STRASSE UND VERKEHR NR. 9, SEPTEMBER 2012
ROUTE ET TRAFIC N° 9, SEPTEMBRE 2012

## Systemarchitektur Schweiz

# Schweizer Strasseninfrastrukturen wirksam vor elektronischen Bedrohungen schützen

Im Rahmen des Projekts «Systemarchitektur Schweiz» erneuert und vernetzt das ASTRA die Leittechnik für die Betriebs- und Sicherheitsausrüstungen des gesamten Nationalstrassennetzes. Sämtliche Verkehrsmanagement-Anlagen der Schweizer Nationalstrassen werden dadurch zentral steuerbar. Neben klaren Vorteilen birgt die zunehmende Elektronifizierung und Vernetzung aber auch neue Gefahren.

VON **PHILIPP HURNI** UND **MARKUS MEIER**

## Ausgangslage

Mit der Neugestaltung des Finanzausgleichs (NFA) und der damit verbundenen Neuordnung der Aufgabenteilung zwischen Bund und Kantonen hat das ASTRA die Verantwortung für den Bau und Betrieb des gesamten Schweizer Nationalstrassennetzes von den Kantonen übernommen. Darunter fällt auch die Verantwortung für die technische Infrastruktur auf der Nationalstrasse, die Betriebs- und Sicherheitsausrüstungen (BSA). Im Rahmen des Projekts Systemarchitektur Schweiz (SA-CH) wird deshalb die heute höchst heterogene, auf zahlreichen unterschiedlichen kantonalen Systemen bestehende Infrastruktur der BSA in eine einheitliche Systemarchitektur mit eindeutig definierten Schnittstellen überführt. Die derzeit neu entstehenden Fachapplikationen können später von sämtlichen Akteuren der Schweizer Nationalstrassen (z. B. Polizeien, Gebietseinheiten und Verkehrsmanagement-Zentrale) genutzt werden. Unnötige Mehrkosten, welche durch die eigenständige Entwicklung von ähnlichen Systemen in allen Kantonen bisher angefallen sind, fallen weg.
Dem Themenkomplex der Sicherheit der BSA vor Cyber-Bedrohungen wurde in der bisherigen kantonal geprägten Systemlandschaft höchst unterschiedliches Gewicht beigemessen. Während einige Kantone vorbildliche Sicherheitskonzepte ausgearbeitet und weitreichende Sicherheitsvorkehrungen getroffen haben, blieb das Thema der Cyber-Sicherheit der BSA in den Verkehrsinfrastrukturen anderer Kantone relativ unbeachtet. Viele Anlagen in der Schweiz wurden noch vor dem breiten Aufkommen des Internets und den damit verbundenen Cyber-Gefahren installiert und erst nachträglich an kantonale Übergeordnete Leitsysteme (UeLS) angeschlossen. Deshalb hat man Sicherheitsbedenken in Bezug auf Cyber-Bedrohungen vorerst nicht die höchste Aufmerksamkeit geschenkt. Der Datenverkehr zwischen Anlagen und Verkehrs- und Betriebsleitzentralen blieb weitgehend unverschlüsselt. Zugriffsberechtigungs- und Zugriffskontrollkonzepte blieben oft auf einem vergleichsweise bescheidenen Niveau, zumal die BSA weitgehend von öffentlichen Netzen abgeschottet waren – abgesehen von einigen Modem-Zugängen für das Servicepersonal. Die Gefahr, dass jemand physisch in Anlagesteuerungen einbrechen könnte, um vor Ort Anlagen zu manipulieren, wurde deshalb lediglich durch physische Schutzmassnahmen eingedämmt.
Die mit SA-CH angestrebte schweizweite Vernetzung der gesamten BSA der Nationalstrassen und deren generell fortschreitende Elektronifizierung eröffnen zahlreiche neue Möglichkeiten für zentrales und effizientes Verkehrs- und Betriebsmanagement. Sie birgt daneben aber auch neue Risiken, welche in der bisherigen, kantonal geprägten Systemlandschaft eher von untergeordneter Bedeutung war. Würde es nämlich beispielsweise Unbefugten gelingen, Zugriff auf Verkehrsmanagement- und Sicherheitsanlagen zu erhalten, könnte das Schadenspotenzial im Missbrauchsfall enorm sein. Die grosse Anzahl von Schnittstellen der BSA mit umliegenden Systemen innerhalb des ASTRA, aber auch zum Internet (z. B. Publikation von BSA-Daten) vergrössert die Reichweite von eingedrungener Schadsoftware und von Hackerangriffen massgeblich.

## Angriffe auf Verkehrsinfrastrukturen

Mit dem Aufkommen von Wechseltextanzeigen in den letzten beiden Jahrzehnten haben sich auch die Meldungen über Manipulationen dieser Installationen gehäuft. Hier zeigen die Abbildungen 1/2 zwei von Hackern modifizierte Wechseltextanzeigen in den USA. Obgleich die abgebildeten Angriffe kaum das Potenzial aufweisen, riesige Schäden zu verursa-


1 | Zwei von Hackern modifizierte Wechseltextanzeigen in den USA – was hier klar als Witz identifizierbar ist, kann bei gezielter Falschinformation schwerwiegende Folgen haben.
1 | Deux panneaux à message variable modifiés par des pirates aux USA – ce qui est ici clairement identifiable comme plaisanterie peut avoir des conséquences graves lors de fausses informations ciblées.

chen, sollte man sie als Alarmzeichen interpretieren und keinesfalls auf die leichte Schulter nehmen.

Im Folgenden sind einige weitere Angriffe auf Verkehrsinfrastrukturen aufgeführt, welche sich in den letzten Jahren ereignet haben und teilweise weitaus höheres Schadenspotenzial aufweisen:

- Im August 2006 haben zwei Mitglieder der Gewerkschaft Engineers and Architects Association der Los Angeles Verkehrsbehörde die Lichtsignalanlagen von vier grossen Kreuzungen im Stadtzentrum von Los Angeles manipuliert und permanent auf Rot geschaltet. Der entstandene Stau und das Verkehrschaos sollte genutzt werden, um der eigenen Argumentation in den laufenden Vertragsverhandlungen besonderen Nachdruck zu verleihen. Es dauerte ganze vier Tage, bis die Ampelanlagen wieder einwandfrei funktionierten. Unzählige Autofahrer verbrachten Stunden im Stau, der dadurch entstandene volkswirtschaftliche Schaden war beträchtlich.
- Im Mai 2009 drangen Hacker in kritische Rechner der U.S. Luftverkehrsbehörde Federal Aviation Administration (FAA) in Alaska ein. Es gelang ihnen, zentrale Teile des Systems für die Flugverkehrsaufsicht abzuschalten, worauf einige Flugzeuge zur Sicherheit umgeleitet werden mussten. In einer Untersuchung wurde dann festgestellt, dass die Angriffe über schlecht geschützte, öffentlich zugängliche Internetseiten ermöglicht wurden. Spezialisten erkannten daraufhin über 700 hochriskante Schwachstellen, welche ein Eindringen in zentrale Systeme zuliessen.
- Im Jahre 2008 wurde das Road-Pricing-System der kostenpflichtigen Autobahnstrecken in der California Bay Area geknackt. Betrügern gelang es, die Identifikationsnummer der Transponder von anderen Autofahrern zu kopieren, um auf deren Kosten die Autobahninfrastruktur zu benutzen.
- Im April 2011 haben Hacker in Nimwegen die Fussgängersymbole der Strassenampeln mit anzüglichen Bildern ausgewechselt. Gemäss Polizeiberichten ist es in der Folge zu mehreren Auffahrunfällen gekommen.
- 2011 setzten die US-Geheimdienste die Schadsoftware Stuxnet ein, um die Steuerungen von Uran-Anreicherungsanlagen im Iran zu beschädigen. Als Reaktion darauf soll der Iran laut Insiderberichten mittlerweile zahlreiche Hacker rekrutiert haben, um im Falle eines militärischen Angriffs auf die Uran-Anreicherungsanlagen das Stromnetz und kritische Verkehrsinfrastrukturen der USA anzugreifen.

FR

## Protéger efficacement les infrastructures routières suisses des menaces électroniques

**Dans le cadre du projet «Architecture du système en Suisse», l'OFROU renouvelle et met en réseau la technique de commande des équipements d'exploitation et de sécurité sur l'ensemble du réseau des routes nationales. Toutes les installations de gestion du trafic des routes nationales suisses pourront être ainsi gérées de manière centralisée. A côté d'avantages très nets, l'électronification et l'imbrication croissante recèlent de nouveaux dangers.**

Auch die Melde- und Analysestelle Informationssicherung MELANI des Bundes macht in ihrem Halbjahresbericht 2011/II auf die erhöhte Gefahr für Supervisory Control And Data Acquisition (SCADA)-Systeme* aufmerksam. Thematisiert werden in diesem Zusammenhang auch die Schadsoftware Stuxnet oder Duqu.

Bei den meisten Angriffen auf Anlagen kritischer Infrastrukturen blieben die Motive bisher im Verborgenen und liegen wohl am ehesten darin begründet, dass die daran beteiligten Hacker Aufmerksamkeit erregen und ihre Fähigkeiten unter Beweis stellen wollten. Heute muss man vermehrt von gezielten Angriffen mit krimineller Absicht ausgehen: oft gehen Hackerangriffe mit Erpressungen einher, die möglichen Gefahren von Cyber- und Ökoterrorismus auf kritische Infrastrukturen können kaum hoch genug eingeschätzt werden.

Gegen das Schreckensszenario, dass Angreifer Teile der elektronischen Strasseninfrastrukturen der Schweiz tage- oder gar wochenlang unter ihre Kontrolle bringen könnten, muss sich das ASTRA im Rahmen des Projektes Systemarchitektur Schweiz bereits heute wappnen. Gelänge es nämlich Eindringlingen, Betriebs- und Sicherheitselemente auszuschalten, und beispielsweise Tunnelbeleuchtungen, Tunnelbelüftungen und Signalisationsanlagen ausser Gefecht zu setzen, könnte dies zu vorübergehenden Sperrungen von Nationalstrassenabschnitten führen. Dadurch könnte zum Beispiel im Falle des Gotthard-Strassentunnels sehr schnell ein gesamtwirtschaftlicher Schaden in mehrstelliger Millionenhöhe entstehen.

## Richtlinie Sicherheit BSA

Kritische Infrastrukturen wie die Stromversorgung oder Verkehrsinfrastrukturen wie Flughäfen, Schienennetze und Strassenanlagen gilt es deshalb gegen die Cyber-Gefahren zu wappnen, zumal diese mit der zunehmenden Vernetzung und Elektronifizierung unweigerlich zunehmen. Die momentan entstehende Richtlinie Sicherheit BSA [1] ist ein wesentliches Element dieser Stossrichtung. Erstmals werden ASTRA-seitig einheitliche Vorgaben zum Schutz von Objekten der Betriebs- und Sicherheitsausrüstungen (BSA) festgelegt, welche schweizweite Gültigkeit haben. Sie legen verbindliche Standards fest, wie elektronische und physische Schutzobjekte vor verschiedenen Gefahren (z. B. unbefugtem Zugriff) geschützt werden müssen. Die Richtlinie gibt klare Vorgaben zu praktischen Fragen in der konkreten Ausgestaltung der Anlagen und Datennetze.

Die Richtlinie Sicherheit BSA macht Vorgaben zu den folgenden Sicherheitsaspekten für Schutzobjekte:

- **Identitäts- und Zugriffsmanagement:** Die Sicherheitsrichtlinie schreibt ein zentralisiertes Identity- and Accessmanagement (IAM) und ein rollenbasiertes Zugriffsmodell (Role Based Access Control) vor. Der Mitarbeiter loggt sich überall mit demselben Account ein, auch wenn er verschiedene Rollen im Rahmen seiner Berufstätigkeit wahrnehmen muss. IAM ist die Voraussetzung, damit Akteure Ressourcen nur in der für ihre Aufgabe notwendigen Art und Weise verwenden. Durch die zentrale Verwaltung der Identitäten und deren Zugriffsattribute wird garantiert, dass durchgängig über alle Systeme die gleichen Regeln angewendet werden. Dies erlaubt z. B. einem Mitarbeiter mit einer neuen Funktion zentral die dafür notwendigen Rollen zuzuweisen, damit er umgehend mit den für diese Funktion notwendigen Anwendungen arbeiten kann. Dadurch kann im Gegenzug auch sichergestellt werden, dass ein Zugriffskonto eines Mitarbeiters zentral und damit vollständig über alle Systeme hinweg deaktiviert wird, wenn er die Firma verlässt. Dies verhindert mögliche Angriffe von ehemaligen, möglicherweise verärgerten oder enttäuschten Mitarbeitern, welche sich am ehemaligen Arbeitgeber rächen wollen.
- **Zugriffsschutz:** Sämtliche Benutzer müssen sich für Zugriffe auf Ressourcen eindeutig authentifizieren. Bei Ressourcen mit erhöhtem Schutzbedarf ist zudem eine starke Authentifizierung (Zweifaktorauthentifikation) erforderlich. Für Zugriffe auf Ressourcen müssen Benutzer entsprechend autorisiert sein. Es gilt das Prinzip des «Least Privilege» – der Ressourcenzugriff wird verweigert, ausser der Benutzer besitzt die dafür notwendige Rolle.
- **Informationsfluss:** Für die Datenübertragung auf öffentlichem Grund dürfen ausschliesslich sichere Protokolle verwendet werden, welche mit zeitgemässen Verschlüsselungsstandards chiffriert sind.
- **Netzwerke:** Zur Erhöhung des Schutzes vor Eindringlingen werden Netzwerke segmentiert und die jeweiligen Zonenübergänge mit Firewalls neuerer Generation gesichert. Netzwerkübergänge lassen nur explizit erlaubte Zugriffe mit den für die Steuerung der Anlagen vorgesehenen

3 | Hacker können verschiedene Motive haben – Geld, Fanatismus, Spass und vermehrt auch kriminelle Absichten.
3 | Les pirates peuvent avoir différents motifs – argent, fanatisme, plaisanterie et de plus en plus aussi des intentions criminelles.

* Supervisory Control And Data Acquisition (SCADA) – Systeme wie z. B. Verkehrsmanagement- oder Sicherheitsanlagen.

Netzwerkprotokollen zu. Sämtliche für die Steuerung der Anlagen nicht verwendeten Zugangspunkte werden geschlossen.
- **Verfügbarkeit:** Die Anlagen müssen eine der Anforderung genügende Verfügbarkeit aufweisen.
- **Audit:** Sicherheitsrelevante Ereignisse werden sicher protokolliert. Dadurch wird z. B. die gesetzliche Nachvollziehbarkeit gewährleistet.

Die Sicherheitsrichtlinie macht auch Vorgaben zur physischen Sicherheit von Schutzobjekten. Es geht z. B. um Vorgaben zu Gebäuden, Einrichtungen und Behältnissen der Anlagen, wie folgende Beispiele illustrieren:
- **Server-Räume:** Diese sollen möglichst im Zentrum des Gebäudes stehen; Kellergeschosse sollten daher nicht verwendet werden (Überflutungsgefahr).
- **Gebäuderichtlinien:** Es gibt Richtlinien für die Feuerfestigkeit der Wände, Richtung der Türöffnung, Notbeleuchtung, Überdruck in Räumen, Fensterdicke und Fensterschutzmassnahmen usw.
- **Physischer Zutrittsschutz**: Es gibt z. B. Vorgaben zu Schlüsselsystemen, Notfallöffnungen, elektronischen Zugangssicherungen (Badge, Codes), sich selbstständig schliessende Türen, Personenschleusen, Protokollierung des Zutritts.
- **Stromversorgung:** Die Richtlinie enthält Vorgaben zur Erstellung von Konzepten für eine unterbruchsfreie Stromversorgung (USV), Steuerung der Stromqualität (Abfederung von Spannungsschwankungen).

Die Richtlinie Sicherheit BSA bildet ein zentrales Element zur Festlegung eines einheitlichen Sicherheitsniveaus für die Betriebs- und Sicherheitsausrüstungen (BSA) des ASTRA. Die Gesamtsicherheit eines Systems wird oft mit einer mehrgliedrigen Kette verglichen. Es ist lange bekannt, dass die Gesamtsicherheit nur so hoch ist wie das schwächste Glied in dieser Kette. Die Sicherheitsrichtlinie BSA legt die Grundlage für ein einheitliches Sicherheitsniveau. Das Einhalten dieses Sicherheitsniveaus ist hinsichtlich der zunehmenden Vernetzung der schweizweiten BSA von zentraler Bedeutung. ||

## Literatur:

[1] Richtlinie Sicherheit BSA (Arbeitstitel), AWK Group AG im Auftrag des ASTRA, April 2012.

**PHILIPP HURNI**
Dr. phil. nat., CISSP
Consultant
AWK Group AG, Zürich

**MARKUS MEIER**
Dipl. El.-Ing. ETH
Principal Consultant
AWK Group AG, Zürich