Bedrohungen aus dem Cyberraum

Verwundbarkeiten und Sicherheitsstrategien in kritischen Infrastrukturen

Die Sicherheit kritischer Infrastrukturen wird als Selbstverständlichkeit angesehen: Wirkliche Probleme, wie häufige Stromausfälle, unrichtige Daten oder Lieferengpässe, kennt man eher aus anderen Ländern und die Gefahren des Cyberraums erscheinen im Vergleich unwirklich. Wie verwundbar sind kritische Infrastrukturen gegenüber Cyberbedrohungen?

Von Ulrike Lechner

Die Zukunft wird in Deutschland mit Leitbildern wie Smart Energy, Industrie 4.0 oder dem automatisierten Fahren illustriert. Funktionierende Informations- und Kommunikationsstrukturen sind die Voraussetzung und IT-Sicherheit der Lebensnerv für die medienbruchfreien Prozesse, für smartes Management von Ressourcen oder autonome Fahrzeuge – für eine Zukunft, die aus ethischer Sicht nicht zuletzt eine positive Risikobilanz für den/die Einzelne/n und die Gesellschaft aufweisen muss (Ethik-Kommission 2017). Diese Zukunft der Digitalisierung birgt Chancen: Smartes Management von Ressourcen, Reduktion von Gefahren und Risiken oder auch Teilhabe für alle in ganz neuen Strukturen der wirtschaftlichen Wertschöpfung und neuen Arbeitswelten. Die Ethik-Kommission zum Automatisierten Fahren – einem der wichtigen Leitbilder der Digitalisierung – formuliert als ethische Leitlinien unter anderem eine positive Risikobilanz und dass die letztendliche Verantwortung und Entscheidungskompetenz beim Menschen liegen muss.

Digitalisierung und kritische Infrastrukturen

Die Digitalisierung birgt jedoch auch neue Verwundbarkeiten und Risiken – für jede/n Einzelne/n als Privatperson, als Kundschaft und Anwender/in und für die digitale Souveränität der Zivilgesellschaft (Waidner et al. 2017). Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit besonderer Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2017). Mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) und den beiden KRITIS-Verordnungen werden Anforderungen an das IT-Sicherheitsmanagement für die Betreibenden kritischer Infrastrukturen mit dem Ziel formuliert, die kritischen Infrastrukturen in Deutschland zu den sichersten weltweit zu machen (Bundesamt für Sicherheit in der Informationstechnik o. J.).

Verwundbarkeiten, Risiken und Akteure der IT-Sicherheit

Das Thema der IT-Sicherheit für Industrieanlagen rückt mit Stuxnet im Jahr 2010 ins Bewusstsein der Öffentlichkeit (Zetter 2014). Eine Schadsoftware konnte über längere Zeit hinweg unbemerkt Steuerungsanlagen und Leittechnik in der Uranaufbereitungsanlage Natanz und dem Kernkraftwerk Buschehr stören. Eine neuere und ebenfalls prominente Schadsoftware ist das „Mirai-Botnetz" mit dem Distributed Denial of Service (DDoS) Angriffe auf Infrastrukturen organisiert werden und das im Jahr 2016 Router in Privathaushalten auch in Deutschland betraf. Die Blackouts von 2015 und 2016 in der Ukraine werden der Schadsoftware Industroyer zugeschrieben. Verschiedene Versionen von „Ransomware" haben sowohl Privatpersonen als auch Universitäten, Krankenhäuser und Behörden betroffen. Fake News und auch die Diskussion über Manipulationsmöglichkeiten von demokratischen Wahlen sind weitere Beispiele für Verwundbarkeiten der Zivilgesellschaft.

Die Relevanz des Themas IT-Sicherheit zeigen auch Daten der Studie „Monitor IT-Sicherheit Kritischer Infrastrukturen" aus dem Jahr 2017, in der IT-Sicherheitsverantwortliche befragt wurden (Lechner 2017): 13 % der befragten IT-Sicherheitsverantwortlichen berichteten von mehr als 100 gezielten Cyberangriffen auf ihre Organisation und 45 % der KRITIS- Unternehmen hatten einen Serviceausfall oder Datenverlust zu verzeichnen.

Die Angreifer/innen („Threat Actors") verfügen über unterschiedliche Motive und unterschiedliche technischen Fähigkeiten (Rieb et al. 2017). Mit „Nation States" und durch sie finanzierte Kräfte verbindet man unlimitierte finanzielle Ressourcen und technische Fähigkeiten. Ihnen traut man zu, unbekannte Schwachstellen – „Zero Day Exploits" – zu entwickeln und zu nutzen. „Hacktivisten" sind politisch motiviert. Cyberkriminelle streben finanziellen Gewinn an, nutzen auf dem Markt vorhandene Werkzeuge genau wie Eigenentwicklungen. „Script-Kiddies" experimentieren, haben kaum Ressourcen und beschränkte technische Fertigkeiten, während Innentäter von Zugangsrechten und Wissen profitieren. Die unterschiedlichen Motive der „Threat Actors" machen umfang-

*Ökologisches*Wirtschaften 4.2017 (32) | DOI 10.14512/OEW320419

© 2017 U. Lechner; licensee IÖW and oekom verlag. This is an article distributed under the terms of the Creative Commons Attribution Non-Commercial No Derivates License (http://creativecommons.org/licenses/by-nc-nd/4.0/deed.de), which permits copying and redistributing the material in any medium or format, provided the original work is properly cited, it is not used for commercial purposes and it is not remixed, transformed or built upon. The access to the digital version of this article is reserved to subscribers of *Ökologisches*Wirtschaften until two years after the date of publication; after two years it is available to all readers.

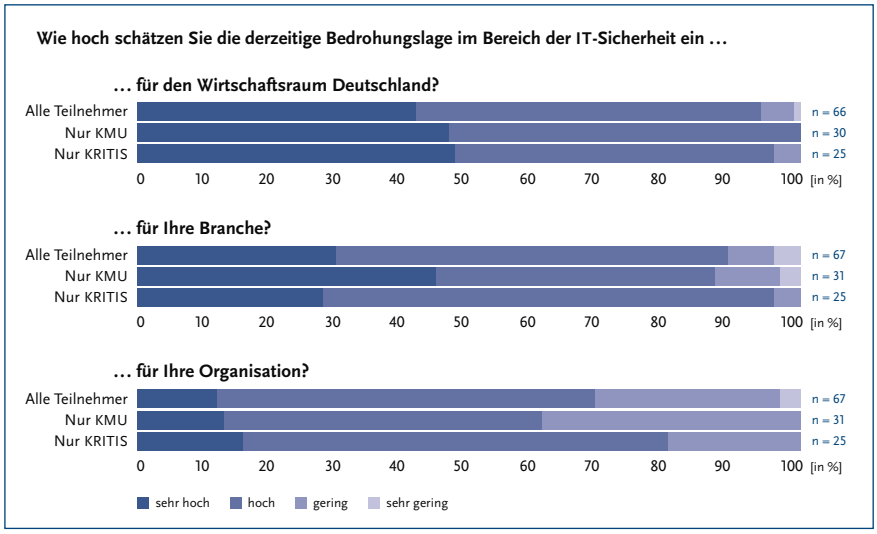

Abbildung 1: Die Einschätzung der Bedrohungslage durch IT-Sicherheitsverantwortliche *(Quelle: Lechner 2017b)*

reiche Schutzmaßnahmen bei kritischen Infrastrukturen notwendig – denn unterschiedliche Motive und Fertigkeiten implizieren unterschiedliche Ziele und Angriffsarten. Die Bedrohungen der Sicherheit beginnen und enden häufig genug beim Menschen, sodass „Faktor Mensch" eine zentrale Verwundbarkeit kritischer Infrastrukturen darstellt.

Faktor Mensch

Menschen – Mitarbeiter/innen bei Betreibern kritischer Infrastrukturen oder Anwender/innen von IT-Technologien – stehen im Zentrum vieler Angriffe. „Social Engineering" bezeichnet Methoden, um unberechtigten Zugang zu Informationen oder IT-Systemen durch „Aushorchen" zu erlangen. Beim Social Engineering werden „menschliche Eigenschaften, wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt (Bundesamt für Sicherheit in der Informationstechnik 2015)." Mitarbeiter/innen können manipuliert werden zur Weitergabe von Passwörtern, Öffnen von Dateien, Einbringen von Datenträgern, Besuch von Webseiten mit Schadsoftware, Ausführen von unbekannten Befehlen genau wie Verrat von Geschäftsgeheimnissen oder das Tätigen von Transaktionen, wie der Überweisung von Firmengeldern. So nutzen entsprechend den Informationen des BSI (Bundesamt für Sicherheit in der Informationstechnik 2016) die Cyberangreifer Techniken des Social Engineerings, um IT-Infrastrukturen zu kompromittieren. Basierend auf der initialen Kompromittierung, die primär den Menschen adressiert, nutzen die Cyberangreifer im Zuge der Sekundärangriffe überwiegend technische Angriffsvektoren, um beispielsweise die Privilegien zu erweitern oder Daten auszuleiten.

Die Sensibilität von Mitarbeitern/innen für Themen der IT-Sicherheit mit dem Wissen um IT-Sicherheit, von IT-Sicherheitsmaßnahmen und der Fähigkeit und Energie, die richtigen Handlungen abzuleiten, ist ein zentrales Thema in KRITIS. Mitarbeiter/innen rechtfertigen ihre IT-Sicherheitsverstöße beispielsweise mit, „die Arbeit muss erledigt werden", „nur dieses eine Mal" und Abschreckung, Angst vor Blamage oder Strafen helfen kaum. Verstöße gegen IT-Sicherheitsrichtlinien können mindestens die Übereinstimmung mit gesetzlichen Anforderungen verletzen: Wenn beispielsweise Kundendaten oder Geschäftsgeheimnisse auf privat genutzten Cloud Services landen.

Die Selbsteinschätzung der Risikolage ist ein weiteres Thema bei „Faktor Mensch". Die befragten IT-Sicherheitsverantwortlichen schätzen die Risiken für die eigene Organisation niedriger ein, als das Risiko für die eigene Branche und dieses wiederum niedriger als das Risiko für den Wirtschaftsraum Deutschland. Solch ein „Optimism Bias", also eine optimistische Einschätzung eigener Risiken, kann dazu führen, dass Risiken dauerhaft toleriert werden.

Den Menschen, also Mitarbeitenden, Anwendenden und Führungskräften, die Schuld zu geben, greift deutlich zu kurz – denn die Fähigkeiten, die Bedrohungslage einzuschätzen, hängt auch erheblich von Technik ab – dem Thema des nächsten Abschnitts.

Verwundbarkeiten und Risiken der Technik kritischer Infrastrukturen

Die Technik der kritischen Infrastrukturen und die Verfügbarkeit von Kraftwerksblöcken, Verkehrsleitsystemen, Transaktionssysteme von Banken, von industriellen Produktions- und Steuerungsanlagen müssen – vor dem Hintergrund von Vernetzung und Digitalisierung – geschützt werden. Typische Elemente einer technischen Infrastruktur können dargestellt werden mit Netzwerken für Produktion und für die Büroinfrastruktur und einer Verbindung zum Internet mit Firewall(s), „Switches" und Routern. Typische Verwundbarkeiten auf Ebene der Technik bei kritischen Infrastrukturen sind PCs in den industriellen Produktions- und Steuerungsanlagen mit Betriebssystemen auf einem veralteten Stand der IT-Sicherheit; Produktions- und Steuerungssysteme in Netzwerken ohne Absicherungen; private Smartphones, die über WLAN in das Firmennetz eingebracht werden, und Fernzugänge für die Wartung, für das Monitoring von Anlagen oder für neue Abrechnungs- und Servicemodelle (Lechner 2017a).

Die Technologie der kritischen Infrastrukturen mit Industrieanlagen ist langlebig – sehr viel langlebiger und schlechter wartbar als dies in der klassischen IT heute üblich ist. Lebenszyklen von 50 Jahren oder Wartungszyklen von Monaten oder Jahren, in denen beispielsweise kein Sicherheitsupdate aufge-

spielt werden kann, sind nicht ungewöhnlich. Technologie kritischer Infrastrukturen ist zudem häufig dem physischen Zugriff durch Anwender/innen oder Kund/innen ausgesetzt: Manipulationen wie das Einbringen von Schadsoftware können nicht verhindert werden. Selbst virtuelle oder physische Trennungen von Netzwerken können mit verschiedenen Methoden umgangen werden. Das Auslesen von Sensoren beispielsweise in Automobilen ist ein vieldiskutiertes Thema. Zudem sind Produktions- und Steuerungsanlagen häufig Individualanfertigungen, die dann eine entsprechend individuelle IT-Sicherheitslösung benötigen – und auch das macht das Thema komplex.

Die Verwundbarkeit kritischer Infrastrukturen resultiert auch aus der schieren Komplexität mit einer Vielzahl von Geräten, Protokollen, von individuellen Hardware- und Softwarelösungen, und vielfältigen Abhängigkeiten zwischen Hardware, Software und Services in den Geschäftsprozessen. IT-Risikomanagement wird angesichts dieser Komplexität zu einer großen Herausforderung. Der Umgang mit der Komplexität des Themenfeldes IT-Sicherheit kritischer Infrastrukturen ist auch eine Frage der Organisation.

Organisatorische Verwundbarkeiten

Von den KRITS-Betreibenden fordert das IT-Sicherheitsgesetz ein IT-Sicherheitsmanagement. Auf organisatorischer Ebene müssen zwei Welten zusammenfinden – die IT mit ihren etablierten Prozessen des Managements der IT-Infrastruktur und die Technik der kritischen Infrastrukturen – unterschiedliche Verfahren und Prozesse, unterschiedliche Werte und Kulturen und vor allem unterschiedliche Schwerpunkte in der IT-Sicherheit machen Organisationen verwundbar. Organisation von IT-Sicherheit bedeutet auch, dass rechtliche Aspekte, Normen und Standards für die Sektoren spezifisch sind. Der Normennavigator (Förderschwerpunkt ITS KRITIS 2017) illustriert, wie viele Regelungen in der IT-Sicherheit beachtet werden müssen.

Die Empirie aus den „IT-Security Matchplays“, einem serious Game zur IT-Sicherheit kritische Infrastrukturen, zeigt, dass die Spielteilnehmenden sich vor allem organisatorische Maßnahmen vornehmen: stärkere Kooperation zwischen Anwendenden und IT-Fachpersonal oder Umsetzung bestehender IT-Sicherheitspolicies sowie einfache Vorkehrungen wie „Büro abschließen“ sind hier typische Beispiele, die illustrieren, wie wichtig Organisation für die IT-Sicherheit von KRITIS ist (Rieb et al. 2017).

IT-Sicherheit und die notwendigen Innovationen

Die Leitbilder für die Zukunft erfordern neue Strukturen und bieten neue Möglichkeiten. Jedoch ist IT-Sicherheit nicht mehr ein Hemmnis für den notwendigen technischen Fortschritt. In der Monitor-Umfrage (Lechner 2017b) sehen allerdings weniger die KRITIS-Organisationen IT-Sicherheit als Innovationshemmnis, als die Gesamtheit der Befragten – ein Mehr an Organisation und IT-Sicherheitsmanagement scheint sich hier positiv auszuwirken – auch wenn es noch erheblichen Bedarf an neuen, besseren IT-Sicherheitslösungen und entsprechender Forschung gibt.

Anmerkung

Das Bundesministerium für Bildung und Forschung hat diese Forschung des Projekts „Vernetzte IT-Sicherheit Kritischer Infrastrukturen“ (VeSiKi) gefördert.

Literatur

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2017): Glossar: Kritische Infrastrukturen (KRITIS). www.kritis.bund.de

Bundesamt für Sicherheit in der Informationstechnik (2016): Industrial Control System Security. Top 10 Bedrohungen und Gegenmaßnahmen. In: BSI-Veröffentlichungen zur Cyber-Sicherheit, BSI-CS 005 | Version 1.20.

Bundesamt für Sicherheit in der Informationstechnik (2015): IT-Grundschutz: G 0.42 Social Engineering. www.bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (o. J.): Industrie und Kritische Infrastrukturen: Das IT-Sicherheitsgesetz. www.bsi.bund.de

Ethik-Kommission (2017). ePrivacy – APF 2017. www.vda.de/de/themen/innovation-und-technik/automatisiertes-fahren/automatisiertes-fahren.html

Förderschwerpunkt ITS KRITIS (2017): Förderschwerpunkt IT-Sicherheit für Kritische Infrastrukturen. www.itskritis.de

Lechner, U. (2017a): Fallstudien der IT-Sicherheit Kritischer Infrastrukturen (In Vorbereitung).

Lechner, U. (2017b): Monitor IT-Sicherheit Kritischer Infrastrukturen. Forschungsprojekt VeSiKi. München, Universität der Bundeswehr München.

Rieb, A./Hofmann, M./Laux, A./Rudel, S./Lechner, U. (2017): Wie IT-Security Matchplays als Awarenessmaßnahme die IT-Sicherheit verbessern können. In: Leimeister, J. M./Brenner, W.: Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017), St. Gallen. 867–881.

Waidner, M./Backes, M./Müller-Quade, J. (2017): Positionspapier Cybersicherheit in Deutschland. Stuttgart, Fraunhofer Verlag.

Zetter, K. (2014): Countdown to Zero Day. New York, Crown.

AUTORIN + KONTAKT

Dr. Ulrike Lechner ist Inhaberin des Lehrstuhls für Wirtschaftsinformatik an der Universität der Bundeswehr München.

Universität der Bundeswehr München, Fakultät für Informatik, Werner Heisenberg Weg 39, 85577 Neubiberg. Tel: +49 896004-2504, E-Mail: Ulrike.Lechner@unibw.de