisierung und	Dadurch wird sichergestellt, dass nur Personen auf eine bestimmte Ressource zugreifen dür-

	Autorisierung möglich sein.	fen, die sich einerseits erfolgreich authentifiziert haben (also deren Identität erfolgreich bestätigt werden konnte) und die für den Zugriff auf die entsprechende Ressource autorisiert sind (d.h. die Berechtigung haben, die entsprechende Ressource zu verwenden). Gemäss dem Prinzip von "Least Privilege" sollte eine Person nur auf jene Ressourcen zugreifen dürfen, die sie für die Erledigung ihrer Aufgaben absolut benötigt.
➡	Sicherung "sensitiver" Verbindungen mit kryptographischen Massnahmen.	Mit Hilfe der "kryptographischen Massnahmen" soll die Integrität, Authentizität und Vertraulichkeit der übertragenen Daten gewährleistet werden. Dadurch wird erreicht, dass sensitive Daten nicht von Dritten abgehört werden können (Vertraulichkeit - Verschlüsselung der Daten), es wird gewährleistet, dass die Daten unterwegs nicht böswillig verändert wurden (Integrität - z.B. mittels MAC (Message Authentication Code) oder digitalen Signaturen) und schliesslich kann dadurch eindeutig überprüft werden, "wer" die Daten gesendet hat (Authentizität - ebenfalls z.B. mittels MAC oder digitalen Signaturen).
➡	Malwareschutz/Personal Firewalls installieren (auf Clients, auf Server).	Ein Malwareschutz sollte wenn möglich auf allen Clients und Server installiert werden. Die Malwaredefinitionen sollten regelmässig aktualisiert werden. Personal Firewalls sollten auf möglichst allen Clients, insbesondere aber auch auf den Servicelaptops, installiert werden. Personal Firewalls können beispielsweise den Spielraum von Malware auf einem Client einschränken (indem eingehende und ausgehende Verbindungen nur für vertrauenswürdige Programme zugelassen werden).
➡	Netzwerktopologie mit klaren Trennungen	Business-Netze sollten gut von den Betriebs-

	zwischen verschiedenen Netzwerkebenen (In-Depth-Architektur).	netzen getrennt werden. Die unterschiedlichen Netzbereiche sollten dabei mit angemessenen Massnahmen voneinander getrennt werden (siehe auch [NIST, 2008]). Durch eine angemessene Trennung unterschiedlicher Netzbereiche (mit unterschiedlichen Aufgaben) lässt sich der Netzwerkverkehr besser kontrollieren (beispielsweise durch geeignete Firewallregeln). Ausserdem kann so z.B. auch verhindert werden, dass sich eine Malware im gesamten Netz ausbreiten oder dass ein externer Angreifer das gesamte Netz kompromittieren kann, wenn er bereits einen Teil des Netzes kompromittiert hat.
➡	Kritische Systemkomponenten redundant auslegen (Kommunikationsnetzwerk, Server, Backups).	Dadurch wird verhindert, dass im Falle eines Ausfalls einer kritischen Komponente das gesamte Netz lahm gelegt wird.
➡	Verwendung vertrauenswürdiger Zertifikate bei Webportalen mit SSL/TLS-Verschlüsselung (HTTPS).	Bei nicht vertrauenswürdigen Zertifikaten kann ein Benutzer nicht sicher sein, ob er tatsächlich mit dem "richtigen" Server spricht oder ob es einem Angreifer gelungen ist, eine Man-In-The-Middle-Attacke (MITM) durchzuführen, da in beiden Fällen eine Zertifikats-Warnung im Browser angezeigt wird. Deshalb sollten nur vertrauenswürdige Zertifikate eingesetzt werden.

9.3.2 Weiterführend

➡	Verwendung von Intrusion-Detection-/Prevention-Systeme (IDS/IPS).	Firewalls können bereits einen beträchtlichen Anteil an "ungewolltem Verkehr" verhindern. "Normale" Packet-Filtering Firewalls arbeiten jedoch "nur" auf Layer 3, d.h. es kann im Wesentlichen nur kontrolliert werden, "wer mit wem sprechen darf". Der genaue Inhalt der Pakete (Payload) lässt sich jedoch nicht genauer analysieren. Deshalb ist es wichtig, nebst dem

		Einsatz von Firewalls auch IDS/IPS einzusetzen. Dadurch können gezielt gewisse Pakete herausgefiltert werden, welche einen "schädlichen" oder "ungewollten" Inhalt aufweisen.
➡	Sicheres Löschen beim Entsorgen von Datenträgern mit sensitiven Daten.	Dadurch wird verhindert, dass sensitive Informationen in die falschen Hände gelangen.

9.4 Physische Sicherheitsmassnahmen

9.4.1 Grundlegend

➡	Einhalten der Vorgaben des Bundesamtes für Bauten und Logistik und Bundessicherheitsdienstes für den physischen Schutz.	Beim Bau oder Ausbau von IT-Räumlichkeiten liefern diese Grundlagen die Minimalanforderungen für den physischen Schutz.
➡	Innenschutz sicherstellen.	Der Innenschutz umfasst für die Informatiksicherheit alle Bereiche mit Informatikinfrastrukturen. Für den Innenschutz müssen insbesondere die Komponenten Standortwahl, Zutrittschutz, Brandschutz, Wassereinbruchschutz, Überspannungsschutz, Kabelschutz und Sabotageschutz beachtet werden. [BSG, 2008]
➡	Einbruchsschutz sicherstellen.	Der Einbruchsschutz ist bereits in der Bauplanung zu berücksichtigen. Sensible Bereiche sind am besten im mittleren Gebäudeteil untergebracht (Erdgeschoss: Bedrohung durch Einbruch, Anschlag, Vandalismus und höhere Gewalt. Keller: Bedrohung durch Wassereinbruch; Oberstes Stockwerk: Bedrohung durch Blitzeinschlag, Sturm) [BSI]

9.4.2 Weiterführend

➡	Zutrittskontrolle, mit Protokollierung führen.	Bei Bedarf kann es sehr wichtig sein, Ereignisse vollständig rekonstruieren zu können. Dafür ist die Protokollierung wer war wann an welchem Ort ein wertvolles Hilfsmittel. Die Zutritts-

		kontrolle kann manuell mittels Journalen oder automatisch erfolgen. Wenn immer möglich sollte die automatische Variante bevorzugt werden.
➡	Schlüsselverteilung verwalten und periodisch überprüfen.	Jeder Schlüssel ist zu registrieren und an nur einer Person zuzuordnen. Das Verzeichnis sollte regelmässig überprüft werden. Insbesondere sind die Prozesse des Mitarbeiteraustritts und des Wechsels von Lieferanten diesbezüglich speziell zu betrachten.

10 Empfehlungen und Ausblick

In Kapitel 9 wurde einen Massnahmenkatalog mit sinnvollen Massnahmen aufgestellt, der den VT-Betreibern behilflich sein soll, sich vor aktuellen Bedrohungen angemessen zu schützen. Diese Massnahmen reflektieren jedoch "nur" die aktuelle Bedrohungslage. Um mittel- und längerfristig angemessen gegen mögliche Bedrohungen geschützt zu sein, müssen die Bedrohungslage ständig neu analysiert und die Massnahmen entsprechend aktualisiert werden. Entsprechend wurde zusätzlich zu den vier Stufen nach BSI die Stufe "Empfehlung" eingeführt (siehe Kapitel 1.3). In der Stufe "Empfehlung" sollen Anweisungen und Ratschläge aufgeführt werden, die dazu dienen, das Sicherheitskonzept mittel- und langfristig aktuell zu halten. Als weiterer Aspekt der Stufe "Empfehlung" werden die Themen identifiziert, die in zukünftigen Normen oder Richtlinien zu berücksichtigen sind.

Zu diesem Zweck möchten wir in Abschnitt 10.1 zunächst einige wesentliche Punkte reflektieren, die wir im Laufe dieses Forschungsprojektes gelernt haben. Abschnitt 10.2 zeigt sodann auf, mit welchen Prozessen und Praktiken eine Organisation ihr Sicherheitskonzept auf einem aktuellen Stand halten kann. In Abschnitt 10.3 soll schliesslich diskutiert werden, welche Bereiche und Themen dieses Berichts normierungswürdig sind oder in einer Richtlinie zusammengefasst werden sollten.

10.1 Erkenntnisse aus dem Forschungsprojekt

In diesem Forschungsprojekt haben wir gesehen, dass die IT-Schutzziele in SCADA-Netzen grundsätzlich anders bewertet werden als in Business-Netzen. Das oberste Schutzziel bei SCADA-Netzen ist eindeutig die Verfügbarkeit. Auch die Integrität der Daten ist wichtig, denn mit fehlerhaften oder gar bewusst manipulierten Daten kann ein reibungsloser Betrieb nicht mehr gewährleistet werden. Eine eher untergeordnete Rolle spielt die Vertraulichkeit. Bei Business-Netzen ist das im Prinzip genau umgekehrt: Hier geniesst die Vertraulichkeit der Geschäftsdaten oft die oberste Priorität. Das bedeutet aber auch, dass man beim Betrieb von VT-Systemen gewisse Dinge beachten muss. So ist zum Beispiel beim Einspielen von Patches und Updates besondere Vorsicht geboten, da das System bei unsachgemässer Handhabung neu eingespielter Software lahm gelegt werden kann. Gängige IT-Security-Praktiken müssen an die Bedürfnisse und Gegebenheiten von SCADA-Systemen angepasst werden. Wir haben auch gesehen, dass SCADA-Systeme nicht alleine durch technische Massnahmen gesichert werden können, sondern dass es einen Mix aus technischen, organisatorischen und physischen Massnahmen braucht. IT-Security ist ein kontinuierlicher Prozess - die Gefahrenlage ändert sich stetig aufgrund neuer und sich ändernder Bedrohungen. Die Sicherheitsmassnahmen müssen deshalb laufend hinterfragt und bei Bedarf überarbeitet werden.

Anhand der Interviews mit den Gebietseinheiten konnte festgestellt werden, dass betreffend IT-Sicherheit zurzeit unterschiedliche Verfahren sowie heterogene Umsetzungen vorhanden sind. Es existieren keine einheitlichen IT-Sicherheitsrichtlinien. Ausserdem haben wir gesehen, dass die Gebietseinheiten momentan noch wenig miteinander vernetzt sind, was sich in Zukunft aber wahrscheinlich ändern wird, vor allem im Zusammenhang mit VM-CH. Die vermehrte Vernetzung bringt natürlich auch neue Gefahren mit sich, welche von den Gebietseinheiten und den VM-Zentralen entsprechend berücksichtigt werden müssen. Die meisten Interviewpartner haben angegeben, dass ihre Systeme zum aktuellen Zeitpunkt in sich autonom und gut von anderen Systemen isoliert sind. Als Schwachstelle wird oft der Zugriff von Lieferanten genannt, welche entweder über schlecht kontrollierbare Zugänge auf die Systeme zugreifen oder Patches ohne vorgängige Tests in das System einspeisen.

Wirklich kritische Risiken mit hohen Eintrittswahrscheinlichkeiten und katastrophalen Konsequenzen konnten in diesem Forschungsprojekt keine identifiziert werden. Allerdings wurden einige Risiken mit kritischen Konsequenzen identifiziert, die gelegentlich vorkommen können. Dabei handelt es sich um die Angriffsvektoren "Patches/OS-Updates/Malware-Updates", "Einstecken eines mit Malware verseuchten Geräts", "allge-

meine Wartungsarbeiten" und "arglistiges Bedienen von VT-Systemen". DoS-Attacken haben zwar geringe Konsequenzen, können theoretisch jedoch häufig vorkommen. Ausserdem existieren auch einige Risiken mit kritischen Konsequenzen, die jedoch selten vorkommen sollten.

10.2 Betreiben des Sicherheitskonzepts

Damit die Gebietseinheiten und die VM-Zentralen auch mittel- und längerfristig genügend gegen Bedrohungen aus der IT-Welt geschützt sind, müssen die Sicherheitsmassnahmen gemäss der Checkliste im Kapitel 9 ständig hinterfragt und neu beurteilt werden. Folgende Prozesse und Praktiken sollten in einer aktiven IT-Security-Governance nicht fehlen:

- IT-Risiken beurteilen: IT-Risiken müssen in einem formalen Risk-Management-Prozess ständig im Auge behalten werden. Die Risiken gilt es regelmässig neu zu beurteilen um die aktuelle Bedrohungslage zu berücksichtigen.
- Massnahmen anpassen: Aufgrund der Erkenntnisse aus dem Risikomanagement müssen die implementierten Massnahmen ständig neu hinterfragt und bei Bedarf angepasst werden. Das gilt sowohl für technische, als auch für organisatorische und physische Massnahmen.
- Externe Audits durchführen: Externe Audits zeigen Sicherheitsmängel auf, die der Organisation selbst nicht bekannt waren oder welche die Organisation übersehen hat. Ausserdem wird dadurch aufgezeigt, wie gut die implementierten Sicherheitsmassnahmen gegen aktuelle Bedrohungen schützen.
- Sensibilisierung der Mitarbeiter schulen: Die Mitarbeiter müssen über mögliche Bedrohungen informiert und im sicheren Umgang mit Informatik-Mitteln geschult werden.
- Risiken durch Lieferanten: Die Lieferanten sollten aktiv in den Sicherheitsmanagement-Prozess miteinbezogen werden. Die Produkte sollten gewisse Vorgaben einhalten. Die Lieferanten sollen dazu ermutigt werden, IT-Security aktiv bereits beim Design ihrer Produkte zu berücksichtigen.
- Pflegen der Sicherheitsrichtlinien: Security-Policies, Security-Pläne, Standards, etc. müssen gepflegt und bei Bedarf angepasst werden.

10.3 Empfehlung zur Normierung

Im Forschungsprojekt werden sowohl methodische als auch inhaltliche Aspekte der IT-Security behandelt, die dazu beitragen VM-Zentralen oder Gebietseinheiten beim Aufbau und Betrieb eines Sicherheitskonzepts zu unterstützen. Die methodischen Aspekte beruhen bereits auf einem Standard (BSI) der auch für SCADA-Netze angewendet werden kann. Ein Normierungsbedarf in diesem Bereich besteht aus unserer Sicht nicht. Inhaltlich bildet das Sicherheitskonzept im Kapitel 9 eine Checkliste auf Grund derer eine Organisation eine Abschätzung der Massnahmen zur Verbesserung der technischen, organisatorischen und physischen Sicherheit durchführen kann. Der Inhalt des Kapitels 9 könnte in eine Richtlinie zur Überprüfung der IT-Security überführt werden. Diese ist dann periodisch zu verifizieren und auf die sich ändernden Risiken anzupassen.

Anhänge

I Matrix Angriffsvektoren / Angriffgruppen

5.3.10 Physische Attacken/Unfälle	5.3.9 Unmotivierte oder verärgerte Mitarbeiter	5.3.8 Fehlmanipulation durch berechtigte Benutzer	5.3.7 Social Engineering	5.3.6 Sniffing	5.3.5 Eindringen in das System über unsichere konfigurierte Remote-Zugänge oder Wireless-Zugänge	5.3.4 Password Cracking	5.3.3 Ausnutzen von softwarebedingten Systemschwachstellen	5.3.2 Scanning und Enumeration	5.3.1 Zusammenstellen eines umfangreichen Profils mit Hilfe öffentlicher Informationen (Information Gathering)	
		x								Allgemeine Wartungsarbeiten am System
	x									Backdoors installieren
x										Backup-Tapes zerstören
x										Beschädigung von Feldkomponenten
								x		Betriebssystem bestimmen
x										Brandmeldesensor manipulieren
						x				Brute Forcing
	x						x			Daten löschen/korrumpieren
x										Defekte Wasserleitung (in BLZ)
						x				Dictionary PW Guessing/Rainbowtables
									x	DNS Interrogation (zone transfer)
							x			DoS/DDoS
			x							E-Mail mit schädlichem Code versenden
x										Einbruch
	x	x								Einstecken mit Viren verseuchten Laptops/USB Sticks
			x							E-Mail mit vertrauenswürdiger Absender-Adresse versenden um an interne Informationen ranzukommen
								x		Enumeration (Banner Grabbing, etc.)
									x	Facebook, Jobwebseiten
x	x									Feldkomponenten umprogrammieren
x										Feuer legen
x										Gasexplosion (in BLZ)
									x	Google Hacking
					x					GSM-/GPRS-Hacking
								x		ICMP Queries
	x									Insiderkenntnisse
x										Kabel durchtrennen/ausstecken
							x			Keyloggers installieren
		x								Logische/physische Bedienfehler
							x			Malware installieren, die Schwachstellen im Browser ausnutzen können
							x			Malware verbreiten, die Rechner fernsteuern
							x			Malware verbreiten, welche aggressives Scanning durchführt
							x			Manual Webapplication Assessment
								x		Nach offenen Ports scannen
								x		Nach Schwachstellen scannen
									x	Network Reconnaissance
		x								Patches/OS-Updates/Virenupdates, welche System lahm legen können
			x							Phishing
			x							Physischen Zugang erhalten
								x		Ping Sweeps
x										Rechner herunterfahren/ausstecken
x										Rechner mit Gewalt zerstören
							x			Schwachstellen ausnutzen mit bekannten Exploits
	x						x			Sensitive Daten stehlen
			x							Sich am Telefon als Lieferant/Mitarbeiter ausgeben, um sich einen Remotezugang freischalten zu lassen
				x						Sniffing (z.B. PW Exchange, etc.)
	x						x			Strassenanlagen bedienen für arglistige Zwecke
x										Videokameras ausstecken
					x					VPN-Hacking (z.B. IKE-Aggressive-Mode hacken, etc.)
					x					Wardialing
									x	Webcrawling
							x			Web-Cyberattacken
							x			Webseiten verunstalten
					x					WEP-/WPA-Hacking
									x	WHOIS & DNS Enumeration
	x									Zugang zum System über nicht entfernte Benutzerkonten
	x									Zugang zum System über Schlüssel, die dem Benützer nicht entzogen worden sind

Abkürzungen

Begriff	Bedeutung
ACL	Access Control List
AfBN	Amt für Betrieb Nationalstrassen
AGK	Abschnittsgeschwindigkeitskontrollanlagen
ARP	Address Resolution Protocol
A-SIT	Zentrum für sichere Informationstechnologie
ATA	Advanced Technology Attachment
ATM	Asynchronous Transfer Mode
ASTRA	Bundesamt für Strassen
BCIT	British Columbia Institute of Technology
BIOS	basic input/output system
BIT	Bundesamt für Informatik und Telekommunikation (CH)
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BLS	Betriebsleitsystem
BKA	Österreichischen Bundeskanzleramtes
BLZ	Betriebsleitzentrale
BMI	Bundesministerium des Innern
BSA	Betriebs- und Sicherheitsausrüstungen
BSI	Bundesamts für Sicherheit in der Informationstechnik (D)
CA	Certificate Authority
CCIP	Centre for Critical Infrastructure Protection - New Zealand
CCIRC	Canadian Cyber Incident Response Centre
CD	Compact Disk
CMOS	Complementary Metal Oxide Semiconductor
CMS	Content Management System
CPNI	Centre for the Protection of National Infrastructure (UK)
CPU	Central Processing unit
CSRF	Cross Site Request Forgery
CSSP	Control Systems Security Program
CVE	Common Vulnerabilities and Exposures
DHCP	Dynamic Host Configuration Protocol
DHS	US Department of Homeland Security
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS/DDoS	Denial of Service/Distributed Denial of Service
DVD	Digital Video Disk
FTP	File Transfer Protocol
GOVCERT	Australian Government Computer Emergency Readiness Team
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HERMES	Handbuch der elektronischen Rechenzentren eine Methode für Entwicklung von Systemen
HMI	Human Machine Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HW	Hardware
ICMP	Internet Control Message Protocol
IDS/IPS	Intrusion Detection System / Prevention System

Begriff	Bedeutung
IIS	Internet Information Services
IKE	Internet Key Exchange
INA	Integrierte Applikationen
INEEL	Idaho National Engineering and Environmental Laboratory
IPS	Intrusion Prevention System
IRB	Informatikrat Bund
ISB	Informatikstrategieorgan Bund
ISB-O	Informatiksicherheitsbeauftragten einer Organisation. Begriff aus der WIsB.
ISDN	Integrated Services Digital Network
ISDS	HERMES Informations- und Datenschutzkonzept
ISID	Industrial Security Incident Database
ISO	International Organization for Standardization
IT	Informationstechnologie
ITS	Intelligent Transport Systems
ITSCM	IT-Service Continuity Management
KAPO	Kantonspolizei
KMU	Kleine und mittlere Unternehmen
KRITIS	Kritische Infrastrukturen
LAN	Local Area Network
LSA/VDE	Lichtsignalanlage
LUNET	Netzwerk Luzern
LWL	Lichtwellenleiter
MELANI	Melde- und Analysestelle Informationssicherung
MITM	Man-In-The-Middle
MMI-Gremium	Man Machine Interface Gremium
NIC	Network Interface Card
NISCC	National Infrastructure Coordination Centre
NIST	National Institute of Standards and Technology (USA)
NPSI	Nationaler Plan zum Schutz der Informationsinfrastrukturen
NSNW	Nationalstrassen Nordwestschweiz
NSTB	National SCADA Testbed
NZZ	Neue Zürcher Zeitung
NTSB	National Transportation Safety Board
OPC	Open Connectivity via Open Standards
OS	Operating System - Betriebssystem
PSK	Pre-Shared Key
PCSRF	Process Control Security Requirements Forum
PHP	Hypertext Preprocessor
PW	Passwort
RAID	Redundant Array of Independent Disks
RAS	Remote Access Service
ROM	Read-only memory
RTU	Remote Telemetry Unit
SAM	Security Account Manager
SCADA	Supervisory Control and Data Acquisition
SLA	Servicelevel Agreement
SMB	Shared Message Block
SMTP	Simple Mail Transfer Protocol
SN	Schweizer Norm
SQL	Structured Query Language

Begriff	Bedeutung
SQLi	SQL Injection
SSH	Secure Shell
SSI	Server Side Includes
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Datagram Protocol
ÜLS	Übergeordnetes Leitsystem
URL	Uniform Resource Locator
USB	Universal Serial Bus
US-CERT	US Computer Emergency Readiness Team
USV	Unterbrechungsfreie Stromversorgung
VLAN	Virtual Local Area Network
VM-CH	Verkehrsmanagement Schweiz
VMZ-CH	Verkehrsmanagementzentrale Schweiz
VPN	Virtual Private Network
VSS	Verband Schweizer Strassen- und Verkehrsfachleute
VT	Verkehrstelematik
WAF	Web Application Firewall
WEP	Wired Equivalent Privacy
WIsB	Weisungen über die Informatiksicherheit in der Bundesverwaltung
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WTA	Wechseltextanzeige
XML	Extended Markup Language
XSS	Cross-Site Scripting
XST	Cross-Site Tracing

Glossar

Begriff	Bedeutung
Access Control List	Eine Access Control List (ACL) ist eine Software-Technik, mit der Betriebssysteme und Anwendungsprogramme Zugriffe auf Daten und Funktionen eingrenzen können.
Active Directory	Ein von Microsoft entwickelter Verzeichnisdienst. Ein Verzeichnisdienst stellt in einem Netzwerk eine zentrale Sammlung an Daten bestimmter Art zur Verfügung (im Falle von Active Directory insbesondere Daten zur Benutzerverwaltung).
Address Resolution Protocol	Das Address Resolution Protocol (ARP) ist ein Netzwerkprotokoll, das zu einer Netzwerkadresse der Internetschicht die physikalische Adresse (Hardwareadresse) der Netzzugangsschicht ermittelt und diese Zuordnung gegebenenfalls in den so genannten ARP-Tabellen der beteiligten Rechner hinterlegt. Es wird fast ausschließlich im Zusammenhang mit IPv4-Adressierung auf Ethernet-Netzen, also zur Ermittlung von MAC-Adressen zu gegebenen IP-Adressen verwendet, obwohl es nicht darauf beschränkt ist.
ARP-Spoofing	ARP-Spoofing (vom engl. *to spoof* - dt. *täuschen*, *reinlegen*) oder auch ARP Request Poisoning (zu dt. etwa *Anfrageverfälschung*) bezeichnet das Senden von gefälschten ARP-Paketen. Beim ARP-Spoofing wird das gezielte Senden von gefälschten ARP-Paketen dazu benutzt, um die ARP-Tabellen in einem Netzwerk so zu verändern, dass anschließend der Datenverkehr zwischen zwei Rechnern in einem Computernetz abgehört oder manipuliert werden kann.
Backbone	Verbindung eigenständiger Netzwerke oder Teilnetze, meist durch ein weiteres Netwerk oder einen FDDI - Ring. Ein Back-Bone soll effektive und wirtschaftliche Kommunikation gewährleisten. Durch Back-Bone lassen sich auch nicht homogene Netze koppeln (verschiedene Systeme). Backbone ist der englische Begriff für "Rückgrat" - ein Backbone ist der Daten-Hauptstrang eines Netzwerks. Je höher die Bandbreite dieser wichtigen Leitungen und auf je mehr ein Provider zurückgreifen kann, desto grösser ist die Geschwindigkeit beim Surfen.
Backdoor	Backdoor (auch *Trapdoor* oder *Hintertür*) bezeichnet einen (oft vom Autor eingebauten) Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen.
Banner	Banner sind für Hacker potentiell interessante Informationen über ein System wie zum Beispiel Hersteller, Systemversion, etc.
Banner Grabbing	Banner Grabbing bezeichnet eine Technik, um an den Banner eines Systems zu kommen. Häufig greift man dazu mit einer einfachen Telnet-Session auf ein System zu und schaut mal, "was genau zurückkommt". Für praktisch jedes Netzwerk-Protokoll (z.B. FTP) gibt es allerdings jeweils unterschiedliche Enumerations-Techniken um an Banner zu gelangen.
Bot-Netz	Ein Botnet oder Bot-Netz ist eine Gruppe von Software-Bots. Die Bots laufen auf vernetzten Rechnern, deren Netzwerkanbindung sowie lokale Ressourcen und Daten ihnen zur Verfügung stehen. Betreiber illegaler Botnetze installieren die Bots ohne Wissen der Inhaber auf Computern und nutzen sie für ihre Zwecke (beispielsweise zum Versenden von Spam-Emails oder für DDoS-Attacken).
Brute Forcing	Bezeichnet das Knacken eines Passworts oder geheimen Schlüssels mit "roher Gewalt", d.h. es werden ganz einfach alle möglichen Kombinationen durchprobiert.
Canonicalization Attacks	"Canonicalization" bezeichnet das Abbilden einer beliebigen Identifikation einer Datei auf eine eindeutige "kanonische Form". Eine Canonicalization Attack tritt nun auf, wenn ein Angreifer spezielle Zeichen in einen Request für eine Datei so injiziert, dass bei der Kanonisierung ein Ausnahmezustand eintritt. Das Resultat kann vielfältig sein. So kann es sein, dass der Angreifer bei einer erfolgreichen Attacke Zugriff auf beliebige Files hat, auf die er keinen Zugriff haben sollte.
Cookie Stealing	Bezeichnet das Stehlen des Cookies eines Internet-Benutzers (z.B. mit XSS). Dadurch kann der Angreifer zum Beispiel eine gültige Session des Internet-Benutzers übernehmen (z.B. wenn der Benutzer gerade bei seiner Bank eingeloggt ist).
Cross Site Request Forgery	Eine Cross-Site Request Forgery (zu deutsch etwa "Site-übergreifende Aufruf-Manipulation") ist ein Angriff auf ein Computersystem, bei dem der Angreifer unberechtigt Daten in einer Webanwendung verändert. Er bedient sich dazu eines Opfers, das ein berechtigter Benutzer der Webanwendung sein muss. Mit technischen Maßnahmen oder zwischenmenschlicher Überredungskunst wird hierzu ein kompromittierter HTTP-Request an die Webanwendung abgesetzt.
Cyberattacke	Eine Cyberattacke bezeichnet einen beliebigen elektronischen Angriff auf ein Informations-verarbeitendes System.
Denial of Service/Distributed Denial of Service	Cyberattacken, die das Ziel verfolgen, einen gewissen Service für legitime Benutzer unerreichbar zu machen.

Begriff	Bedeutung
Dynamic Host Configuration Protocol	Vereinfacht: Ermöglicht das automatische Zuweisen einer IP-Adresse an ein Gerät im Netzwerk
Dial-Up Hacking	Dial-Up bedeutet "Einwahl" und bezeichnet das Erstellen einer Verbindung zu einem anderen Computer über das Telefonnetz. Dial-Up Hacking bezeichnet das unbefugte Eindringen in ein Computersystem über das Telefonnetz.
Dictionary PW Guessing	Dictionary PW Guessing ist eine Form, um Brute Forcing zu betreiben. Dabei werden mögliche Passwort-Kandidaten aus einer vorgegeben Liste durchprobiert.
Directory Listing	Bezeichnet eine Technik, um auf Bereiche einer Website zu gelangen, die zwar nicht direkt über Links erreichbar aber trotzdem verfügbar sind (aufgrund unsicherer Konfiguration).
Demilitarized Zone	Bezeichnet in der Informatik den Bereich eines Netzwerkes einer Organisation, in welchem öffentliche Dienste bereitgestellt werden, wobei das interne Netz vor ungerechtfertigten Zugriffen geschützt wird.
DNS Interrogation	DNS Interrogation ist eine Technik, die versucht, möglichst viel interessante Informationen (z.B. interne IP-Adressen eines Firmennetzes) von einem DNS-Server eines Opfers zu erhalten.
Domain/Domänen	Der Domain Name (z. B. www.example.com) kann durch das DNS (Domain Name System) in eine IP-Adresse aufgelöst werden, die dann verwendet werden kann, um Netzwerkverbindungen zu diesem Rechner aufzubauen.
Domain Hijacking	Domain Hijacking ist eine Methode, um eine an sich legitime Website auf einen Server umzuleiten, welcher sich unter der Kontrolle eines Angreifers befindet.
Domain Name System	Mit Hilfe von DNS lassen sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z.B. www.melani.admin.ch).
Enumeration	Bei der Enumeration wird versucht, über verschiedene Netzprotokolle an möglichst sensitive Informationen zu gelangen. Sensitive können z.B. Systemversionen eines Rechners sein aber auch Benutzernamen, Dateifreigaben in einem Netzwerk, etc.
Exploit	Ein Programm, ein Script oder eine Codezeile, mit der sich Schwachstellen in Computersystemen ausnutzen lassen.
Firewall	Eine Firewall (engl. für Brandmauer) schützt Computersysteme, indem sie ein- und ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. Im Gegensatz dazu ist eine Personal Firewall (auch Desktop-Firewall) für den Schutz eines einzelnen Rechners ausgelegt und wird direkt auf dem zu schützenden System - das heisst auf Ihrem Rechner - installiert.
File Transfer Protocol	FTP ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke. FTP kann beispielsweise verwendet werden, um Webseiten auf einen Webserver zu laden.
Forced Browsing	Bezeichnet eine Technik, mit der versucht wird, verschiedene Verzeichnisse auf einem Webserver ausfindig zu machen, die nicht direkt verlinkt sind (d.h. es gibt auf der "regulären Webseite" keinen Link, welcher auf solche Verzeichnisse zeigt). Solche Verzeichnisse können zum Beispiel sensitive Informationen enthalten. Forced Browsing wird häufig mit entsprechenden Tools automatisiert durchgeführt.
General Packet Radio Service	General Packet Radio Service (deutsch: "Allgemeiner paketorientierter Funkdienst") ist ein paketorientierter Dienst zur Datenübertragung, welcher in GSM-Netzen (Mobilfunknetzen) verwendet wird.
HTTP Response Splitting	HTTP Response Splitting ist eine Sicherheitslücke, welche zur Durchführung von Cross-Site Scripting-Attacken, (Cross-User) Defacements, Web cache poisoning und ähnlichen Exploits verwendet werden kann.
IKE-Aggressive Mode	IKE ist ein Protokoll, das bei IPsec für die Erstellung von so genannten Security Associations (SAs) zuständig ist. SAs definieren unter Anderem, welche kryptographischen Funktionen bei der Verschlüsselung verwendet werden. IKE-Aggressive-Mode ist ein Modus des IKE-Protokolls, welcher potentiell anfällig auf Brute-Force-Attacken ist.
Information Gathering	Zusammenstellen eines umfangreichen Profils über ein Opfer mit Hilfe öffentlich zugänglicher Informationen. Interessante Informationen können z.B. Telefonnummern und Domainnamen sein, aber auch IP-Adressen, Firewallkonfigurationen, verwendete Netzwerkprotokolle, etc.
Integrität	Integrität bedeutet, dass die Daten so beim Empfänger ankommen, wie sie der Sender abgesendet hat (d.h. die Daten werden während der Übertragung nicht arglistig verändert).
Internet Control Message Protocol	Ein Internetprotokoll zum Austausch von Informations- und Fehlermeldungen. ICMP-Pakete werden zum Beispiel beim Pingen verwendet (ICMP Type 8: Echo Request und ICMP Type 0: Echo Reply).
Intrusion Detection System	Systeme, mit denen man unautorisierte Zugriffe auf Daten oder Rechner erkennen kann.
Kollisionsdomäne	Eine Kollisionsdomäne umfasst alle Netzwerkgeräte, die gemeinsam um den Zugriff auf

Begriff	Bedeutung
	ein Übertragungsmedium konkurrieren.
LanManager(LM)-Hashes	Der LAN-Manager-Hash oder LM-Hash ist eine kryptographische Hashfunktion. Sie wird vom Microsoft LAN Manager und teilweise von Windows-NT-basierten Betriebssystemen verwendet, um 128-Bit-Hashwerte von Passwörtern zu speichern.
Malware	Setzt sich aus den englischen Begriffen "Malicious" und "Software" zusammen. In diesem Zusammenhang wird zum Teil auch der Begriff "Malicious Code" verwendet. "Malicious Code" ist ein Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
Metasploit	Metasploit ist ein Framework für Security-Tester, welches erlaubt, vorgefertigte Exploits zu konfigurieren und auf einem Ziel-Host ausführen zu lassen. Ausserdem können auch eigene Exploits mit dem Framework geschrieben werden.
Network Reconnaissance	Bezeichnet das Zusammenstellen eines kompletten Profils der Netzwerkarchitektur eines (Router, Rechner, etc. - jeweils inkl. zugehörige IP-Adressen) Opfers.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.
Ping	Ping ist ein Diagnose-Werkzeug, mit dem überprüft werden kann, ob ein bestimmter Host in einem IP-Netzwerk erreichbar ist.
Ping Sweep	Bei einem Ping Sweep werden mehrere Hosts (typischerweise ganze Netzbereiche) auf Erreichbarkeit geprüft.
Port	Ein Port ist ein "Adressierungsmechanismus", um gewisse Services, die auf einem Rechner laufen, zu adressieren (z.B. Port 80 - HTTP, um eine Webseite von einem Rechner abzurufen).
Portscan	Mit einem Portscan kann bestimmt werden, welche Services auf einem bestimmten Host aktiviert sind.
Promiscuous Mode	Der Promiscuous Mode bezeichnet einen bestimmten Empfangsmodus für netzwerktechnische Geräte. In diesem Modus liest das Gerät den gesamten ankommenden Datenverkehr an die in diesen Modus geschaltete Netzwerkschnittstelle mit und gibt die Daten zur Verarbeitung an das Betriebssystem weiter.
Rainbow Tables	Die Rainbow Table ist eine von Philippe Oechslin entwickelte Datenstruktur, die eine schnelle, probabilistische Suche nach dem einem Hash-Wert zugeordneten Klartext (z.B. ein Passwort) ermöglicht.
Redundant Array of Independent Disks	Ein Verfahren, bei dem die Daten gleichzeitig auf mehrere Festplatten abgelegt werden. Im Falle eines Festplattenfehlers kann somit Datenverlust vermieden werden. Mit RAID-Systemen ist es auch möglich, die Datentransferraten der Festplatten erheblich zu steigern.
Salt	Salt bezeichnet in der Kryptographie eine zufällig gewählte Zeichenfolge, die an einen gegebenen Klartext vor der Verwendung als Eingabe einer Hashfunktion angehängt wird, um die Entropie der Eingabe zu erhöhen.
Supervisory Control and Data Acquisition	Konzept zur Überwachung und Steuerung technischer Prozesse.
(Web-Server) Sample Files	Damit sind Dateien gemeint, die standardmässig mit Webserver-Software ausgeliefert werden, um gewisse Funktionalitäten zu demonstrieren. Solche Dateien können auch missbraucht werden, um an Dateien zu gelangen, die theoretisch nicht von aussen erreicht werden sollten (z.B. ist eine Source Code Disclosure Attacke möglich).
Script Kiddy	Script Kiddies sind jugendliche Leute, die aus Neugierde irgendwelche bekannte Exploits auf einem System ausprobieren wollen. Zwar verstehen Script Kiddies die Hintergründe, wieso eine Attacke funktioniert, meist nicht, allerdings kann der Schaden, den sie mit vorgefertigten Exploits anrichten können, trotzdem sehr gross werden.
Session Hijacking	Bezeichnet das Übernehmen einer bestehenden Session eines Internet-Benutzers durch einen Angreifer (z.B. mit Hilfe von Cookie Stealing).
Sniffing	Sniffing bezeichnet das Abhören des Netzwerkverkehrs. Ein Angreifer kann so auf einfache Art und Weise an sensible Informationen herankommen (insbesondere dann, wenn der Netzwerkverkehr nicht verschlüsselt wurde).
Social Engineering	Social Engineering ist ein mächtiges Werkzeug, mit dem ein Angreifer zum Beispiel unbefugterweise an (nicht öffentliche) Informationen herankommen kann. Der Angreifer täuscht dazu seine Identität vor: Er gibt sich beispielsweise als vertrauenswürdiger Mitarbeiter aus.
Source Code Disclosure	Das ist eine Attacke, welche es dem Angreifer erlaubt, den Source Code einer (Web-) Applikation einzusehen. Mit Hilfe des Source Code kann der Angreifer potenzielle Schwachstellen der Software entdecken. Ausserdem kann es sein, dass z.B. Datenbankpasswörter im Source Code fest kodiert wurden.

Begriff	Bedeutung
SQL Injection	SQL-Injection (SQL-Einschleusung) bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken, die durch mangelnde Überprüfung von zu übermittelnden Variablen entsteht. Der Angreifer versucht dabei eigene Datenbankbefehle einzuschleusen, um Daten in seinem Sinne zu verändern oder Kontrolle über den Server zu erhalten.
Vertraulichkeit	Vertraulichkeit bedeutet, dass nur die Parteien eine Nachricht lesen können, die auch dazu berechtigt sind.
Virtual Private Network	Ermöglicht durch Verschlüsselung des Datenverkehrs eine sichere Kommunikation zwischen Rechnern über öffentliche Netzwerke (z.B. das Internet).
VPN Hacking	Beim VPN-Hacking versucht ein Angreifer, sich über VPN unbefugt in Netzwerk einzuwählen.
Vulnerability	Engl. Begriff für "Schwachstelle".
Wardialing	Wardialing ist eine Technik, um Dial-Up Hacking zu betreiben. Dabei wird ein bestimmter Bereich von Telefonnummern mit spezieller Software durchprobiert, um so potenziell vorhandene Modems ausfindig zu machen.
Web Proxy	Ein Proxy ist ein "Vermittler". Web Proxies dienen als Zwischenschnittstelle zwischen dem Browser und dem Webserver. Solche Proxies können auch von einem Angreifer missbraucht werden, um zum Beispiel Daten, die vom Browser abgesendet wurden, abzufangen und so zu ändern, dass die Webapplikation in einen Ausnahmezustand eintritt.
Webcrawling	Beim Webcrawling wird eine Webseite auf den lokalen Rechner eines Angreifers kopiert und mit speziellen Tools nach sensitiven Informationen (zum Beispiel Passwörter) durchsucht.
Webserver-Hardening	Webserver-Hardening bezeichnet das sichere Konfigurieren eines Webservers.
WHOIS	Die Domainnamen und IP-Adressen, die im Internet verwendet werden, müssen irgendwo zentral verwaltet werden. Auf so genannten WHOIS-Servern erhält man Zugang zu diesen Informationen. Das ist besonders für Hacker interessant, um beispielsweise IP-Adressblöcke und Namensserver seines Opfers zu bestimmen. Aber auch Kontaktinformationen lassen sich abfragen (gemeint sind Kontaktinformationen der Person/Organisation, die eine bestimmte Domain registrieren liess). Mögliche Kontaktinformationen, die sich herauslesen lassen, sind Namen, E-Mail Adresse, Telefonnummer, etc.
Wi-Fi Protected Access	Verbesserte Verschlüsselungsmethode, die bei Wireless-LAN-Verbindungen (WLAN) eingesetzt wird.
Wired Equivalent Privacy	Ein älteres, als unsicher geltendes Verschlüsselungsverfahren, das bei WLAN-Verbindungen eingesetzt wird.
Wireless Hacking	Bezeichnet das unbefugte Eindringen eines Angreifers in ein drahtloses Netzwerk.
Wireless Local Area Network	Wireless Local Area Network steht für drahtloses lokales Netzwerk.
Zombie	Auch unter Bot/Malicious Bot bekannt. Ursprung im slawischen Wort für Arbeit (Robota). Bezeichnet ein Programm, das bestimmte Aktionen nach dem Empfang eines Befehls selbstständig ausführt. So genannte Malicious Bots können kompromittierte Systeme fernsteuern und zur Durchführung beliebiger Aktionen veranlassen.
Zone Transfer	Bei einem Zone Transfer werden Informationen über die gesamte Zone, die von einem DNS Server verwaltet wird, auf einen anderen Rechner transportiert. Dieser Mechanismus wird normalerweise dazu verwendet, um zwei DNS Server miteinander zu synchronisieren, so dass das System im Falle des Ausfalls eines Servers weiterhin funktionstüchtig ist. Werden die DNS-Server unsicher konfiguriert, kann aber auch ein externer Angreifer einen Zone Transfer durchführen und so zum Beispiel an firmeninterne IP-Adressen herankommen.

Literaturverzeichnis

[BSI, 2006]	BSI, Leitfaden IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (2006)
[SN 671'951, 2007]	VSS, Strassenverkehrstelematik: Funktionale Systemarchitektur
[WIsB]	Weisungen über die Informatiksicherheit in der Bundesverwaltung
[Beirer, 2008]	Beirer, Stephan (2008). IT-Security in Automatisierungs- und Prozesssteuerungssystemen. http://www.gai-netconsult.de/WP-SCADA.pdf (19.2.2010)
[ASTRA, 2010]	ASTRA, Fachhandbuch BSA (26.03.2010)
[Lingwood, 2008]	Lingwood, Stephen et al. (2008). IT-Sicherheit für Verkehrstelematiksysteme. Strasse und Verkehr. 3. 21-24
[MELANI, 2009]	Melde- und Analysestelle Informationssicherung MELANI (2009). Informationssicherung - Lage in der Schweiz und international. Halbjahresbericht. 2009/1. 13
[Deck, 2004]	Deck, Bernhard et al. (2004). IT Security for Utility Automation Systems. http://www05.abb.com/global/scot/scot221.nsf/veritydisplay/2e2f181f04faf59ec125705a004db2bc/$File/B5-105.pdf (20.2.2010)
[Falco, 2004]	Falco, Joseph et al. (2004). IT Security for Industrial Control Systems: Requirements Specification and Performance Testing. http://www.isd.mel.nist.gov/projects/processcontrol/members/documents/NDIA_NIST_Paper.pdf (20.2.2010)
[Litteer, 2005]	Litteer, Jerry et al. (2005). Improving SCADA Security. http://csrp.inl.gov/pcsf/2005/d/improving_scada-security-litteer-rohde.pdf (21.2.2010)
[Carlson, 2002]	Carlson, Rolf (2002). Sandia SCADA Program High-Security SCADA LDRD Final Report. http://www.sandia.gov/scada/documents/020729.pdf (21.2.2010)
[Kilman, 2005]	Kilman, Dominique (2005). Framework for SCADA Security Policy. http://www.sandia.gov/scada/documents/sand_2005_1002C.pdf (21.2.2010)
[Robertson, 2003]	Robertson, Bernie (2003). Integrating security into SCADA solutions. http://www.europarl.europa.eu/stoa/archive/workshops/20030910/robertson_slides_en.pdf (21.2.2010)
[Hildick-Smith, 2005]	Hildick-Smith, Andrew (2005). Security for Critical Infrastructure SCADA Systems. http://www.sans.org/reading_room/whitepapers/standards/security_for_critical_infrastructure_scada_systems_1644 (21.2.2010)
[Giani, 2008]	Giani, Annarita et al. (2008). A Testbed for Secure and Robust SCADA Systems. http://www.cs.virginia.edu/sigbed/archives/2008-07/24.pdf (21.2.2010)
[Graham, 2006]	Graham, Robert et al. (2006). SCADA Security and Terrorism: We're not crying wolf. http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf (21.2.2010)
[Igure, 2006]	Igure, Vinay M. et al. (2006). Security issues in SCADA networks. http://www1.elsevier.com/homepage/saf/infosecurity/research/1206_scada.pdf (21.2.2010)
[Mitretek, 1997]	Mitretek Systems (1997). Protecting Our Transportation Systems: An Information Security Awareness Overview. http://www.fhwa.dot.gov/tfhrc/safety/pubs/its/resourceguides/protecttrans.pdf (21.2.2010)
[Byres, 2007]	Byres, Eric et al. (2007). Technical Article: Security Incidents and Trends in SCADA and Process Industries. http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=1823 (24.2.2010)
[Campbell, 2003]	Campbell, Phil et al. (2003). Sustainable Security for Infrastructure SCADA. http://www.sandia.gov/scada/documents/SustainableSecurity.pdf (28.2.2010)
[CPNI]	Centre for the Protection of National Infrastructure (CPNI). Good Practice Guide - Process Control and SCADA Security. http://www.cpni.gov.uk/Docs/Overview_of_Process_Control_and_SCADA_Security.pdf (3.3.2010)
[BITKOM, 2007]	BITKOM (2007). Kompass der IT-Sicherheitsstandards - Leitfaden und Nachschlagewerk. http://www.bitkom.org/files/documents/Kompass_der_IT_Sicherheitstandards_final_12_11_2007.pdf (6.3.2010)
[BITKOM b]	BITKOM. Sicherheit für Systeme und Netze in Unternehmen - Einführung in die IT-Sicherheit und Leitfaden für erste Massnahmen. http://www.bitkom.org/files/documents/ACF897.pdf (6.3.2010)
[BITKOM a]	BITKOM. IT-Risiko- und Chancenmanagement in Unternehmen - Ein Leitfaden für kleinere und mittlere Unternehmen. http://www.bitkom.org/files/documents/Bitkom_Leitfaden_IT-Risikomanagement_V1.0_final.pdf (6.3.2010)
[BMI, 2005]	Bundesministerium des Innern (2005). Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI). http://www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13576/Nationaler_Plan_Schut

	z_Informationsinfrastrukturen.pdf (6.3.2010)
[BMI]	Bundesministerium des Innern. Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf (6.3.2010)
[BSI]	Bundesamt für Sicherheit in der Informationstechnik. Kritische Infrastrukturen in Staat und Gesellschaft. https://www.bsi.bund.de/cae/servlet/contentblob/476046/publicationFile/29279/F17KritischeInfrastruktur_pdf.pdf (6.3.2010)
[BSI, 2008]	Bundesamt für Sicherheit in der Informationstechnik (2008). Informationstechnik in der Prozessüberwachung und -steuerung - Grundsätzliche Anmerkungen. https://www.bsi.bund.de/cae/servlet/contentblob/476032/publicationFile/40996/IT_in_der_Prozesssteuerung_pdf.pdf (6.3.2010)
[A-SIT, 2007]	Zentrum für sichere Informationstechnologie (A-SIT) (2007). Österreichisches Informationssicherheitshandbuch. http://www.a-sit.at/pdfs/OE-SIHA_I_II_V2-3_2007-05-23.pdf (7.3.2010)
[Fink, 2006]	Fink, Raymond K. et al. (2006). Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems. http://www.inl.gov/scada/publications/d/nstb_lessons_learned_from_cyber_security_assessments.pdf (7.3.2010)
[NIST, 1995]	National Institute of Standards and Technology. An Introduction to Computer Security: The NIST Handbook. http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (7.3.2010)
[Bowen, 2006]	Bowen, Pauline et al. (2006). Guide for Developing Security Plans for Federal Information Systems. http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf (7.3.2010)
[Duggan, 2005]	Duggan, David P. (2005). Penetration Testing of Industrial Control Systems. http://www.sandia.gov/scada/documents/sand_2005_2846p.pdf (7.3.2010)
[Schneier, 1999]	Schneier, Bruce (1999). Attack Trees. Dr. Dobb's Journal. 12. 21-29
[McClure, 2009]	McClure, Stuart et al. (2009). Hacking Exposed 6: Network Security Secrets & Solutions. McGraw-Hill
[Ollmann, 2004]	Ollmann, Gunter (2004). Passive Information Gathering - The Analysis of Leaked Network Security Information. http://www.ngssoftware.com/Libraries/Documents/Passive_Information_Gathering_-_The_Analysis_of_Leaked_Network_Security_Information.sflb.ashx (23.5.2010)
[Grossman, 2003]	Grossman, Jeremiah (2003). Cross-Site Tracing (XST). http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf (22.7.2010)
[Hills, 2005]	Hills, Roy (2005). Common VPN Security Flaws. http://www.nta-monitor.com/posts/2005/01/VPN-Flaws-Whitepaper.pdf (22.7.2010)
[YEHG, 2008]	YGN Ethical Hacker Group (2008). Multiple Tricky Ways To Protect Sensitive Files & Directories Of Your Critical Web Applications. http://yehg.net/lab/pr0js/papers/MULTIPLE%20TRICKY%20WAYS%20TO%20PROTECT.pdf (23.7.2010)
[Dravet, 2008]	Dravet, J. (2008). Cracking Passwords Version 0.8. http://forums.remote-exploit.org/66562-post1.html (6.8.2010)
[NIST, 2006]	Burr, William E. et al. (2006). Electronic Authentication Guide. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf (13.8.2010)
[Bögeholz, 2005]	Bögeholz, Harald (2005). Bärendienst - Wie ATA-Sicherheitsfunktionen Ihre Daten gefährden. c't. 8. 172-175
[Hatfield, 2006]	Hatfield, Jim (2006). ATA Security feature Set Clarifications. http://www.t13.org/documents/UploadedDocuments/docs2006/e05179r4-ACS-SecurityClarifications.pdf (23.9.2010)
[Bosen, 2007]	Bosen, Bill (2007). Hard Drive Passwords Easily Defeated; the Truth about Data Protection. http://www.wwpi.com/?option=com_content&task=view&id=2669&Itemid=129 (23.9.2010)
[Benz, 2005]	Benz, Benjamin (2005). Datentresor - Verschlüsselte Festplatten schützen vor Datenklau. c't. 7. 136-139
[Gleissner, 2008]	Gleissner, Werner (2008). Grundlagen des Risikomanagements im Unternehmen. Vahlen
[MELANI, 2010]	Melde- und Analysestelle Informationssicherung MELANI (2010). Informationssicherung - Lage in der Schweiz und international. Halbjahresbericht. 2010/1. 7-8
[Gresser, 2006]	Gresser, Christian H. (2006). Hacking SCADA/SAS Systems - Used Techniques, Known Incidents and Possible Mitigations. http://www.ptil.no/getfile.php/z Konvertert/Health, safety and environment/Safety and working environment/Dokumenter/microsoftpowerpoint4hackingscadaptil.pdf (9.11.2010)
[BSG, 2008]	Baer, Dietrich (2008). BSG ITSEC Advice Catalog, praktische Sicherheitsmassnahmen

[NISCC, 2006]	National Infrastructure Co-Ordination Centre (2006). Good Practice Guide Patch Management. http://www.cpni.gov.uk/Docs/re-20061024-00719.pdf (10.1.2011)
[NIST, 2008]	Falco, Joe et al. (2008). Guide to Industrial Control Systems (ICS) Security. http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf (10.1.2011)
[DHS, 2009]	US. Department of Homeland Security (2009). Catalog of Control System Security Requirements. http://www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf (10.1.2011)
[CPNI, 2007]	Centre for the Protection of National Infrastructure (2007). Personnel Security : Threats, Challenges and Measures. http://www.cpni.gov.uk/Docs/Pers_Sec_TCM_v2.pdf (10.1.2011)
[NIST, 2005]	Bergeron, Tiffany (2005). Creating a Patch and Vulnerability Management Program. http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf (10.1.2011)
[Rövekamp, 2010]	Rövekamp, Lucas (2010). ISDS INA - Security Strategie.

Projektabschluss

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK
Bundesamt für Strassen ASTRA

FORSCHUNG IM STRASSENWESEN DES UVEK **ARAMIS SBT**

Formular Nr. 3: Projektabschluss

erstellt / geändert am:	24.03.2011

Grunddaten

Projekt-Nr.:	**VSS2007 / 904**
Projekttitel:	IT-Security im bereich Verkehrstelematik
Enddatum:	28.04.2011

Texte:

Zusammenfassung der Projektresultate:

Das Forschungsprojekt erarbeitet nach einem vierstufigen Standardverfahren des Bundesamts für Sicherheit in der Informationstechnik (BSI) ein Sicherheitskonzept für Betriebs- und Sicherheitsausrüstungen (BSA) der Verkehrstelematik.

In der ersten Stufe wird die Schutzbedürftigkeit der Anlagen an Hand von breit ausgelegten Interviews sowie einem umfassenden Literaturstudium ermittelt. Dabei wird der Verfügbarkeit der Anlagen das höchste Schutzziel zugewiesen.

Die zweite Stufe analysiert systematisch realistische Bedrohungsszenarien. Daraus resultiert eine Menge sinnvoller Angriffsvektoren. Diese werden verwendet um bei den Interviewpartnern die Systeme auf bereits umgesetzte Sicherheitsmassnahmen zu überprüfen und Schwachstellen hervorzuheben.

In der dritten Stufe wird eine Risikoanalyse durchgeführt. Die Resultate der Risikoanalyse zeigen, dass keine Angriffsvektoren mit katastrophalen Konsequenzen und hohen Eintrittswahrscheinlichkeiten vorhanden sind. Allerdings sind doch einige Angriffsvektoren vorhanden, die kritische Konsequenzen haben und gelegentlich eintreten könnten.

Die vierte Stufe umfasst eine sinnvolle Menge von Massnahmen, die für die Reduktion der in der Risikoanalyse erkannten Risiken für BSA Anlagen relevant sind. Diese können den Gebietseinheiten oder einer VM-Zentrale als Hilfsmittel zur Verfügung gestellt werden.

	Das Forschungsprojekt schliesst mit Empfehlungen für den Betrieb ab.
Zielerreichung:	Die Ziele des Forschungsprojekts sind erreicht. Insbesondere konnten: – IT-Security-Regeln für die Betriebs- und Sicherheitsausrüstungen sowie für VM-Zentralen und Gebietseinheiten festgelegt werden. – Verkehrstelematik-Anwendungen, elektromechanische Anlagen für Strassen und Tunnels, Verkehrs- und Betriebsleitsysteme sowie zugehörige Netz-werk- und Kommunikationskomponenten auf Sicherheitslücken untersucht werden. – Mögliche technischen und organisatorischen Massnahmen abgestimmt auf das spezifische Verkehrsumfeld (Bund, Gebietseinheiten, Kantone und Städte) in Form eines Massnahmenkatalogs beschrieben werden.
Folgerungen und Empfehlungen:	Eine wesentliche Erkenntnis aus dem Forschungsprojekt ist, dass in IT-Netzwerken mit BSA-Anlagen die IT-Schutzziele grundsätzlich anders bewertet werden als in herkömmlichen Netzwerken wie zum Beispiel der Büroautomation. Das oberste Schutzziel ist eindeutig die Verfügbarkeit. Auch die Integrität der Daten ist wichtig, denn mit fehlerhaften oder gar bewusst manipulierten Daten kann ein reibungsloser Betrieb nicht mehr gewährleistet werden. Bei herkömmlichen Netzen sind die Prioritäten der Schutzziele genau umgekehrt: Hier geniesst die Vertraulichkeit der Geschäftsdaten oft die oberste Priorität. Eine weitere Folgerung aus dem Forschungsprojekt ist, dass die VT-Systeme nicht alleine durch technische Massnahmen gesichert werden können, sondern dass es einen Mix aus technischen, organisatorischen und physischen Massnahmen braucht. Die Dritte Folgerung ist dass IT-Security ein kontinuierlicher Prozess ist wo die Gefahrenlage sich stetig aufgrund neuer und sich ändernder Bedrohungen verändert. Die Sicherheitsmassnahmen müssen deshalb laufend hinterfragt und bei Bedarf überarbeitet werden. Es wird vorgeschlagen den Massnahmenkatalog im Kapitel 9 als Grundlage für eine Richtlinie zu verwenden.
Publikationen:	Forschungsbericht VSS 2007 / 904 "IT-Security im Bereich Verkehrstelematik", April 2011

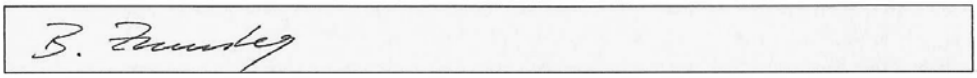
Beurteilung der Begleitkommission:
Diese Beurteilung der Begleitkommission ersetzt die bisherige separate fachliche Auswertung.

Beurteilung:	**Zielsetzungen** wurden vollumfänglich erfüllt. **Methode und Vorgehen** sind zweckmässig, praxisbezogen und auf die aktuellen Systeme abgestützt. **Resultate** sind in Kapitel 9 in einer generischen, praxisbezogenen Checkliste zusammengefasst. **Zusammenarbeit** zwischen Forschungsteam und BK waren stets sehr angenehm, zielorientiert und effizient.
Umsetzung:	Die Umsetzung der Erkenntnisse aus der vorliegenden Forschungsarbeit hat für die Betreiber und Benutzer von VT-Systemen (ASTRA, kantonale und städtische Tiefbauämter und Polizei etc.) grosse Bedeutung, da deren Nichtbeachtung für Verkehrsteilnehmer und Volkswirtschaft durch unerwartete Verkehrsbehinderungen erhebliche Folgen haben können. Insbesondere die Übertragung der generischen Checkliste gemäss Kapitel 9 in entsprechende Weisungen, Vorgaben, Richtlinien oder techn. Merkblätter kann für die verantwortlichen VT-System-Planer, - Betreiber und Benutzer ein wertvolles Hilfsmittel sein und entscheidend zur Verfügbarkeit und Sicherheit der VT-Systeme beitragen.
weitergehender Forschungsbedarf:	Keiner Regelmässige Überprüfung und Aktualisierung erforderlich, da die Bedrohungslage mit dem Wandel der Technik kurzfristig ändern kann.
Einfluss auf Normenwerk:	Da bei der IT-Security organisatorische, technische und physische Aspekte zu berücksichtigen sind, sind bei der aktuell verfügbaren, heterogenen VT-Systemlandschaft keine allgemein verbindlichen CH-Normen vorgesehen. Es liegt in der Verantwortung der Betreiber und Benutzer von VT-Systemen die Erkenntnisse aus der Forschungsarbeit (vorwiegend Kapitel 9) in geeigneter Form in ihre Arbeitsprozesse und Betriebsvorschriften einzubinden.

Präsident Begleitkommission:

Name:	Zumsteg	Vorname:	Beat
Amt, Firma, Institut:	R. Brüniger AG		
Strasse, Nr.:	Zwillikerstrasse 8		
PLZ:	8913	Email:	beat.zumsteg@R-BRUENIGER-AG.CH
Ort:	Ottenbach	Telefon:	044 760 00 66
Kanton, Land:		Fax:	044 760 00 68

Unterschrift Präsident Begleitkommission:



Verzeichnis der Berichte der Forschung im Strassenwesen

Forschungsberichte seit 2009

Bericht-Nr.	Projekt Nr.	Titel	Datum
616	AGB 2002/020	Beurteilung von Risiken und Kriterien zur Festlegung akzeptierter Risiken in Folge aussergewöhnlicher Einwirkungen bei Kunstbauten *Appréciation et critères d'acceptation des risques dus aux actions extraordinaires pour les ouvrages d'art* *Assessment of residual risks and acceptance criteria for accidental loading for infrastructural facilities*	2009
618	AGB 2005/102	Sicherheit des Verkehrssystems Strasse und dessen Kunstbauten: Methodik zur vergleichenden Risikobeurteilung *Bases d'une méthode pour une appréciation comparative des risques* *Methodological basis for comparative risk assessment*	2009
620	AGB 2005/104	Sicherheit des Verkehrssystems Strasse und dessen Kunstbauten: Effektivität und Effizienz von Massnahmen *Efficacité et efficience des interventions* *Effectiveness and efficiency of interventions*	2009
623	AGB 2005/107	Sicherheit des Verkehrssystems Strasse und dessen Kunstbauten: Tragsicherheit der bestehenden Kunstbauten *Sécurité structurale des ouvrages d'art existants* *Structural safety of existing highway structures*	2009
625	AGB 2005/109	Sicherheit des Verkehrssystems Strasse und dessen Kunstbauten: Effektivität und Effizienz von Massnahmen bei Kunstbauten *Efficacité et efficience des interventions sur les ouvrages d'art* *Effectiveness and efficiency of interventions on highway structures*	2009
626	AGB 2005/110	Sicherheit des Verkehrssystems Strasse und dessen Kunstbauten: Baustellensicherheit bei Kunstbauten *Sécurité sur les chantiers d'ouvrages d'art* *Safety on constructions sites off highway structures*	2009
636	AGB 2002/028	Dimensionnement et vérification des dalles de roulement de ponts routiers *Bemessung und Nachweis der Fahrbahnplatten von Strassenbrücken* *Design and verification of bridge deck slabs for highway bridges*	2009

Bericht-Nr.	Projekt Nr.	Titel	Datum
637	AGB 2005/009	Détermination de la présence de chlorures à l'aide du Géoradar *Georadar zur Auffindung von Chloriden* *Detection of chlorides using ground penetrating radar*	2009
1233	ASTRA 2000/420	Unterhalt 2000 Forschungsprojekt FP2 Dauerhafte Komponenten bitumenhaltiger Belagsschichten *Components durables des couches bitumineux* *Durable components in bituminous layers*	2009
1237	VSS 2007/903	Grundlagen für eCall in der Schweiz *Bases pour eCall en Suisse* *Technical and organisational basis for eCall in Switzerland*	2009
1239	VSS 2000/450	Bemessungsgrundlagen für das Bewehren mit Geokunststofffen *Bases de dimensionnement pour le renforcement par géosyntétiques* *Design of reinforcement with geosynthetics*	2009
1240	ASTRA 2002/010	L'acceptabilité du péage de congestion: Résultats et analyse de l'enquête en Suisse *Stau auf Strassen: Resultate und Analysen von Untersuchungen in der Schweiz* *Acceptance of road pricing: results and analysis of surveys carried out in Switzerland*	2009
1241	ASTRA 2001/052	Erhöhung der Aussagekraft des LCPC Spurbildungstests *Amélioration des informations fournies par l'essai d'orniérage LCPC* *Improving information on materials behaviour oblainded from the LCPC wheel tracking test*	2009
1246	VSS 2004/713	Massnahmenplanung im Erhaltungsmanagement von Fahrbahnen: Bedeutung Oberflächenzustand und Tragfähigkeit sowie gegenseitige Beziehung für Gebrauchs- und Substanzwert *Influences et interactions de l'état de surface et de la portance sur la valeur intrinsèque et la valeur d'usage* *Influences and interactions of the surface quality and the bearing capacity on the intrinsic value and the user value*	2009
1247	VSS 2000/348	Anforderungen an die strassenseitige Ausrüstung bei der Umwidmung von Standstreifen	2009

Bericht-Nr.	Projekt Nr.	Titel	Datum
		Exigences à l'équipement routier pour l'utilisation de la bande d'arrêt d'urgence *Requirements for road side equipment by hard shoulder usage*	
1249	FGU 2003/004	Einflussfaktoren auf den Brandwiderstand von Betonkonstruktionen *Facteurs d'influence sur la résistance au feu de structures en béton* *Influences on the fire resistance of concrete structures*	2009
1252	SVI 2003/001	Nettoverkehr von verkehrsintensiven Einrichtungen (VE) *Trafic net des installations générant un trafic important (IGT)* *Net traffic induction of installations producing high traffic volumes (VE)*	2009
1253	VSS 2001/203	Rétention des polluants des eaux de chausées selon le système "infilitrations sur les talus". Vérification in situ et optimisation *Retention der Schadstoffe des Strassenabwassers durch das "über die Schulter Versickerungs-System". In situ Verifikation und Optimierung* *Road runoff pollutant retention by infiltration through the Roadside Slopes. In Situ verification and optimization*	2009
1254	VSS 2006/502	Drains verticaux préfabriqués thermiques pour la consolidation in-situ des sols *Vorfabrizierte, vertikale, thermische Entwässerungsleitungen für die in-situ Konsolidierung von Böden* *Prefabricated thermal vertical drains for in-situ consolidaation of soils*	2009
1255	VSS 2006/901	Neue Methoden zur Erkennung und Durchsetzung der zulässigen Höchstgeschwindigkeit *Nouvelles méthodes pour reconnaitre et faire respecter la vitesse maximale autorisée* *New methods to identify and enforce the authorized speed limit*	2009
1256	VSS 2006/903	Qualitätsanforderungen an die digitale Videobild-Bearbeitung zur Verkehrsüberwachung *Exigences de qualité posées au traitement vidéo numérique pour la surveillance du traffic routier* *Quality requirements for digital video-analysis in traffic surveillance*	2009
1257	SVI 2004/057	Wie Strassenraumbilder den Verkehr beeinflussen Der Durchfahrtswiderstand als Arbeitsintrument bei der städtebaulichen Gestaltung von Strassenräumen *L'influence de l'aménagement de l'espace de la route sur le trafic*	2009

Bericht-Nr.	Projekt Nr.	Titel	Datum
		La résistance de passage du trafic comme instrument de travail pour la conception urbaine de zone routière	
1258	VSS 2005/802	Kaphaltestellen Anforderungen und Auswirkungen *Arrêt en cap - exigences et effets* *Cape stops - requirements and impacts*	2009
1260	FGU 2005/001	Testeinsatz der Methodik "Indirekte Vorauserkundung von wasserführenden Zonen mittels Temperaturdaten anhand der messdaten des Lötschberg-Basistunnels *Test de la méthode "Prédiction indirecte de zones de venue d'eau au moyen de données thermiques" à l'aide des données du tunnel de base du Lötschberg* *Test of the method "indirect prediction ahead of water bearing zones with temperatures data" with the measured data from the Lötschberg-Basisitunnel*	2009
1261	ASTRA 2004/018	Pilotstudie zur Evaluation einer mobilen Grossversuchsanlage für beschleunigte Verkehrslastsimulation auf Strassenbelägen *Etude de pilote pour l'évaluation d'une machine mobile à vrai grandeur qui permet de simuler le trafic sur les routes dans une manière accélérée* *Pilot-study for the evaluation of a mobile full-scale accelerated pavement testing equipment*	2009
1262	VSS 2003/503	Lärmverhalten von Deckschichten im Vergleich zu Gussasphalt mit strukturierter Oberfläche *Caractéristiques de bruit de couches de roulement en comparaison avec des couches d'asphalte coulé (Gussasphalt) avec surface construite* *Comparison of noise characteristics of wearing courses with mastic asphalt (Gussasphalt) with designed surface*	2009
1264	SVI 2004/004	Verkehrspolitische Entscheidfindung in der Verkehrsplanung *Politique de transport: la prise de décision dans la planification des transports* *Transport-potry decision-talking in transport planning*	2009

Bericht-Nr.	Projekt Nr.	Titel	Datum
1265	VSS 2005/701	Zusammenhang zwischen dielektrischen Eigenschaften und Zustandsmerkmalen von bitumenhaltigen Fahrbahnbelägen (Pilotuntersuchung) *Relation entre les propriétés diélectiques des revêtements routiers et leur condition* *A relationship between the dielectric properties of asphalt pavements and the present condition of the road*	2009
1267	VSS 2007/902	MDAinSVT Einsatz modellbasierter Datentransfernormen (INTERLIS) in der Strassenverkehrstelematik *Utilisation des standards d'échange de données basés modélisation pour la télématique des transports routiers à l'exemple des données de trafic* *Use of modal driven data transfer standards in the road transport telematic exemplified by traffic data*	2009
1268	ASTRA 2005/007	PM10-Emissionsfaktoren von Abriedspartikeln des Strassenverkehrs (APART) *PM10 emission factors of abrasion particles from road traffic* *Facteurs d'émission des particules d'abrasion dues au trafic routiers*	2009
1269	VSS 2005/201	Evaluation von Fahrzeugrückhaltesystemen im Mittelstreifen von Autobahnen *Evaluation of road restraint systems in central reserves of motorways* *évaluation de dispositifs de retenue de véhicule sur le terre-plein central des autoroutes*	2009
1270	VSS 2005/502	Interaktion Strasse Hangstabilität: Monitoring und Rückwärtsrechnung *Interaction route - stabilité des versants: Monitoring et calcul à rebours* *Road-landslide interactions: Monitoring and inverse stability analysis*	2009
1271	VSS 2004/201	Unterhalt von Lärmschirmen *Entretien des écrans antibruit* *Maintenance of noise reducing devices*	2009
1274	SVI 2004/088	Einsatz von Simulationswerkzeugen in der Güterverkehrs- und Transportplanung *Applications des modèles simulations dans le domaine de planification en transport marchandises* *Application of simulation tools in freight traffic and transport planning*	2009

Bericht-Nr.	Projekt Nr.	Titel	Datum
1275	ASTRA 2006/016	Dynamic Urban Origin - Destination Matrix - Estimation Methodology *Méthodologie pour l'estimation de matrices origine-destination dynamiques en réseau urbain* *Methode zur Ermittlung dynamischer Quell-Ziel-Matrizen für städtische Netzwerke*	2009
1278	ASTRA 2004/016	Auswirkungen von fahrzeuginternen Infor,ationssystemen auf das Fahrverhalten und die Verkehrssicherheit - Verkehrstechnischer Teilbericht *Influence des systemes d'information embarqués sur le comportement de conduite et la sécurité routière* *Rapport partiel d'ingéniérie de la circulation* *Influence of In-Vehicle Information Systems or driver behaviour and road safety* *Report part of traffic engineering*	2009
1279	VSS 2005/301	Leistungsfähigkeit zweistreifiger Kreisel *Capacité des giratoires à deux voies de circulation* *Capacity of two-lane roundabouts*	2009
1285	VSS 2002/202	In-situ Messung der akustischen Leistungsfähigkeit von Schallschirmen *Mesures in-situ des propriétés acoustiques des écrans anti-bruit* *In-situ measurement of the acoustical properties of noise barriers*	2009
1287	VSS 2008/301	Verkehrsqualität und Leistungsfähigkeit von komplexen ungesteuerten Knoten: Analytisches Schätzverfahren *Procédure analytique d'estimation de la capacité et du niveau de service de carrefours sans feux complexes* *Analytic procedure to estimate capacity and level of service at complex uncontrolled intersections*	2009
619	AGB 2005/103	Sicherheit des Verkehrssystems / Strasse und dessen Kunstbauten / Ermittlung des Netzrisikos *Estimation du risque pour le réseau* *Estimation of the network risk*	2010
624	AGB 2005/108	Sicherheit des Verkehrssystems / Strasse und dessen Kunstbauten / Risikobeurteilung für Kunstbauten *Appréciation des risques pour les ouvrages d'art* *Risk assessment for highway structures*	2010

Bericht-Nr.	Projekt Nr.	Titel	Datum
945	AGB 2005/021	Grundlagen für die Verwendung von Recyclingbeton aus Betongranulat *Bases pour l'utilisation du béton de recyclage en granulats de béton* *Fundamentals for the use of recycled concrete comprised of concrete material*	2010
1272	VSS 2007/304	Verkehrsregelungssysteme - behinderte und ältere Menschen an Lichtsignalanlegen *Aménagement des feux de signalisation pour les personnes a mobilité réduite ou âgées* *Traffic control systems - Handicapped and older people at signalized intersections*	2010
1277	SVI 2007/005	Multimodale Verkehrsqualitätsstufen für den Strassenverkehr - Vorstudie *Niveaux de service multimodales de la circulation routière - études préliminaires* *Multimodal level of service of road traffic - preliminary study*	2010
1282	VSS 2004/715	Massnahmenplanung im Erhaltungsmanagement von Fahrbahnen: Zusatzkosten infolge Vor- und Aufschub von Erhaltungsmassnahmen *Coûts supplémentaires engendrés par l'exécution anticipée ou retardée des mesures d'entretien* *Additional costs caused by bringing forward or delaying of standard interventions for road maintenance*	2010