Nr. 235, November 2018, Herausgeber: Benno Zogg

Intelligente Schutzsysteme für die Stadt der Zukunft

Intelligente Städte müssen kritische Infrastrukturen intelligent schützen. Nur so lässt sich die resiliente Erbringung kritischer Dienste langfristig sicherstellen. Eine zunehmend zentrale Rolle spielen hierbei neue Technologien. Vor allem Entwicklungen in den Bereichen Künstliche Intelligenz und Internet der Dinge machen eine Anpassung der bestehenden Schutzsysteme notwendig.

Von Marie Baezner, Linda Maduz und Tim Prior

Vernetzung ist die Grundlage sozialer und technischer Systeme. Vernetzung kann jedoch auch die Exponierung und Anfälligkeit von technischen Systemen für natürliche, technische und soziale Risiken erhöhen. Wenn diese technischen Systeme kritische Dienste für die sozialen Systeme erbringen, kann Vernetzung zu einem Problem werden.

Unsere Gesellschaft kann ohne bestimmte kritische Dienste wie die Wasser-, Energie- und Nahrungsversorgung sowie Transport und Sicherheit nicht funktionieren. Diese Dienste werden durch kritische Infrastrukturen produziert, verteilt oder gewährleistet. Entsprechend ihrer Bedeutung als Grundlage für unseren Alltag ist der Schutz Kritischer Infrastrukturen (SKI) zu einer regionalen, nationalen und internationalen Sicherheitspriorität geworden.

Ein Besucher im Hauptsaal der «Internet Security Conference 2018» in Peking, China, 4. September 2018. *Jason Lee / Reuters*

Parallel zum weltweiten Urbanisierungstrend und der wachsenden Komplexität kritischer Infrastruktursysteme beschleunigen sich auch die technologischen Entwicklungen exponentiell. Technologische Fortschritte wie jene im Bereich der Künstlichen Intelligenz werden oft als Allheilmittel angepriesen. Können wir aber dem prognostizierten Nutzen von Technologie beim Schutz kritischer Dienste vertrauen? Diese Frage muss angesichts der Möglichkeit untersucht werden, dass wir den Schutz kritischer Dienste in der Zukunft möglicherweise nicht gewährleisten können, wenn die SKI-Instrumente und -Prozesse nicht an die zukünftigen Herausforderungen angepasst werden.

Das Internet der Dinge und der SKI

Es ist zu erwarten, dass die Stadt der Zukunft auf einer cyber-physischen Plattform basieren wird, die sich durch miteinander vernetzte kritische «Systeme von Systemen» auszeichnet. Ein Beispiel dafür wäre ein ineinandergreifendes Energie-Kommunikation-Gesundheit-System. In intelligenten Städten wird das traditionelle kritische Infrastrukturnetz durch bidirektionale Informationssysteme ersetzt, die kritische Dienstleister und Konsumenten vernetzen. Intelligente Stromnetze greifen auf verschiedene Geräte zurück, die in kritischen Infrastrukturen und den von Konsumenten genutzten Räumlichkeiten angebracht sind,

um die Wirksamkeit, Effizienz, Zuverlässigkeit, Sicherheit, Nachhaltigkeit und Stabilität des Dienstes zu überwachen, zu analysieren und zu steuern.

Intelligente Stromnetze werden durch das Internet der Dinge (IdD) ermöglicht. Die rasante Digitalisierung aller Aspekte der modernen Gesellschaft ist die treibende Kraft hinter der Entstehung des IdD, das die Vernetzung (über das Internet) zwischen Computern beschreibt, die in Haushalts- oder Industrieobjekte eingebettet sind. Im Kontext intelligenter Stromnetze und kritischer Infrastrukturen bildet das IdD die Grundlage für die Vernetzung, die Automatisierung und die Nachverfolgung von vernetzten Gegenständen und Geräten. Während die Vernetzung von modernen Geräten die Effizienz und den Komfort vieler Aspekte des täglichen Lebens verbessert, vernachlässigen Hersteller und Nutzer solcher Geräte jedoch oft ihre Sicherheit.

Vor kurzem durchgeführte Untersuchungen (Huq/Hellberg 2017, siehe Textbox) zeigten, dass über das IdD vernetzte Geräte, die von kritischen Sektoren wie Notfalldiensten, Finanzdiensten, Versorgung und Bildung genutzt wurden, Cyber-Angriffen sehr stark ausgesetzt sind. Solche Geräte besitzen oft keine Benutzeroberfläche und sind daher nicht oder nur sehr schwierig einzurichten und zu aktualisieren. Die unsicheren Werkseinstellungen werden deshalb beibehalten. Dadurch sind diese Geräte unbefugten Zugriffen ausgesetzt und es entstehen Angriffspunkte für böswillige Cyber-Aktivitäten, welche die Erbringung kritischer Dienste stören können.

Drei Arten von IdD-Geräten sind in diesem Zusammenhang von besonderer Relevanz: 1) Geräte in Haushalten wie intelligente Beleuchtung, Kühlschränke oder Sicherheitssysteme, 2) Geräte, die in der kritischen Infrastruktur selbst eingebettet sind, wie Messsensoren oder SCADA-Systeme (Supervisory Control and Data Acquisition System) und 3) Geräte, die in Industriemaschinen eingebettet sind, nicht direkt mit kritischen Infrastrukturen vernetzt sind, aber durch die indirekt auf die kritischen Infrastrukturen zugegriffen werden kann (z.B. ein SCADA-System bei einer Automobilfertigungsstrasse). Jede Geräteart verursacht andere Sicherheitsprobleme für kritische Infrastrukturen. Auf Haushaltsebene kann dies zu Problemen wie Daten- oder Identitätsdiebstahl führen oder den bösartigen Zugriff auf die Netzwerke von kritischen Infrastrukturen ermöglichen. Da diese Geräte auch direkt (intelligente Zähler und Stromnetze) oder indirekt (Router, Kühlschränke, Wiedergabegeräte, Drucker etc.) mit Netzwerken von lokalen, regionalen und nationalen kritischen Infrastrukturen vernetzt sind, können bösartige Zugriffe auf Haushaltsebene als Eintrittstor missbraucht werden. In Zukunft wird das ein erhebliches Problem für den SKI darstellen, hauptsächlich, da die Sicherheit von über das IdD vernetzten Geräten im Haushalt und der Industrie sehr wahrscheinlich nie dieselben Sicherheitsstandards wie jene kritischer Infrastrukturen erreichen wird.

Fortschritte im Bereich des maschinellen Lernens werden Auswirkungen auf den Schutz kritischer Infrastrukturen haben.

Inwiefern diese Entwicklungen im Kontext vom SKI antizipiert werden können, hängt auch von anderen wichtigen Trends ab. Insbesondere technologische Trends (wie Automatisierung und Künstliche Intelligenz) werden erhebliche Herausforderungen bezüglich der Modernisierung von alternden kritischen Infrastrukturen mit sich bringen. Eine weitere wichtige Aufgabe zukünftiger SKI-Manager wird sein, dafür zu sorgen, dass die kritischen Infrastrukturen von Städten ihre Dienste auch dann erbringen können, wenn sich die Nutzung durch eine wachsende Stadtbevölkerung stark intensiviert.

SKI und das Zeitalter der KI

Einer der bedeutendsten technologischen Fortschritte mit grossem Einfluss auf unsere Zukunft ist die Entwicklung der Künstlichen Intelligenz. Auch wenn nach wie vor Uneinigkeit darüber herrscht, wie schnell diese Technologie Teil des täglichen Lebens und der Arbeit werden wird, steht ausser Frage, dass sie sowohl positive als auch negative Auswirkungen auf die Gesellschaft haben wird. Gegenwärtig finden heftige Debatten statt zwischen jenen, die über den Gebrauch und den Missbrauch von Künstlicher Intelligenz besorgt sind, und jenen, die diese Technologie als Lösung zentraler Probleme betrachten.

Zurzeit ist Künstliche Intelligenz noch begrenzten Fachaufgaben vorbehalten. Es handelt sich dabei um eine Form von Künstlicher Intelligenz, die als «schwache Künstliche Intelligenz» («Artificial Narrow Intelligence») bezeichnet wird. Beispiele dafür sind der «Google Assistant» und «Siri» von Apple. Der Schritt zu «starker Künstlicher Intelligenz» oder Künstliche Intelligenz auf menschlichem Niveau wurde bis anhin trotz grosser wissenschaftlicher Bemühungen noch nicht geschafft (siehe CSS-Analysen 220). Trotzdem erfolgt die Entwicklung der Künstlichen Intelligenz schneller als erwartet, insbesondere auf dem Teilgebiet des maschinellen Lernens (Allen/Chan 2017, siehe Textbox).

Fortschritte im Bereich des maschinellen Lernens, besonders bezüglich der Computerprogrammierung für den Betrieb kritischer Infrastrukturen, werden Auswirkungen auf deren Schutz haben. Maschinelles Lernen bildet im Endeffekt die Grundlage für die moderne Automatisierung. Durch maschinelles Lernen können die Programmierungseffizienz gesteigert und eigene Codes geschrieben werden. Für die Sicherheit ist vor allem relevant, dass Künstliche Intelligenz die Funktionalität von Programmen steigern könnte – insbesondere bei Updates, die vor der Verteilung auf Schwachstellen oder Fehler getestet werden könnten. Problematisch ist jedoch, dass Künstliche Intelligenz auch zur Programmierung von Schadsoftware eingesetzt werden könnte, die sich rasch anpassen kann und nur schwer aufzufinden und zu stoppen ist. In den richtigen Händen ist maschinelles Lernen jedoch ein vielversprechendes Instrument für den SKI im Zusammenhang mit intelligenten Abwehrsystemen (Cazorla et al. 2013, siehe Textbox).

Da kritische Infrastrukturen üblicherweise ein enges Spektrum an Diensten erbringen, eignet sich die aktuell verfügbare Künstliche Intelligenz gut für den SKI, wo sie für die Effizienzsteigerung bei Fachaufgaben eingesetzt werden könnte. Mit dem Fortschritt der Technologie werden zunehmend mehr Prozesse – auch solche, die üblicherweise dem Menschen vorbehalten sind – durch Künstliche Intelligenz ausgeführt werden. Das Management und die Überwachung von aktuell automatisierten Kontrollsystemen werden zukünftig wahrscheinlich von «starker Künstlicher Intelligenz» übernommen werden. Bereits heute werden die Prozesse zur Risikoanalyse als eine wesentliche Aufgabe des SKI zu den Bereichen gezählt, in denen Künstliche Intelligenz sich hervortun wird. Die Fähigkeit maschineller Intelligenz, Risiken und Reaktionen durch Betriebsdaten, die durch miteinander vernetzte Sensoren und Gerä-

te über lange Zeit gesammelt wurden, objektiv abwägen zu können, wird die subjektiven Fähigkeiten eines menschlichen Risikomanagers rasch übertreffen.

«Intelligenter» SKI

Der SKI ist in der Schweiz aufgrund des subsidiären Aufbaus des politischen Systems dezentraler organisiert als in vielen anderen Ländern. Gegenwärtig folgt der SKI einer übergreifenden Strategie, bei der das Management natürlicher, sozialer und technischer Gefahren mit Cybersicherheit und der wirtschaftlichen Landesversorgung kombiniert wird. Gemäss gesetzlicher Vorgaben sind die Betreiber für den SKI verantwortlich (wobei den Kantonen eine unterstützende Rolle zukommt).

Traditionell konzentrierte sich der SKI stark auf die physische Sicherheit von Objekten wie Stromleitungen, Generatoren, Strassen oder Spitäler. Die Dienste, die der Bevölkerung durch kritische Infrastrukturen erbracht werden, wie die Gesundheitsversorgung, Finanzdienste, Telekommunikation oder Mobilität, rücken aber zunehmend in den Mittelpunkt. Diese Entwicklung zeigt, dass es die erbrachten Dienste sind, welche die Infrastrukturen kritisch machen, und dass diese Dienste von einem System aus vielen vernetzten kritischen Infrastrukturobjekten erbracht werden. Wenn wir uns auf den Schutz individueller Objekte konzentrieren, die von verschiedenen Betreibern verwaltet werden, besteht das Risiko, dass wir das Gesamtsystem, das den Dienst erbringt, nicht berücksichtigen – und wir den Wald vor lauter Bäumen nicht mehr sehen. Die Verschiebung des Schwerpunkts weg von der Sicherheit und dem Schutz von Objekten hin zur Sicherheit und dem Schutz von Diensten führt dazu, dass bei kritischen Infrastrukturen systemische Sicherheits- und Schutzprinzipien in den Mittelpunkt rücken. De facto bedeutet das eine Verschiebung der SKI-Ziele von der Sicherheit von Objekten zur Sicherung der Erbringung kritischer Dienste.

> Bei jeder neuen Technologie oder Praktik gibt es Risiken und Nutzen.

Das IdD wird die Dezentralisierung des Managements und des Schutzes kritischer Infrastruktursysteme in der Schweiz zusätzlich verstärken. Künstliche Intelligenz wird hier eine zentrale Rolle spielen, damit die Sicherheitsverantwortlichen die Vernetzung eingrenzen und sie für den Schutz kritischer Infrastruktur nutzen können. Dezentralisierte Sicherheitsansätze können potenzielle Lösungen für hypervernetzte, aber exponierte kritische Infrastrukturen darstellen. Beispielsweise sollten intelligente Stromnetzsensoren oder mit dem Internet verbundene Geräte in einem sektorübergreifenden Infrastruktursystem sich nicht nur darauf beschränken, Informationen zwischen dem Dienstleister und dem Verbraucher zur Verbesserung des Dienstes auszutauschen. Das System könnte auch dazu genutzt werden, Informationen über die Sicherheit des Dienstes oder des Geräts zu liefern, um die Betreiber vor Problemen wie Objekt- oder Geräteschwachstellen, Cyber-Angriffen sowie Ausfällen zu warnen.

Sensoren und Geräte, die über das IdD vernetzt sind, könnten ausserdem Echtzeitinformationen über die Wirksamkeit von SKI-Massnahmen liefern. Angesichts des Informationsvolumens wird zunehmend Künstliche Intelligenz den Löwenanteil dieser Aufgaben übernehmen. Befürworter von Künstlicher Intelligenz, maschinellem Lernen und Automatisierung argumentieren, dass durch diese Technologien gestützte Prozesse kritischer Infrastrukturen deutlich effizienter wären als die gegenwärtigen, von Menschen gesteuerten Systeme.

Das Potenzial für eine stark dezentralisierte Sicherheit, die durch das IdD bereitgestellt wird, könnte zudem mit einem «Distributed Ledger» ergänzt werden. Diese Technologie, die beispielsweise bei der Blockchain-Technologie zum Schutz der Kryptowährung Bitcoin eingesetzt wird, bietet einen neuen Ansatz zum Schutz von mit dem Internet verbundenen Geräten in einem dezentralisierten System. Bei der Blockchain-Technologie wird ein System in einzelne Blöcke aufgeteilt, von denen jeder Sicherheitsinformationen des Systems enthält. Für den Zugriff auf oder eine Änderung des Systems muss ein Befehl durch jeden einzelnen Block genehmigt werden.

Durch die Nutzung von intelligenten Stromnetzgeräten in Verbindung mit Technologie wie Künstliche Intelligenz und «Distributed Ledgers» sind SKI-Manager für die sich ändernden Gegebenheiten im heutigen Zeitalter besser gewappnet – insbesondere im Kontext des IdD. Wenn jedoch die Chancen neuer Technologien nicht ergriffen werden, weil ihnen nicht zugetraut wird, herkömmliche Aufgaben zum Schutz kritischer Infrastrukturen zu übernehmen, kann der intelligente SKI nicht verwirklicht werden.

Der Technologie vertrauen

Es besteht eine unbestreitbare Spannung zwischen dem Streben nach Komfort und der zunehmenden Bedeutung von Infrastruktur. In diesem Zusammenhang ist die Aufregung rund um neue Technologien weder neu noch unberechtigt. Die Komplexität und Vernetzung könnte sich negativ auf die Sicherheit auswirken, besonders, wenn man sich dieser Aspekte nicht bewusst ist und sie nicht thematisiert. Neue Technologien und Entwicklungen wie Künstliche Intelligenz und das IdD als Synonyme für den Fortschritt bringen auch Unsicherheiten mit sich. Der Balanceakt zwischen der Aufrechterhaltung der Sicherheit und der Offenheit gegenüber neuen Chancen, die Fortschritt, aber auch Unsicherheiten mit sich bringen, ist eine wesentliche Herausforderung für SKI-Manager.

Es ist schwer abzuschätzen, wie nützlich Technologien wie Künstliche Intelligenz und «Blockchain» in Zukunft sein werden. Die Herausforderungen, die aus intelligenten Stromnetzen und dem IdD in intelligenten Städten für den Schutz kritischer Dienste entstehen, könnten auch verborgene Chancen für die Sicherheit und den Schutz bieten, vorausgesetzt man ist bereit sie zu nutzen. Bei jeder neuen Technologie

Weiterführende Literatur

Huq, N., Hilt, S. & Hellberg, N. **US Cities Exposed: Industries and ICS. A Shodan-Based Security Study of Exposed Systems and Infrastructure in the US.** (2017).

Wildavsky, A. **Searching for safety. Searching for Safety** (2017).

ECORYS UK. **Digital Skills for the UK Economy.** (2016).

Schuetze, J. **Warum dem Staat IT-Sicherheits-expert:innen fehlen. Eine Analyse des IT-Sicherheitsfachkräftemangels im Öffentlichen Dienst.** (2018).

Cazorla, L., Alcaraz, C. & Lopez, J. Towards automatic critical infrastructure protection through machine learning. Siehe: **Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)** 8328 LNCS, 197–203 (2013).

Allen, G. & Chan, T. **Artificial Intelligence and National Security.** (2017).

oder Praktik gibt es Risiken und Nutzen. Wenn Risikofreiheit zum Kriterium für die Einführung einer neuen Technologie oder Praktik bei der organisatorischen Weiterentwicklung oder Anpassung wird, werden Vorteile übersehen.

Insbesondere Sicherheitsorganisationen neigen dazu, sich Veränderungen zu widersetzen. Das mag daran liegen, dass Veränderungen als Unsicherheit wahrgenommen werden, die sich auf die Erfüllung wichtiger Aufgaben auswirken könnte. Die Sicherheit kann jedoch auch beeinträchtigt werden, wenn Praktiken, die einst nützlich waren, unter veränderten Gegebenheiten gefährlich werden (Wildavsky 2017, siehe Textbox). Der Kontext, in dem SKI bislang betrieben wurde, hat sich durch die zunehmende Vernetzung und Komplexität moderner kritischer Infrastrukturen sowie die Künstliche Intelligenz stark verändert.

Es ist vorstellbar, dass zentrale Aspekte im Zusammenhang mit kritischer Infrastruktur und ihrem Schutz in naher Zukunft automatisiert werden.

Herausforderungen

Für die Gewährleistung des Schutzes der «Systeme von Systemen» kritischer Infrastrukturen müssen entsprechenden Massnahmen, Handlungen und Praktiken angewendet werden. Die Gegebenheiten für den SKI verändern sich und die Identifizierung und Priorisierung neuer Sicherheits- und Schutzmassnahmen ist genauso wichtig wie die Identifizierung neuer Risiken und Bedrohungen. Technologie kann in diesem Zusammenhang eine Rolle spielen. Die Bewältigung anderer wichtiger zukünftiger Herausforderungen organisatorischer, technischer und sozialer Art, wie die Modernisierung von Altsystemen oder die Schulung qualifizierter Arbeitskräfte, wird die Grundlage schaffen, auf der neuen Technologien beim Schutz kritischer Infrastrukturen vertraut werden kann.

Angesichts der rasanten technologischen Fortschritte und der zunehmenden Komplexität von cyber-physischen Infrastruktursystemen stellen alternde Infrastrukturobjekte eine erhebliche Herausforderung dar. Früher wurden Aktivitäten zum SKI durch die Standardisierung von Komponenten, Techniken, Strategien und Prozessen optimiert. Aber Massnahmen, die sich in jüngster Vergangenheit noch eigneten, könnten sich in naher Zukunft als hinderlich oder gefährlich erweisen. Im kommenden Jahrzehnt wird die Modernisierung von Altsystemen durch den Einsatz neuer Technologien in einer Welt des IdD eine anspruchsvolle Aufgabe sein. Beispielsweise würde sich bei kritischen Infrastrukturen ein objektorientierter Risikomanagementansatz für die Untersuchung und Bewältigung der physischen Sicherheit des Objekts eignen. Dieser Prozess wäre aber unzureichend für die Untersuchung und Bewältigung der Sicherheit eines kritischen Infrastruktursystems und des Diensts, den es erbringt.

Es ist vorstellbar, dass zentrale Aspekte im Zusammenhang mit kritischer Infrastruktur und ihrem Schutz in naher Zukunft automatisiert werden. Ob wir für eine derartige Zukunft gewappnet sind oder nicht, ist eine wichtige Frage. Jüngste Untersuchungen zeigen, dass trotz entsprechender Bildungsinitiativen (ECORYS UK 2016, siehe Textbox) der Einstieg in die Arbeitswelt durch Fortschritte im Cyber- und Technologiebereich in der Wirtschaft überholt wird und sich damit die bereits breite Interoperabilitätskluft zwischen Mensch und Maschine in der Industrie zusätzlich vertieft (Schuetze 2018, siehe Textbox). So hätte ein Risikomanager für kritische Infrastrukturen, der nicht über die Fähigkeiten zur Nutzung einer maschinenbasierten Risikoanalyse verfügt, mit der Interpretation und der Verwendung der resultierenden Analyse zur Optimierung des Schutzes kritischer Dienste Schwierigkeiten.

Diese Herausforderungen schaffen zusätzliche Unsicherheiten für den Schutz kritischer Dienste. Tatsächlich verstärken sie die mit dem Aufkommen neuer Technologien wie Automatisierung und maschinellem Lernen sowie mit nahtlos über das IdD vernetzen Infrastruktursystemen bereits verbundenen Unsicherheiten. Diese Herausforderungen müssen auf dem Weg zum intelligenten Schutz kritischer Dienste thematisiert und bewältigt werden. Dies sollte es erleichtern, neuen Technologien zu vertrauen, diese einzuführen und somit den Schutz kritischer Dienste in einem entsprechenden operativen Umfeld auch in der Zukunft sicherstellen zu können.

Marie Baezner ist Researcher im Cyber Defense Team am Center for Security Studies (CSS) der ETH Zürich und Autorin von «Cybersicherheit in den US-chinesischen Beziehungen» (2018).

Linda Maduz ist Senior Researcher im Risk & Resilience Team am CSS/ETH.

Dr. Tim Prior ist Team Head im Risk & Resilience Team am CSS/ETH und unter anderem Autor von «Measuring Critical Infrastructure Resilience» (2015).

Die **CSS Analysen** zur Sicherheitspolitik werden herausgegeben vom Center for Security Studies (CSS) der ETH Zürich. Jeden Monat erscheinen zwei Analysen auf Deutsch, Französisch und Englisch. Das CSS ist ein Kompetenzzentrum für schweizerische und internationale Sicherheitspolitik.

Herausgeber: Christian Nünlist, Fabien Merz, Benno Zogg
Lektorat: Fabien Merz
Layout und Infografiken: Miriam Dahinden-Ganzoni
ISSN: 2296-0236; DOI: 10.3929/ethz-b-000300587

Feedback und Kommentare: analysen@sipo.gess.ethz.ch
Bezug und Abonnement: www.css.ethz.ch/cssanalysen