Jahresthema 2018 „Gestern gehörten meine Daten mir - gehören sie morgen meinen Feinden? Eine längst fällige gesellschaftliche Diskussion“

Vierter Vortrag des Jahres 2018 am 16. Juli 2018 in der Hanns-Seidel-Stiftung

PROF. DR. ULRIKE LECHNER, UNIVERSITÄT DER BUNDESWEHR MÜNCHEN

SICHERHEIT VON DATEN, WIRTSCHAFT UND GESELLSCHAFT
– FORSCHUNG, PRAXIS UND DER WEG IN DIE ZUKUNFT –

Unsere Daten können verschwinden oder zerstört werden, z.B. Fotos, Videos, Musik. Sie können nicht mehr brauchbar oder infiziert sein, um andere Rechner zu infizieren. Das betrifft Daten aller Art, auch Algorithmen etc.

Die im Forschungsprojekt **VeSiKi** – Vernetzte IT-Sicherheit Kritischer Infrastrukturen – gefundenen Ergebnisse sollen in die Praxis gebracht und die Bevölkerung informiert werden.

Zur Referentin Ulrike Lechner: Sie hat an der Universität Passau studiert, war an der Universität Bremen für „digitale Medien“ und ist jetzt seit 13 Jahren Professorin für „Wirtschaftsinformatik“ an der Universität der Bundeswehr München in Neubiberg, ohne vorherige militärische Karriere. Übrigens gibt es recht viele weibliche Dozenten gerade in der IT-Sicherheit.

Kritische Infrastruktur und ihre Sicherheit

Definition *Kritische Infrastruktur*: Das sind „Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ (Bundesministerium des Inneren, KRITIS-Strategie)[1]

Die Entwicklung

Angesichts des heute (16.7.2018) stattfindenden Treffens der Präsidenten Putin und Trump wird klar, dass Freiheit und Sicherheit zu verteidigen so wichtig ist.

[1] Zitat aus „Monitor IT-Sicherheit Kritischer Infrastrukturen“, Ulrike Lechner (Hg.), München 2017, S. 12.

Beispiele für Angriffe auf Freiheit und Sicherheit:

- 2007 gab es einen Denial of Service-Angriff[2] auf Estland, hierbei blieb das sehr IT-bestimmte Land mehrere Tage ohne IT-Infrastruktur; die Datenspuren führten nach Russland;
- heute passieren DoS ständig, werden erkannt und verhindert;
- 2010 Stuxnet: eine Malware[3] gegen den nahen und mittleren Osten, vor allem die Atomaufbereitung im Iran war betroffen: der Iran musste die Zentrifugen für die Urananreicherung selbst bauen – durch die Malware wurde die Steuerung der Zentrifugen lahmgelegt, Stuxnet blieb mehrere Jahre unentdeckt und ist heute noch auf vielen Anlagen unentdeckt vorhanden, aber unschädlich;

=> *Das war der Beginn der Forschung zum Thema,* ***VeSiKi****.*

- April 2015: Blackout des französischen Fernsehsenders TV5 Monde, angeblich verursacht durch Islamisten[4];
- Dezember 2015: Blackout in der Ukraine, angeblich durch russische Hacker;
- April 2017: Ransomware[5] WannaCry[6] legt deutsche Bahn lahm, Anzeigetafeln (Zugzielanzeigen) und Weichensteuerung betroffen;
- seitdem gab es immer wieder derartige Warnungen in den Medien.

Fake-News-Debatte und Nennung konkreter Namen bezüglich der Beeinflussung von Wahlen beeinflussen und erschweren die Arbeit. Für die Kritische Infrastruktur bedeutet dies, derartige Vorfälle müssen gemeldet und ein Risikomanagement betrieben werden – es gibt dazu zwei Verordnungen.[7]

Dieser Vortrag soll sensibilisieren und die Anstrengungen Deutschlands darstellen – wir sind auf einem guten Weg. Denn die Betreiber Kritischer Infrastruktur machen mit und die diesbezüglichen Meldungen sind auf niedrigem Niveau.

---

[2] Denial of Service, DoS = durch eine ungewöhnlich hohe Anzahl von Anfragen wird der Server außer Betrieb gesetzt, www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/DoS/dos_node.html, eingesehen 31.08.2018.

[3] Malware = Sammelbegriff für alle Arten von Schadprogrammen, siehe https://praxistipps.chip.de/was-ist-malware_28542 vom 15.03.2014, eingesehen am 20.08.2018.

[4] www.herbert-saurugg.net/2015/blog/medienberichte/is-hackerattacke-legt-tv5-monde-lahm, vom 09.04.2015, eingesehen am 20.08.2018, und www.spiegel.de/netzwelt/web/tv5-monde-russische-hacker-sollen-hinter-cyber-angriff-stecken-a-1038032.html, vom 10.06.2015, eingesehen am 31.08.2018.

[5] Ransomware = Zugang zu den eigenen Daten wird versperrt und nur gegen Lösegeld entsperrt.

[6] Siehe www.spiegel.de/netzwelt/web/wannacry-attacke-fakten-zum-globalen-cyber-angriff-a-1147523.html, vom 13.05.2017, eingesehen am 31.08.2018.

[7] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) vom 22.04.2016 in der Fassung vom 21.06.2017 *und* Gesetz über das Bundesamt für Informationstechnik (BSIG) vom 14.08.2009 in der Fassung vom 23.06.2017.

IT-Sicherheit der Infrastruktur

Der Blackout 2003 in New York hatte laut Jewgenij Kaspersky (Interview Spiegel 20.6.2011) [8] ein Virus verursacht. Ohne Strom gab es keine Ampeln und keine öffentlichen Verkehrsmittel – Betroffene übernachteten in den U-Bahnstationen, es dauerte Tage, bis alles wieder wie vorher war.

Das zeigt, dass Kritische Infrastrukturen voneinander abhängig und vernetzt sind.

Wer sind die Angreifer?

Da gibt es:

- die spielerischen Angriffe, um auszuprobieren, was möglich ist;
- Angriffe, um auf Missstände aufmerksam zu machen;
- die Rache von Mitarbeitern;
- die vom Mitarbeiter (unabsichtlich) mitgebrachte Malware, z.B. auf einem USB-Stick mit Musik;
- Kriminelle, die Geld erpressen oder Daten verkaufen wollen;
- staatlich gesponserte Angriffe, wie das Lahmlegen von Energieanlagen, Stuxnet:
- derartige Malware erfordert Ressourcen: um die entsprechende Industrie lahmzulegen, sind entsprechende Anlagen nötig, deren Entwicklung mehrere Jahre dauert -> das kann weder eine Privatperson noch ein Unternehmen, sondern ist nur mit staatlicher Unterstützung möglich.

Wie steht es um die Kritische Infrastruktur in Deutschland?

Die Ausfallsicherheit (SAIDI)[9] betrifft mehr Frankreich – siehe dazu Bundesnetzagentur oder Wissenschaftlicher Dienst des Bundestages[10].

Laut der Cybermap, in der die Cyberangriffe aufgezeichnet werden, wird Deutschland am dritt- oder vierthäufigsten in der Welt angegriffen,[11] aber

[8] Der Spiegel 25/2011, „Das Netz wird Kriegsschauplatz“, S.98-100.
[9] SAIDI = System Average Interruption Duration Index, Kennzahl zur Ermessung der Zuverlässigkeit von Energieversorgungsnetzen.
[10] Wissenschaftlicher Dienst des Bundestags, Sachstand, Vergleich der Stromversorgungsqualität Deutschlands, Frankreichs und Belgiens, 22.02.2017, www.bundestag.de/blob/496056/9b97deb8a246fd8d15a2760596ce28df/wd-5-014-17-pdf-data.pdf
[11] Cyberbedrohung Echtzeitkarte siehe https://cybermap.kaspersky.com/de/, eingesehen am 20.08.2018.

wie dem Monitor zu entnehmen ist, haben wir zu 61 % einen guten und zu 16 % einen sehr guten Stand der IT-Sicherheit.[12]

Aktuelle Themen sind:

- der Datenverlust bei Yahoo;
- die Virenscanner sind vertrauenswürdig – das bekannteste Virenschutzprogramm stammt vom russischen Unternehmer Eugene/Jewgenij Kasperksy;
- die Fake News auf Facebook und Twitter.

Gefährdet sind auch Insulinpumpen, Herzschrittmacher, das Wlan der Bahn und in Hotels in der Form eines angeblichen Updates. Einfallstore sind auch „smarte" Puppen und Smarthomes durch ihre Internetanbindung und damit Angreifbarkeit.

Siehe dazu die Cybercrime-Heatmap von Europol 2015/2016.[13]

Bei den Arten der Angriffe sind vor allem Ransomware gefährlich. Viele Angriffe (57,6 %) sind nicht auf einen Verursacher zurückzuführen

Wie steht es um die Sicherheit?

Es können Daten, Steuerungen, Produkte, Dienstleistungen betroffen sein: Daten können zerstört oder fehlgesteuert werden oder weiteren Schaden auslösen, Produkte oder Dienstleitungen können – entsprechend dem Jahresthema – morgen meinen Feinden gehören…

Das Produkt und die Dokumentation gehören zusammen, wie bei Medikamenten.

Die Zeit digitaler Sorglosigkeit ist vorbei!

Die Architektur von KRITIS zeigt die Vernetzung, egal ob Büro, Produktion oder Klärwerk.

Beispielsweise wird Schadsoftware über einen USB-Stick mit Musik in eine Industrieanlage gebracht (früher hätte der Techniker ein Radio angeschal-

[12] Zahlen aus Monitor (2017), S. 15.
[13] www.iota-2016.pdf, eingesehen am 31.08.2018.

tet), der Techniker ist nicht sensibilisiert für bestehende Gefahren. Oder es wird von einer Person etwas gemacht, ohne andere darüber zu informieren.

Beispielsweise sind Operationsroboter ständig verbunden mit dem Hersteller, um sicherzugehen, ob/dass alles richtig läuft – per Internet: das bedeutet, man kann spontan vor Ort nichts machen.

Bedrohungen der KRITIS sind nach BSI social engineering[14] und phishing[15] – das heißt der Mensch – und auch per USB, Datenhardware, Smartphones.

IT-Sicherheit in der Kritischen Infrastruktur ist ein neues Thema

- Verfügbarkeit ist ein zentrales Schutzziel;
- Verfügbarkeit ohne Vertraulichkeit und Integrität der Daten ist nicht denkbar;
- Anforderungen und Umsetzungen sind sektorenabhängig;
- Hardware mit langen Lebenszyklen – Beispiel: eine Druckmaschine (mehrere Millionen teuer und 30 Jahren in Gebrauch) – wird gesteuert von einem Laptop (unter 500 Euro wert und zwei Jahre in Gebrauch): das Schutzziel „Verfügbarkeit" prägt die IT-Sicherheit.

Kosten für die Sicherheit

Preis + Wahrscheinlichkeit des Schadenseintritts + Höhe des Schadens bilden zusammen den „Calculus of Negligence", ein numerisches Modell zu den Kosten der Sicherheit. Fraglich hierbei ist aber, wie hoch beziffert man den eintretenden Schaden, was bezieht man ein?

Das ist der Return on Security Investment (RoSI).[16]

Fraglich ist auch, wie eine Verminderung des Schadens zu berechnen ist/die Reduktion potentieller Verluste ist unklar. Dazu gibt es das Gordon & Loeb Model, ebenfalls ein mathematisches Verfahren, mit seiner 37 %-Regel.

Diese mathematischen Modelle sind schwierig zu beurteilen/zu handhaben, in Deutschland wird ein anderes Modell angewendet: der Branchenstan-

[14] Menschliche Eigenschaften, wie Hilfsbereitschaft, werden ausgenutzt zur Manipulation von Personen.
[15] Das Erlangen vertraulicher Daten wie Passwörtern durch Tricks.
[16] Siehe z.B. https://www.cio.de/a/wann-sich-investitionen-in-it-sicherheit-rechnen,3260855, vom09.12.2016, eingesehen am 20.08.2018.

dard.[17] Zu finden ist er im IT-Sicherheitsgesetz. Dieses Modell ist sicherer als die numerischen/mathematischen Modelle.

Kosten der Cybervorfälle

Beispiele:

- Ein Cyberangriff auf die Reederei Maersk betraf 45.000 Rechner und 4.000 Server weltweit und verursachte einen Milliardenschaden;
- aufgrund eines Cyberangriffs auf die Firma Merck musste die Arzneimittelproduktion eingestellt werden, was mehrere 100 Millionen Euro kostete;
- ein Cyberangriff auf den Paketdienst TNT verursachte einen Schaden von 300 Millionen Dollar.

Daraus ist zu schließen, dass die Kosten der Cybervorfälle steigen, denn ein erfolgreicher Angriff durch Ransomware zieht weitere nach sich.[18]

Der Faktor Mensch ist das wichtigste Einfallstor!

Dazu ein Zitat von J. Peter Burgess (Peace Research Institute Oslo, PRIO): *„Der Wert der Kritischen Infrastruktur ist der Wert, den ihm die Gesellschaft zuschreibt."*

Die entscheidende Frage in Bezug auf die Kritische Infrastruktur ist also: was ist sie uns wert, worauf wollen wir vorbereitet sein? *Denn gute IT kostet!*

Beispielsweise ist ein Smartphone nur einige wenige Jahre nutzbar, dann gibt es dafür keine Funktionsupdates mehr (anders Sicherheitsupdates).

- Die wirtschaftliche Seite sind die Preise für Daten im Darknet;
- die Geschäftsmodelle der Angreifer werden immer besser: ab 7 €/h gibt es einen Denial of Service – wie ein eigener Handyvertrag kann

[17] Z.B. „KRITIS: Erster branchenspezifischer Sicherheitsstandard anerkannt" (Wasser- und Abwasserverbände), Pressemitteilung des BSI vom 01.08.2017, eingesehen am 31.08.2018, www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/Erster_brancehnspezifischer_Sicherheitsstandard_anerkannt_01082017.html.

[18] Siehe Accenture Security, *From Laggard to Leader*, 2015, www.accenture.com/t20150814T113701Z_w_/us-en/_acnmedia/Accenture/Conversion-Assets/Microsites/iFrame/insight-cybersecurity-research-report/Accenture-Cyber_Security-Leap-2015-Report.pdfla=en#zoom=50, eingesehen am 20.08.2018, und Accenture Security, *2018 State of Cyber Resilience: Gaining Ground on the Cyber Attacker* (Executive Summary), www.accenture.com/t20180416T134038Z_w_/us-en/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf#zoom=50, eingesehen am 27.08.2018.

das „zusammengeklickt“ werden und ist damit unproblematisch (also ohne Fachwissen) zu nutzen.

Der Schutz Kritischer Infrastruktur ist eine gesetzliche Aufgabe!

Der menschliche Faktor

Wenn IT-Sicherheit und Mitarbeiter Schaden verursachen können, müssen wir bessere Technologie bauen.

Die Selbsteinschätzung der Unternehmen der Kritischen Infrastruktur ist schief: sie sehen für das eigene Unternehmen geringeres Risiko als für die gesamte Branche in ganz Deutschland[19]. Die Risikoeinschätzung der Betroffenen ist falsch – vergleiche das Autofahren: wer sieht sich schon als schlechter Autofahrer?

Der Nobelpreis 2017 ging an Richard Thaler für die Beschreibung derartiger Fehleinschätzungen, siehe gesunde Ernährung, siehe Alterssicherung.

EVA DITTRICH, ASS. JUR.

SIEHE AUCH:

- Monitor IT-Sicherheit Kritischer Infrastrukturen, Ulrike Lechner (Hg.), München 2017.
- Monitor 2.0 IT-Sicherheit Kritischer Infrastrukturen, Ulrike Lechner (Hg.), München 2018.
- Cyber-Bedrohung – ein Einstieg, Bundesamt für Sicherheit in der Informationstechnik (BSI), 15.10.2012,
- Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS (Broschüre des BSI), Stand März 2017,
- Website des BSI, *www.bsi.bund.de*,
- und des BSI für Bürger, *www.bsi-fuer-buerger.de.*

[19] Siehe Monitor und Monitor 2.0, S. 15ff.