Selcuk Nisanciogiu, Dr.-Ing., Bundesanstalt für Straßenwesen (BASt), Bergisch Gladbach (D)
Kalliopi Anastassiadou, Dr.-Ing., Bundesanstalt für Straßenwesen (BASt), Bergisch Gladbach (D)
Kai Jacobsen, Dipl.-Math., Dürr Group GmbH, Kiel (D)
Christian Thienert, Dr.-Ing., STUVA e. V., Köln (D)

Erhöhung der Cyber-Sicherheit von Tunnelleitzentralen: Potenzielle Bedrohungen, Bestandsanalyse, Penetrationstests, Leitfaden, Analysesoftware

Tunnelleitzentralen übernehmen wichtige Funktionen für die Gewährleistung der Verfügbarkeit des Straßenverkehrsnetzes. In ihnen werden Überwachungs- und Steuerungsmöglichkeiten von Tunneln gebündelt. Da diese Funktionen durch IT-Systeme gesteuert werden, wird der Schutz vor Cyber-Angriffen zu einer wachsenden Herausforderung. Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Forschungsprojekt Cyber-Safe verfolgt daher das Ziel, Leitzentralenbetreiber in die Lage zu versetzen, Gefährdungen durch Cyber-Angriffe besser als bisher zu erkennen und systematisch geeignete Schutzmaßnahmen zu ergreifen.

Improvement of the Cyber Security of Tunnel Control Centres: Potential Threats, Analysis of the Existing Situation, Penetration Tests, Guideline, Analysis Software

Tunnel control centres, where surveillance and control systems are bundled, undertake important functions to ensure the availability of the road network. Since these functions are controlled by IT systems, protection against cyber-attacks is a growing challenge. The Cyber-Safe research project, sponsored by the Federal Ministry of Education and Research (BMBF), thus has the aim of placing the operators of control centres in a position to detect threats from cyber-attacks better and introduce systematically suitable protection measures.

1 Einleitung

Mobilität und Verkehr sind Grundlagen einer modernen Gesellschaft und ihrer wirtschaftlichen Prosperität. Eine zentrale Voraussetzung ist daher die Gewährleistung der Verfügbarkeit des Verkehrsnetzes. Eine wichtige Aufgabe übernehmen in diesem Zusammenhang Tunnelleitzentralen, welche die Überwachung und Steuerung des Verkehrs in Tunneln ermöglichen, um im Ereignisfall Maßnahmen zur Gewährleistung der Sicherheit der Tunnelnutzer einleiten zu können. Da diese Leitzentralen zunehmend mit IT-Systemen ausgestattet werden, gewinnt ihr Schutz vor Cyber-Angriffen erheblich an Bedeutung. Die Schadsoftware BlackEnergy der Sandworm-Gruppe sabotierte im Jahre 2015 Energieversorger in der Ukraine, mit der Folge, dass mindestens 225.000 Einwohner von einem mehrstündigen Ausfall der Stromversorgung betroffen waren. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde diese Schadsoftware im Wesentlichen gegen Organisationen aus den Sektoren Energie sowie Transport und Verkehr eingesetzt und sollte nicht nur Betreiber, sondern auch indirekt die Bevölkerung treffen [1].

Eine im Rahmen des Forschungsprojekts Cyber-Safe durchgeführte Recherche zu bisher erfolgten Cyber-Angriffen auf Verkehrsinfrastrukturen belegt ebenfalls die Notwendigkeit zu handeln: Im Jahre 2015 musste der bei Haifa (Israel) gelegene und durch das Carmel-Gebirge führende ca. 9 km lange Carmel-Tunnel infolge eines gezielten Hacker-Angriffs für die Dauer von 8 h gesperrt werden, was zu schwerwiegenden Verkehrsbeeinträchtigungen führte [2]. Auch ist vor dem Hintergrund der Entwicklungen im Bereich der intelligenten Verkehrsinfrastrukturen davon auszugehen, dass diese zukünftig immer enger in den Fokus von Cyber-Angreifern rücken werden. Darüber hinaus wurden mit der ersten Verordnung zur Änderung der BSI-Kritisverordnung (KritisV) [3] die Schwellenwerte für den Sektor Transport und Verkehr festgelegt. Demnach gelten grundsätzlich Anlagen wie Verkehrssteuerungs- und Leitsysteme für das Netz der Bundesautobahnen als kritisch und sind entsprechend zu schützen.

Ziel des Projekts Cyber-Safe ist es daher, Handlungshilfen zu entwickeln, welche die Betreiber von Tunnelleitzentralen in die Lage versetzen, mögliche Gefährdungen durch Cyber-Angriffe zielgerichteter als bislang zu erkennen und geeignete Schutzmaßnahmen zu ergreifen. Hierzu wurden im Rahmen einer Bestandsanalyse bereits umgesetzte Maßnahmen auf ihre Effektivität und Wirksamkeit hin überprüft und gleichzeitig bestehende Defizite identifiziert. Ergänzt wird diese Analyse durch einen Penetrationstest, der im Zuge einer detaillierten Tiefenanalyse Einblicke in die IT-Systeme liefern soll.

Um die unmittelbare Umsetzbarkeit der zu entwickelnden Handlungshilfen zu erreichen, wurden zwei Workshops mit Betreibern, Ausstattern und Planern von Leitzentralen durchge-

führt. Hierbei wurden der Bedarf sowie die Anforderungen an Handlungshilfen zur Bewertung der aktuell vorhandenen IT-Sicherheit und Steigerung der Widerstandsfähigkeit gegen Cyber-Angriffe ermittelt [4]. Diese wertvollen Erkenntnisse bezüglich des Nutzerbedarfs werden derzeit in drei zielgruppenorientierte Handlungshilfen überführt und mit Abschluss des Projekts für die direkte Nutzung in der Praxis Betreibern, Ausstattern sowie Planern von Leitzentralen zur Verfügung gestellt.

2 Bestandsanalyse und potenzielle Bedrohungen

Im ersten Schritt erfolgte eine Bestandsanalyse der vorhandenen IT-Systeme und Schutzmaßnahmen unterschiedlicher Leitzentralen auf Grundlage der IT-Grundschutz-Kataloge des BSI [5], die im Vorfeld auf die besonderen Gegebenheiten von Leitzentralen angepasst und konkretisiert wurden. Um ein möglichst differenziertes Bild zu erhalten, wurden Betreiber im gesamten Bundesgebiet befragt. Die Analyse unterscheidet hierbei nach technischen, organisatorischen und personellen sowie chronologisch nach präventiven, mitigativen und restorativen Maßnahmen. Auf dieser Grundlage wurden auch Aussagen über die Qualität der vorhandenen Maßnahmen zur Ereignisvermeidung, Schadensminimierung und Wiederherstellung der Leitstellenfunktionen nach erfolgten Cyber-Angriffen getroffen und in einen Maßnahmenkatalog überführt. Berücksichtigt wurden in diesem Zusammenhang insbesondere die durch das BSI empfohlenen Maßnahmen. Wichtige Voraussetzung für die Entwicklung des Maßnahmenkatalogs war neben der Identifizierung auch die Klassifizierung potenzieller Gefahren. Unterschieden wird hierbei nach:

- Der Art (von innen/außen),
- Dem Ziel (Störung, Zweckentfremdung, Zerstörung),
- Den möglichen Auswirkungen (Funktionsverlust, Sachschaden),
- Der Eintrittswahrscheinlichkeit der Angriffe.

Ausgehend vom Angriffspunkt „Leitzentrale" bestehen für Cyber-Angriffe diverse Möglichkeiten der Einflussnahme auf die Steuerungseinheiten der Tunnelanlagen. Hier besteht die Möglichkeit der Manipulation von Sensordaten, des Blockierens von Steuerbefehlen oder auch einer Ausführung von nicht situationskonformen Steuerungsmaßnahmen.

Die Bestandsanalyse liefert darüber hinaus auch die notwendigen Grundlagen für die Entwicklung der sogenannten virtuellen Leitzentrale, die einen repräsentativen Querschnitt der vorgefunden IT-Systeme darstellt und als Testumgebung für Angriffe und die Bewertung der Wirksamkeit von Schutzmaßnahmen im Rahmen des Projekts genutzt wird.

3 Penetrationstests

Im Rahmen der Schwachstellenanalyse erfolgt ein zweistufiger Penetrationstest in einer Tunnelleitzentrale, um weitere konkrete Schwachstellen zu identifizieren. Ein Penetrationstest im laufenden Betrieb birgt grundsätzlich immer die Gefahr, dass er zu Abstürzen, Verlust der Verfügbarkeit, aber auch zu einer temporären Verletzung von Sicherheitsvorgaben führen kann. Aus diesen Gründen ist ein auf dem Gebiet der kritischen Infrastrukturen erfahrener IT-Spezialist mit der Durchführung beauftragt worden, der die sorgfältige Planung und Ausführung in enger Absprache mit dem Betreiber sowie dem technischen Ausstatter der Leitzentrale konzipiert und durchführt. Ganz wesentlich hierbei ist die Festlegung der Betrachtungsgrenzen sowie der Abbruchkriterien der Penetrationstests. Das so entwickelte Testprogramm orientiert sich eng an den Empfehlungen des BSI [6] und beinhaltet im Detail folgendes Vorgehen:

- Erstellung eines Konzepts zur Durchführung eines zweistufigen Penetrationstests,
- Durchführung des ersten Penetrationstests,
- Ableitung und Umsetzung von Härtungsmaßnahmen,
- Durchführung eines zweiten Penetrationstests, um die Wirksamkeit der umgesetzten Härtungsmaßnahmen zu bewerten,
- Ableitung weiterer Härtungsmaßnahmen und weiterer Handlungsempfehlungen.

Als erste wichtige Erkenntnis zum aktuellen Zeitpunkt kann festgehalten werden, dass ein Penetrationstest tiefergehende und wertvolle Erkenntnisse liefern kann. Insbesondere wurde festgestellt, dass es bei der Umsetzung von Maßnahmen der Leitzentralentechnik zu Abweichungen von der eigentlichen Planung kam. Diese können zu potenziellen Schwachstellen führen. Daher kann die Empfehlung ausgesprochen werden, Penetrationstests prinzipiell bei der Abnahme von Leitzentralentechnik durchzuführen und diese bereits in der Planung und Ausschreibung vorzusehen.

4 Handlungshilfen

Im Zuge der Befragungen und Workshops mit Betreibern von Leitzentralen konnten wertvolle Erkenntnisse zu Bedarf und Nutzeranforderungen an die zu entwickelnden Handlungshilfen gesammelt werden. Diese Handlungshilfen, die aus drei Software-Tools und einem Leitfaden bestehen, sollen Betreiber von Leitzentralen in die Lage versetzen, Hinweise auf Schwachstellen in ihrem IT-System und ihren Organisationsstrukturen zu erkennen. In diesem Zusammenhang sind bei der Entwicklung zwei wesentliche Randbedingungen zu beachten. Zum einen dürfen die Empfehlungen keine Widersprüche zu existierenden Regelwerken, vor allem zum BSI-Grundschutz-Katalog und der ISO 27000-Reihe [7], enthalten. Zum anderen handelt es sich bei praktisch allen Tunnelleitzentralen um Einrichtungen öffentlicher Verantwortungsträger, die öffentliche Mittel nur sparsam und zielgerichtet verwenden dürfen. Die Empfehlungen sollten daher diesen Umständen gerecht werden. Inhaltlich und in der Detailtiefe werden die Handlungshilfen auf insgesamt drei unterschiedliche Zielgruppen zugeschnitten, die nachfolgend dargestellt werden.

4.1 Übergeordnete Managementebene (Checkliste)

Die übergeordnete Managementebene stellt die erforderlichen finanziellen und personellen Ressourcen zur Verfügung. In der Regel handelt es sich dabei nicht um IT-Experten. Sie sind sowohl bei der Bewertung der vorhandenen IT-Sicherheit sowie der Entscheidung über die Umsetzung von Maßnahmen auf die Unterstützung der IT-Verantwortlichen angewiesen. Für diese Ebene wurde daher die Handlungshilfe „Checkliste" (Bild 1), eine kompakte, browser-basierte Software, zur Verfügung gestellt, welche die Umsetzung wichtiger übergeordneter Themen überprüft. Dabei handelt es sich um insgesamt 20 Fragen zu bereits umgesetzten Maßnahmen.

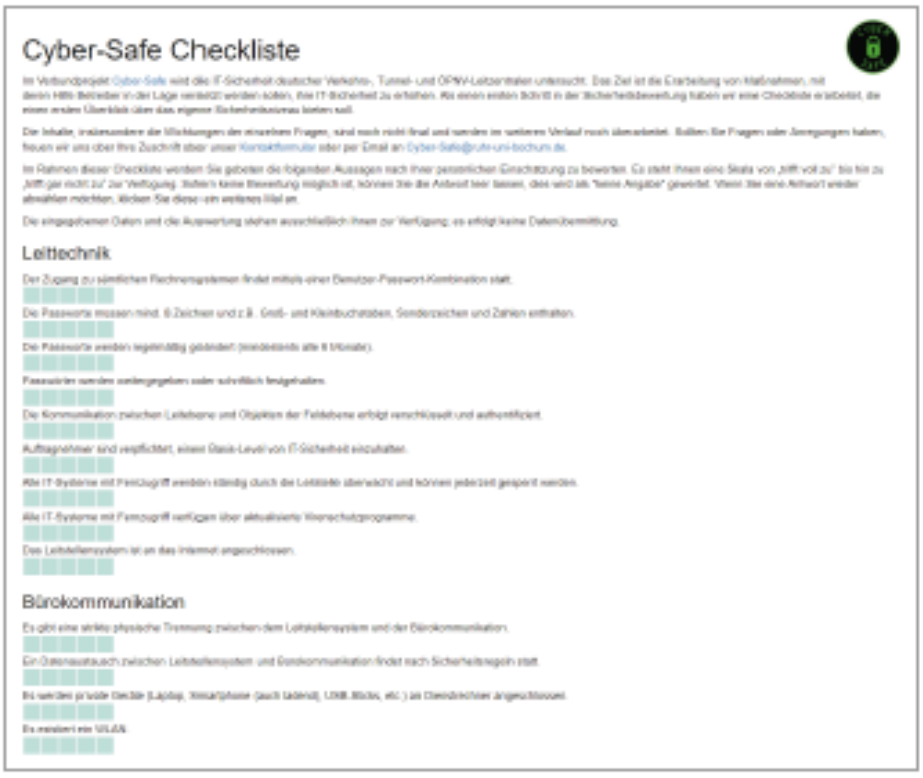

Bild 1 Bedienoberfläche der Handlungshilfe „Checkliste" (Ausschnitt)

4.2 Mittlere Managementebene (Leitfaden und Bewertungs-Software)

Die mittlere Managementebene ist überwiegend mit konkreten organisatorischen und personellen Aspekten befasst. Fachwissen über die IT der Leitzentrale ist in umfangreichem Maße vorhanden, jedoch oft nicht ausreichend zu allen Aspekten der IT-Sicherheit. Für diese Zielgruppe werden ein Leitfaden und eine Bewertungs-Software (Bild 2) erarbeitet, die das Vorhandensein von Maßnahmen aus Technik, Organisation und Personal nach den Ebenen von Leitstellenkomponenten (Leit-, Automatisierungs- und Feldebene) gemäß der Richtlinien für die Ausstattung und den Betrieb von Straßentunneln (RABT) [8] überprüft. Eine besondere Herausforderung bei der Entwicklung hierbei ist, eine übergreifende Bewertung im Rahmen eines Gesamtsicherheitsniveaus zur Verfügung zu stellen.

Diese Handlungshilfe identifiziert nicht automatisch Schwachstellen, kann aber iterativ dazu verwendet werden, das Sicherheitsniveau unter Einbeziehung zusätzlicher umsetzbarer Maßnahmen zu bewerten und damit zweckmäßig zu identifizieren. Begleitet wird diese Handlungshilfe von einem Leitfaden, der den aktuellen Maßnahmenstand zur Verbesserung der IT-Sicherheit in Tunnelleitzentralen zusammenfasst und die Nutzung aller Software Tools nachvollziehbar erläutert.

4.3 IT-Verantwortliche (Tiefenanalyse-Software)

IT-Verantwortliche verfügen sowohl über detailliertes Fachwissen der IT-Struktur als auch über Kenntnisse der zu berücksichtigenden organisatorischen und personellen Aspekte. Für diese Ebene

Bild 2 Bedienoberfläche der Bewertungs-Software für die mittlere Managementebene (Prototyp)

wird daher eine Software entwickelt, auf deren Grundlage eine Tiefenanalyse der vorhandenen IT-Struktur erfolgen kann. Dabei wird ein modellhaftes Abbild geschaffen, das gefährdete Komponenten und Verbindungen aufzeigt. Insofern ist es eine Ergänzung zu der oben beschriebenen Handlungshilfe für die mittlere Managementebene und gleichzeitig auch Planungshilfe für Ausstatter und Planer.

Für die umfängliche sicherheitstechnische Untersuchung und Beurteilung eines vernetzten, aus vielen Komponenten bestehenden IT-Systems ist es notwendig, detaillierte Informationen der vorhandenen Hard- und Software sowie ihrer Vernetzungsstruktur zu erfassen. Für die Bewältigung dieser komplexen Aufgabe bietet sich eine Unterstützung durch eine Software geradezu an. Die einzelnen Komponenten wie Server, PC-Arbeitsplätze und Drucker, aber auch externe Schnittstellen können durch den Benutzer mittels Drag and Drop innerhalb eines vordefinierten Arbeitsbereichs auf einer grafischen Bedienoberfläche platziert werden. Mittels zu ziehender Verbindungslinien zwischen den einzelnen Komponenten kann die Struktur der Netzwerkverbindungen abgebildet und erfasst werden. Die einzelnen Komponenten verfügen über variable Attribute, die durch den Anwender gesetzt werden können. Ebenso ist es möglich, bereits umgesetzte Maßnahmen einzelnen Komponenten zuzuweisen. Auf fehlende oder unvollständige Eingaben wird der Benutzer durch entsprechende Fehlermeldungen hingewiesen. Die eingegebenen Daten werden zur Vermeidung missbräuchlicher Verwendung mit einem Sitzungspasswort verschlüsselt gespeichert. Nach Abschluss dieses Erfassungsprozesses erfolgt die Analyse des IT-Systems. Hierbei werden potenzielle Bedrohungen ermittelt, bereits umgesetzte Maßnahmen bewertet, das aktuelle Sicherheitsniveau bestimmt und geeignete Sicherheitsmaßnahmen auf Grundlage des im Rahmen des Projekts entwickelten Maßnahmenkatalogs empfohlen.

5 Ausblick

Mit Inkrafttreten der ersten Verordnung zur Änderung der BSI-KritisV wurden die Schwellenwerte für den Sektor Transport und Verkehr festgelegt. Grundsätzlich sind Anlagen wie Verkehrssteuerungs- und Leitsysteme für das Netz der Bundesautobahnen als kritisch bewertet worden und daher entsprechend zu schützen. Vor diesem Hintergrund gewinnen die Ergebnisse des Projekts an Bedeutung, denn sie sind gleichwertig von großer Relevanz für die Betreiber dieser Straßenverkehrsinfrastruktur sowie für die Sicherheit der Verkehrsteilnehmer. Die bisherigen Ergebnisse des Projekts zeigen deutlich, dass die Empfehlung eines Mindestschutzniveaus für Tunnelleitzentralen notwendig ist. Planer, Ausstatter und Betreiber von Tunnelleitzentralen verfügen aktuell nur begrenzt über die notwendigen Kenntnisse, um geeignete Schutzmaßnahmen auch bereits in der Planungsphase zu berücksichtigen und ihnen die notwendige Bedeutung beizumessen. Im Zuge der Experteninterviews und Workshops konnte bereits eine Sensibilisierung erreicht werden, und das Interesse der Gesprächspartner lässt den Schluss zu, dass die zu entwickelnden Handlungshilfen ihren Weg in die tägliche Praxis finden werden. Die aktuelle Gesetzeslage infolge der Änderung der BSI-KritisV wird, aller Wahrscheinlichkeit nach diesen Prozess noch beschleunigen. Der große Vorteil der Handlungshilfen ist, dass sie auf Grundlage der Vorgaben des BSI entwickelt und auf die besonderen Randbedingungen von Leitzentralen angepasst und konkretisiert wurden, so dass durch die Nutzung und anschließende Umsetzung der empfohlenen Maßnahmen prinzipiell der BSI-Grundschutz erreicht werden kann. Die Handlungshilfen werden mit Abschluss des Forschungsprojekts Anfang 2018 veröffentlicht und allen interessierten Betreibern, Ausstattern und Planern unentgeltlich zur Verfügung stehen.

Danksagung

Das Projekt Cyber-Safe ist 2015 gestartet und wird mit Mitteln des BMBF innerhalb des Förderschwerpunkts „IT-Sicherheit für kritische Infrastrukturen" gefördert und vom Projektträger VDI/VDE Innovation + Forschung GmbH betreut.

Das Forschungskonsortium, unter der Leitung der Bundesanstalt für Straßenwesen (BASt), besteht aus der Dürr Group GmbH, dem Lehrstuhl für Systemsicherheit der Ruhr Universität Bochum, der STUVA e. V. und Straßen.NRW. Weitere Informationen unter: www.its-kritis.de.

Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2016. Bonn, 2016, S. 40.

[2] The Associated Press: Hallmark of a New Era'//Haifa Tunnel Paralyzed by Cyberattack, Expert Reveals. In: *Haaretz (Archives)*. Stand 27.10.2013. http://www.haaretz.com/israel-news/1.554729 (abgerufen am 14.06.2017).

[3] Erste Verordnung zur Änderung der BSI-Kritisverordnung in der Fassung von der Bekanntmachung vom 21. Juni 2017 (BGBl. I 40/2017 S. 1903).

[4] *Thienert, C., Nisancioglu, S.:* Workshop zur Cyber-Sicherheit von Tunnel- und Verkehrsleitzentralen. Bauverlag Gütersloh, Tunnel Magazin 2016, Heft 3, S. 54 f.

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge. Bonn, 2016.

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ein Praxis-Leitfaden für IS-Penetrationstests. Bonn, 2014.

[7] ISO/IEC 27000-Normenreihe. Internationale Organisation für Normung ISO, Genf, 2013.

[8] Richtlinien für die Ausstattung und den Betrieb von Straßentunneln (RABT 2016), Forschungsgesellschaft für Straßen- und Verkehrswesen (FGSV). Köln, Entwurf 2016.