Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Magazin 2018/01

Mit Sicherheit

Industrial Control Systems in der Industrie 4.0

BSI INTERNATIONAL

Zentrale Britische Behörde für Cyber-Sicherheit (NCSC)

SONDERTHEMA

Cyber-Sicherheit in der Industrie 4.0

DIGITALE GESELLSCHAFT

Blockchains im Einsatz

„Nur wenn Sicherheitsaspekte schon im Design berücksichtigt werden, kann die Digitalisierung erfolgreich gelingen.“

Nachhaltiges Sicherheitsbewusstsein

Moderne Industrieanlagen sind heute hochgradig vernetzte Systeme. Für viele Unternehmen – vom Mittelständler bis zum Industriekonzern – wird es immer wichtiger, Informationen möglichst schnell und direkt innerhalb des Unternehmens, mit Zulieferern oder Kunden auszutauschen. Dafür werden bisher physikalisch voneinander getrennte Bereiche über das Internet miteinander vernetzt – und damit angreifbar. Cyber-Kriminelle können diese Angriffsflächen ausnutzen. Sabotage, Spionage und Erpressung können die Folgen sein.

Immer wieder konnten in den vergangenen Jahren teils folgenschwere Angriffe auf industrielle Anlagen beobachtet werden. Besonders bedroht sind dabei industrielle Steuerungssysteme, die eine zentrale Rolle bei der Produktionssicherheit spielen und folglich besonders schützenswert sind. Das Bewusstsein für Cyber-Sicherheit ist bei den Unternehmen vor diesem Hintergrund gewachsen – und das nicht nur bei den Kritischen Infrastrukturen, die aufgrund des IT-Sicherheitsgesetzes ohnehin in die Cyber-Sicherheit ihrer Anlagen investieren müssen.

Bei der Digitalisierung von Produktionsabläufen spielt Cyber-Sicherheit eine Schlüsselrolle. Nur wenn Sicherheitsaspekte schon im Design berücksichtigt werden, kann die Digitalisierung erfolgreich gelingen und für die Unternehmen das gewünschte Potenzial entfalten. Ein wichtiges Anliegen des BSI ist es daher, ein nachhaltiges Sicherheitsbewusstsein in der Wirtschaft zu schaffen und eine solide Grundlage für die Digitalisierung zu legen.

Welche Gefährdung geht von Angriffen auf industrielle Steuerungssysteme aus? Wie schaffen Unternehmen die Voraussetzungen, um sich adäquat zu schützen? Wie kann Security-by-design helfen, den wachsenden Herausforderungen zu begegnen? In der neuen Ausgabe des BSI-Magazins stellen wir Ihnen einige Aspekte der Cyber-Sicherheit im Kontext der Industrie 4.0 vor. Ich wünsche Ihnen eine anregende Lektüre!

Ihr

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik

INHALT

AKTUELLES

Lagebericht

Lagebericht zur IT-Sicherheit 2017 in Berlin vorgestellt

Am 8.11.2017 stellten der damalige Bundesinnenminister Dr. Thomas de Maizière und BSI-Präsident Arne Schönbohm in Berlin den Bericht des BSI zur Lage der IT-Sicherheit in Deutschland 2017 vor. Der jährlich erscheinende Lagebericht der nationalen Cyber-Sicherheitsbehörde beschreibt und analysiert die aktuelle IT-Sicherheitslage, die Ursachen von Cyber-Angriffen sowie die verwendeten Angriffsmittel und -methoden. Daraus abgeleitet, zeigt das BSI Lösungsansätze zur Verbesserung der IT-Sicherheit in Deutschland auf.

Im Berichtszeitraum Juli 2016 bis Juni 2017 war die Gefährdungslage weiterhin auf hohem Niveau angespannt. Bekannte Einfallstore für Cyber-Angriffe blieben unverändert kritisch. Vor allem die gestiegene Anzahl an IT-Sicherheitsvorfällen mit Erpressungssoftware (Ransomware) zeigt, dass Cyber-Kriminelle hier eine lukrative Möglichkeit gefunden haben, in großem Umfang Geld zu erpressen.

Weitere Informationen: https://bsi.bund.de/Lageberichte

SPS-Drives

SPS IPC Drives 2017

Vom 28. bis zum 30. November war das BSI Aussteller auf der SPS IPC Drives 2017 in Nürnberg. Auf der internationalen Fachmesse für elektrische Automatisierung informierte das BSI zu Herausforderungen der Digitalisierung, die insbesondere im Kontext Industrial Security und Industrie 4.0 entstehen.

Weitere Informationen:
https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/news_SPSIPCDrives_27112017.html

Auszeichnung

Erfolgreiche BSI-Personalkampagne

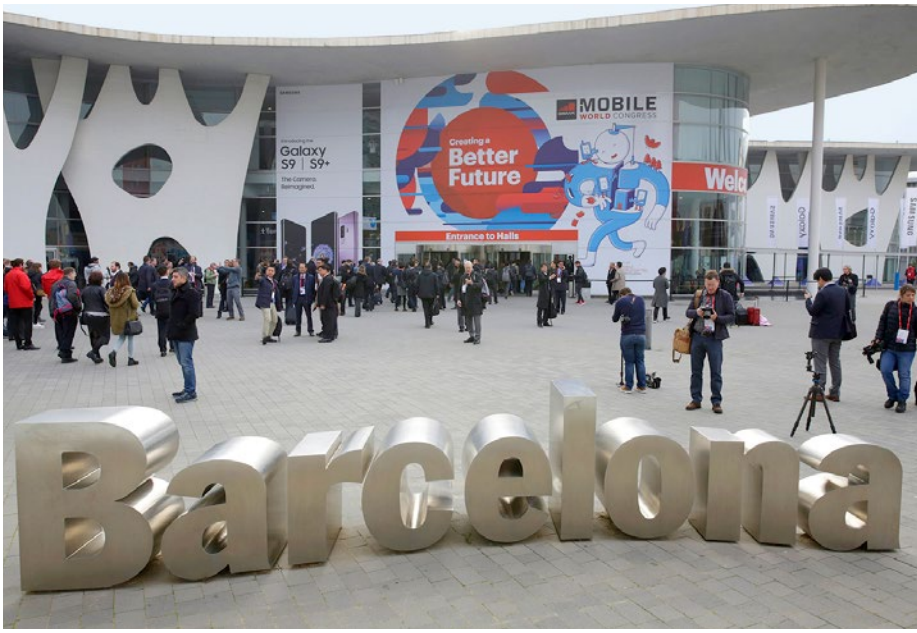
Um 180 neu geschaffene Stellen zu besetzen, ist das BSI im vergangenen Jahr in eine Personalmarketingoffensive gegangen. Die dafür entworfene Anzeigenkampagne kam bei der Zielgruppe offensichtlich gut an: Die Leser des Studierendenmagazins „audimax“ wählten sie zum Leserliebling der Ausgabe 5/17. Mit dem Motto „Was wir wollen: Deine digitale Seite“ wird das BSI auch 2018 weiterhin für neue Mitarbeiter werben.

Weitere Informationen: https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/news_erfolgreiche_Mitarbeiterwerbung_23012018.html

Ausstellung

Mobile World Congress 2018

Das BSI war erstmals vom 26. Februar bis 1. zum März 2018 in Barcelona als Aussteller auf dem Mobile World Congress, Europas größter Mobilfunkmesse, vertreten. Am Gemeinschaftsstand des Landes Nordrhein-Westfalen in Halle 6, Stand 6B40, zeigte die nationale Cyber-Sicherheitsbehörde Lösungen zur sicheren Identifizierung und Authentifizierung, die die Nutzung mobiler Anwendungen sicherer machen.



Weitere Informationen:
https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Mobile_World_23022018.html

BSI INTERNATIONAL

ZENTRALE BRITISCHE BEHÖRDE FÜR CYBER-SICHERHEIT (NCSC)

Sitz des NCSC in London

„Die Kommunikation mit der Öffentlichkeit ist absolut entscheidend für das National Cyber Security Centre.“

Interview mit Ciaran Martin, CEO NCSC

Das National Cyber Security Centre (NCSC) ist die zentrale Behörde Großbritanniens für Cyber-Sicherheit und wurde 2016 als Teil des Government Communications Headquarters (GCHQ) gegründet. Es hat vier Hauptaufgaben: In erster Linie soll es die Reaktion auf Vorfälle koordinieren und Kritische Infrastrukturen schützen. Außerdem soll es gewährleisten, dass sich die Bürger selbst automatisch schützen können, und es soll das Internet sicherer machen. Dies alles soll in Zusammenarbeit mit internationalen Organisationen geschehen.

Das NCSC wurde vor etwa eineinhalb Jahren ins Leben gerufen. Was war das Hauptziel seiner Gründung als Teil des GCHQ?

Die Regierung Großbritanniens nimmt das Thema Cyber-Sicherheit sehr ernst. Allerdings war klargeworden, dass die bisherige Strategie ausgedient hatte. Zu viele Institutionen waren daran beteiligt, aber keine konzentrierte sich auf das eigentliche Problem. Aus diesem Grund haben wir 2015 beschlossen, die Strategie zu ändern und uns neu zu organisieren. Das bedeutete, dass wir uns auf das konzentrieren wollten, was die Regierung tun konnte, um kriminelle, aber nicht sehr komplexe Angriffe abzuwehren. Hier kam unser Programm „Active Cyber Defense“ ins Spiel. Wir hätten das NCSC natürlich außerhalb der Behörde aufbauen können, aber das GCHQ hatte ja bereits Zugang zu Datenfunktionen, Fähigkeiten und Partnerschaften, die keine andere Institution hatte und die sich so nicht auf eine unabhängige Organisation hätten übertragen lassen. Daher haben wir das NCSC als Teil des GCHQ gegründet. Bedingung war, dass es einige Dinge anders handhabt als der Rest des GCHQ – insbesondere etwas, das absolut entscheidend für seine Mission ist: die Kommunikation mit der Öffentlichkeit.

Welche Erfolge konnte das NCSC seit seiner Gründung erzielen?

Die Bedrohung, vor der wir stehen, ist groß, vielfältig und wächst. Es kommen immer einige Angriffe durch, und die erste Pflicht des NCSC besteht darin, die Auswirkungen dieser Angriffe zu

„Das Programm Active Cyber Defense hat die durchschnittliche Zeit, die eine Phishing-Seite online ist, von 27 auf eine Stunde reduziert."

bewältigen und zu entschärfen. Im ersten Jahr unserer Tätigkeit haben wir auf 590 bedeutende Angriffe reagiert. Das reichte von Angriffen auf wichtige nationale Institutionen wie den National Health Service (NHS) und das britische und das schottische Parlament bis hin zu Attacken auf große und kleine Unternehmen und andere Organisationen.

Wir haben unser weltweit führendes Programm Active Cyber Defense im Jahr 2017 gestartet. Es hat seitdem Tausende von Angriffen verhindert und die durchschnittliche Zeit, die eine Phishing-Seite online ist, von 27 auf eine Stunde reduziert. Mit CyberFirst unterstützen wir die Entwicklung der nächsten Generation von Cyber-Experten. Inzwischen haben mehr als 1.000 junge Menschen an Kursen teilgenommen und im letzten Jahr konnten wir 8.000 junge Frauen dafür begeistern, an unserer ersten CyberFirst Girls Competition teilzunehmen.

Wir haben außerdem die wegweisende Initiative „Industry 100" ins Leben gerufen. Zielsetzung ist es, mit 100 Branchenexperten zusammenzuarbeiten bzw. sie in das NCSC einzubinden. Weltweit haben wir mit mehr als 50 Ländern auf fünf Kontinenten kooperiert und konnten ein bahnbrechendes Memorandum of Understanding mit der NATO unterzeichnen.

Wo sehen Sie Potenzial für zukünftige Entwicklungen und Verbesserungen des NCSC?

Wir sind stolz auf das, was wir in unserem ersten Jahr erreicht haben. Es gibt aber aktuell und in folgenden Jahren noch viel zu tun, um dieser strategischen Bedrohung unserer Werte, unseres Wohlstands und unserer Lebensweise zu begegnen.

Wir wollen intensiver mit Hochschulen und der Industrie zusammenarbeiten, um sicherzustellen, dass wir die Anforderungen des Privatsektors an die Fähigkeiten im Bereich Cyber-Sicherheit – sowohl jetzt als auch in Zukunft – verstehen und diese Lücke zuverlässig schließen können.

Ziel ist es, dass sich Organisationen selbstständig in ausreichendem Maß gegen Cyber-Bedrohungen verteidigen können. Damit bleiben uns mehr Kapazitäten, um uns auf die staatlichen Bedrohungen zu konzentrieren, die nur die Regierung bekämpfen kann.

Der Mangel an Diversität ist ein großes Problem innerhalb der Cyber-Sicherheitsbranche, und das NCSC ist bemüht, diesem durch Initiativen wie der CyberFirst Girls Competition abzuhelfen. Aber es gibt noch viel zu tun. Vielfältige Herausforderungen benötigen auch eine von Vielfalt geprägte Herangehensweise. Nur eine von zehn Personen, die in der Branche arbeiten, ist weiblich. Beim NCSC ist es schon ein Drittel – aber das ist immer noch nicht genug und etwas, das wir ändern wollen.

Welches Feedback erhält das NCSC von seinen Zielgruppen?

Die Rückmeldungen bei den Zielgruppen der verschiedenen Abteilungen des NCSC waren überaus positiv.

94 Prozent der Teilnehmer unserer Leitkonferenz „CYBERUK" erklärten, sie wüssten jetzt besser, warum das NCSC eingerichtet wurde, und hätten jetzt ein besseres Verständnis für unsere Struktur, unseren Ansatz und unsere Rolle bei der Umsetzung der nationalen Cyber-Sicherheitsstrategie.

Seit dem Start unseres Online-Kommunikationsforums CiSP (Cyber Information Sharing Partnership) im März 2013 hat die Industrie die Vorteile der Zusammenarbeit erkannt. Die Mitgliederzahl stieg rasant an (um 43 Prozent). Im Dezember 2017 hatten sich knapp 4.020 Organisationen und 9.097 Einzelpersonen aus 30 verschiedenen Industriesektoren angemeldet. Während der WannaCry-Ransomware-Attacke erwies sich das CiSP als äußerst wertvoll: Es stellte topaktuelle Ratschläge zur Schadensbegrenzung bereit und räumte gleichzeitig mit falschen Gerüchten auf.

Zahlreiche Teilnehmerinnen unserer CyberFirst Girls Competition zeigen Interesse an einer Karriere in der Informatik.

Mit über 100.000 Besuchern in einem einzigen Monat entwickelt sich unsere Website zunehmend zu einem Eckpfeiler der Cyber-Community. Unser Twitter-Account hat über 32.000 Follower, die konstruktiv mit den Ratschlägen umgehen, die wir dort veröffentlichen.

Was sind Ihre strategischen Themen in der Cyber-Sicherheit für die nächsten Jahre? National und international?

Am wichtigsten ist es, die grundlegenden Abwehrfähigkeiten zu verbessern. Wir haben einige Methoden entwickelt, dies umzusetzen, und wir müssen sie nun entsprechend gewichten. Außerdem müssen wir die Sicherheitsautomatismen von Technologie deutlich stärken, einschließlich der Integration von Sicherheit ins grundlegende Design.

Kurzprofil Ciaran Martin

Ciaran Martin wurde am 15. März 2016 zum ersten CEO des NCSC ernannt, nachdem er seit Februar 2014 die Position des Director General for Cyber Security des GCHQ innehatte. Bis April 2016 war er außerdem verantwortlich für die Strategie des GCHQ für den Umgang mit Informationsrisiken sowie für die Richtlinien und die Kommunikation der Abteilung.

Eine dritte Priorität besteht darin, unsere komplexen Fähigkeiten stets auf dem neusten Stand zu halten, um den ebenfalls sehr komplexen Angriffen zu begegnen. Ein letzter Punkt ist, dass wir all das auf internationaler Ebene zusammen mit unseren Verbündeten und Kollegen tun. Ich glaube fest daran, dass das Internet die liberalen westlichen Werte nicht erfunden hat. Im Gegenteil: Es wurde von ihnen erfunden und diese Freiheiten sind wertvoll und hart erkämpft. Länder wie Großbritannien und Deutschland stehen auf der gleichen Seite, wenn es darum geht, sie zu verteidigen.

Wie beurteilen Sie die Zusammenarbeit des NCSC mit Deutschland und dem BSI?

Deutschland ist einer der wichtigsten Partner des NCSC. Arne Schönbohm und ich treffen uns regelmäßig, um die gemeinsamen Herausforderungen zu diskutieren. Unsere Zusammenarbeit mit dem BSI, insbesondere bei der Reaktion auf Vorfälle, ist äußerst wertvoll. Ich war wirklich enttäuscht, dass ich kurzfristig die Teilnahme am BSI-Kongress im Mai absagen musste, aber wir steckten noch mitten in der WannaCry-Krise. Arne Schönbohm war hier sehr verständnisvoll!

Gibt es gemeinsame Interessengebiete mit Deutschland? Wo sehen Sie Unterschiede?

Mit Deutschland haben wir weit mehr Gemeinsamkeiten als Unterschiede: Wenn ich mir das Portfolio unserer jeweiligen Arbeit zum Thema Cyber-Sicherheit anschaue, sehe ich sehr wenig darin, was allein Fokus eines britischen oder deutschen Unternehmens sein könnte.

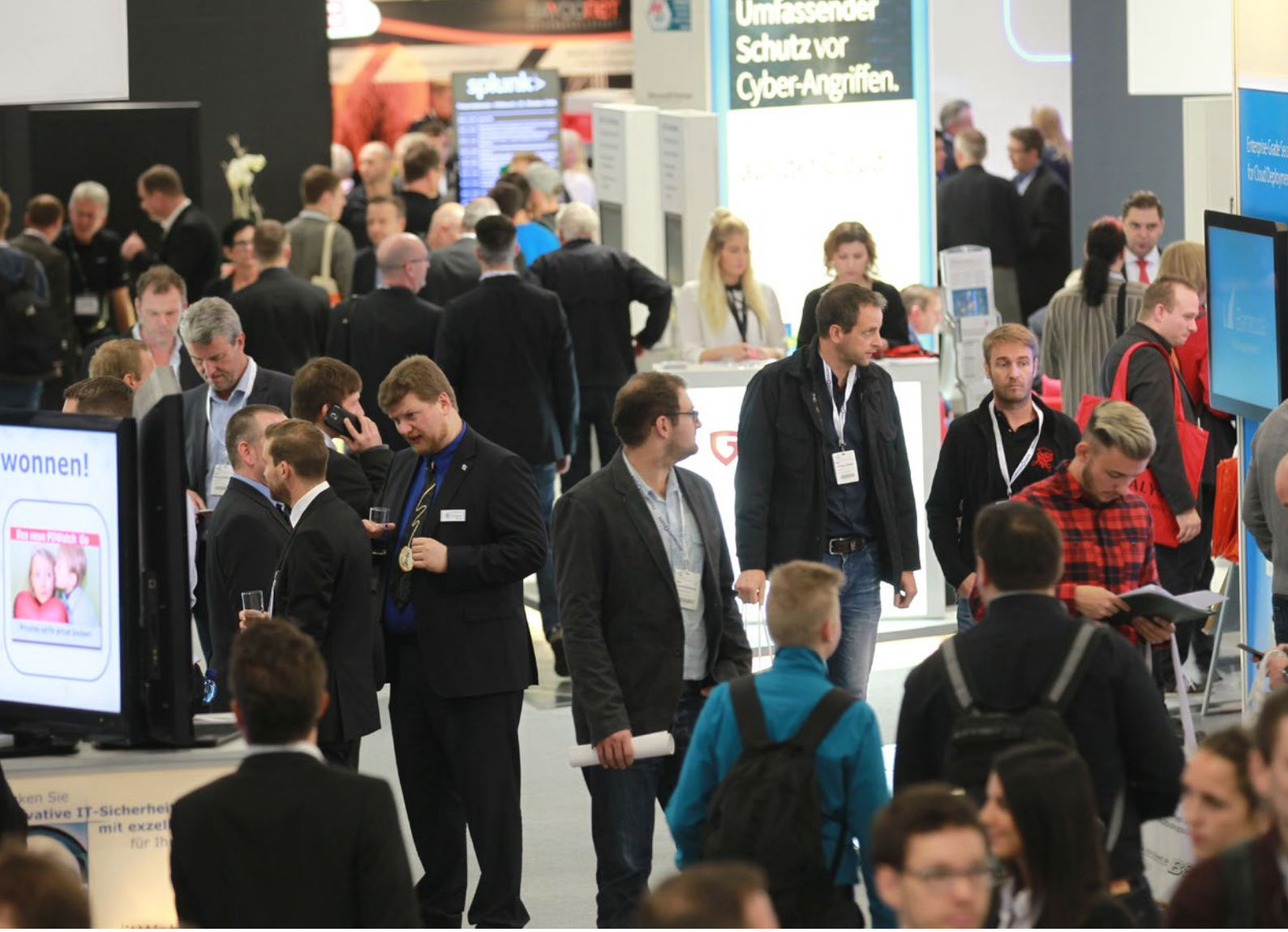
Wie wird das NCSC die Herausforderungen durch den Brexit meistern??

Wir wissen noch nicht, wie genau das künftige Verhältnis Großbritanniens zur EU aussehen wird. Aber die Regierung hat von Anfang an gesagt, dass sie eine tiefe und besondere Partnerschaft mit der EU wünscht. Im Hinblick auf das Thema Sicherheit haben wir deutlich gemacht, dass unser Engagement für Europa uneingeschränkt weiterbesteht. Was auch immer passiert, wir wollen beim Thema Cyber-Sicherheit in enger Partnerschaft mit Deutschland zusammenarbeiten.

Im nächsten Jahr wird das GCHQ sein 100-jähriges Jubiläum feiern. Was denken Sie ... Was werden die Historiker sagen, wenn sie auf die Geschichte des NCSC und die Geschichte der Cyber-Sicherheit zurückblicken, wenn das NCSC 2110 seinen 100. Geburtstag feiert?

Wir alle, die wir von Anfang an am NCSC beteiligt waren, sind sehr überzeugt von dem, was wir tun. Ich hoffe, dass dies als eine Zeit in Erinnerung bleibt, in der wir mit einer Regierungsbehörde etwas Besonderes und Innovatives vollbracht haben. Es kommt nicht oft vor, dass Sie die Chance haben, einen neuen Ansatz zu wählen und ein Problem von Grund auf zu lösen – und das auch noch gemeinsam mit Partnern. Was wir jetzt im Bereich der Cyber-Sicherheit tun, wird darüber bestimmen, wie frei, sicher und erfolgreich wir im nächsten Jahrhundert sein werden. Daher wünsche ich mir, dass Historiker im Rückblick das NCSC als den Eckpfeiler dieser Werte betrachten werden.

Weitere Informationen: https://www.ncsc.gov.uk/



Internationales Symposium ViS!T erstmals zur it-sa

Sichere Informationstechnologie in der Verwaltung

Zum ersten Mal findet das Symposium „Verwaltung integriert sichere Informationstechnologie“ – kurz ViS!T – zur IT-Security Messe it-sa in Nürnberg statt. Auf Einladung des Bundesamts für Sicherheit in der Informationstechnik diskutieren Fachleute aus Deutschland, Österreich, der Schweiz und Luxemburg im Rahmen der ViS!T aktuelle Herausforderungen bei der sicheren Gestaltung von IT-Prozessen. Das Symposium findet alle zwei Jahre statt und wird abwechselnd von einem der beteiligten Länder ausgerichtet.

Das Symposium ViS!T richtet sich an Mitarbeiterinnen und Mitarbeiter in den öffentlichen Verwaltungen der beteiligten Länder. Zielgruppe sind dabei nicht zwangsläufig nur IT-Spezialisten. Das Symposium spricht auch und vor allem die Generalisten und Strategen an. Es geht um den Erfahrungsaustausch, um die multilaterale Diskussion über Vorhaben und Projekte mit dem Fokus IT-Sicherheit.

Beteiligt sind neben dem BSI aus Deutschland, das Zentrum für sichere Informationstechnologie – Austria (A-Sit) aus Österreich, das Informatiksteuerungsorgan des Bundes ISB aus der Schweiz sowie die Regierung des Großherzogtums Luxemburg. Ziel ist es, in den beteiligten Ländern, aber auch darüber hinaus, ein vergleichbares und möglichst auch verbindliches IT-Sicherheitsniveau zu erreichen.

Das Symposium ViS!T findet in diesem Jahr am 08./09. Oktober im Rahmen der IT-Security Messe it-sa statt, die ihrerseits vom 9. bis zum 11. Oktober in Nürnberg ihre Tore öffnet. Auf dem Programm der ViS!T, die in diesem Jahr zum neunten Mal stattfindet, stehen Diskussionen zu Themen der IT-Sicherheit in der Verwaltung. Diese Themen schließen unter anderem Blockchain, IT-/Informationssicherheitsgesetze oder Digitalisierung ein. Erwartet werden rund einhundert Teilnehmer. Wenn auch Sie dazu gehören möchten und im Bereich Verwaltung tätig sind, können Sie sich in Kürze unter dem unten stehenden Link registrieren.

Die it-sa ist mit 630 Ausstellern aus 24 Ländern und mehr als 12.000 Fachbesuchern im vergangenen Jahr eine der wichtigsten Messen zum Thema Informationssicherheit weltweit. Seit 2009 wendet sie sich als eigenständige Messe an alle, die sich beruflich mit dem Thema IT-Sicherheit beschäftigen. Dazu gehören sowohl Entwickler und Praktiker wie auch Projektleiter und Manager. In diesem Jahr erweitern das Sicherheitsnetzwerk München und die Information Security Society Switzerland das Partnernetzwerk der it-sa. ■

Symposium ViS!T: BETEILIGTE INSTITUTIONEN

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde 1991 gegründet und ist eine Bundesoberbehörde, die dem Bundesministerium des Innern untersteht. Als die nationale Cyber-Sicherheitsbehörde gestaltet das BSI Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Das Zentrum für sichere Informationstechnologie – Austria (A-SIT) wurde 1999 als gemeinnütziger Verein gegründet. Seine Mitglieder sind die öffentlichen Institutionen, das Bundesministerium für Finanzen (BMF), die Oesterreichische Nationalbank (OeNB), die Technische Universität Graz (TU Graz) und die Bundesrechenzentrum GmbH (BRZ GmbH).

Das Informatiksteuerungsorgan des Bundes ISB sorgt in der Schweiz für die Umsetzung der Strategie zur Informations- und Kommunikationstechnik in der Bundesverwaltung. Außerdem koordiniert es die Zusammenarbeit von Bund, Kantonen und Gemeinden im Bereich E-Government und führt die Melde- und Analysestelle Informationssicherung MELANI.

Die Regierung des Großherzogtums Luxemburg verabschiedete am 21. Januar 2015 den Entwurf eines Dekrets zur Einrichtung eines Regierungssystems zur Förderung der Informationssicherheit, das unter anderem die Einrichtung einer nationalen Agentur für die Sicherheit der Informationssysteme (ANSSI) für den öffentlichen Sektor und für kritische Infrastrukturen regelt.

Weitere Informationen: https://www.bsi.bund.de/anmeldung_visit

Regulierung für Digitale Dienste

von Marc Schober, Referatsleiter KRITIS-Sektoren Finanz- und Versicherungswesen, IT und TK, Digitale Dienste

Neue Regeln ab Mai 2018

Neue Regeln für ein europaweit einheitliches Mindestsicherheitsniveau stärken den Schutz von Online-Marktplätzen, Suchmaschinen und Cloud-Diensten. Und eine neu eingeführte Meldepflicht für „Sicherheitsvorfälle mit erheblichen Auswirkungen“ verbessert die koordinierte Reaktion auf Cyber-Angriffe. Anbieter Digitaler Dienste müssen die Vorgaben ab Mai 2018 umsetzen.

Wirtschaft und Gesellschaft unterbrechungsfrei mit Strom, Telekommunikation und anderen Kritischen Dienstleistungen zu versorgen, ist seit jeher von essenzieller Bedeutung. Einrichtungen, Institutionen und Unternehmen, die dies gewährleisten, zählen zu den Kritischen Infrastrukturen (KRITIS) und bedürfen eines besonderen Schutzes gegen Cyber-Angriffe. Dem wurde folgerichtig bereits 2015 mit dem IT-Sicherheitsgesetz und der 2016 verabschiedeten EU-Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) Rechnung getragen.

Doch infolge der immer schneller voranschreitenden Digitalisierung geht die Abhängigkeit von Wirtschaft und Gesellschaft weit über den KRITIS-Bereich hinaus. Auch Digitale Dienste wie Suchmaschinen, Cloud-Dienste und Online-Marktplätze müssen störungsfrei funktionieren und ihren Nutzern ein angemessenes Sicherheitsniveau bieten. Die NIS-Richtlinie sieht daher, neben der Regulierung von Kritischen Infrastrukturen, eine EU-weit harmonisierte Regulierung der Anbieter Digitaler Dienste vor. Die Regelungen wurden bereits im Sommer 2017 mit dem Gesetz zur Umsetzung der NIS-Richtlinie in nationales Recht (§ 8c BSIG) überführt und sind ab dem 10. Mai 2018 anwendbar.

DIGITALE DIENSTE

Als Digitale Dienste im Gesetzeskontext gelten dabei ausschließlich Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste (§ 2 Abs. 11 BSIG). Soziale Netzwerke oder Karten- und Navigationsanwendungen werden von den Regelungen nicht erfasst.

- **Online-Marktplätze im Sinne des Gesetzes müssen Angebote mehrerer Anbieter bündeln und den Vertragsabschluss ermöglichen. Onlineshops von einzelnen Händlern oder reine Preisvergleichsportale werden daher nicht von der neuen Regulierung erfasst.**
- **Auf das eigene Webangebot beschränkte Suchfunktionen gelten ausdrücklich nicht als Online-Suchmaschinen.**
- **Cloud-Computing-Dienste im Sinne des Gesetzes müssen den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen.**

Im Unterschied zur KRITIS-Regulierung unterliegen automatisch alle Anbieter aus den erfassten Dienstekategorien der Regulierung, sofern sie nicht als Kleinst- bzw. kleines Unternehmen weniger als 50 Mitarbeiter haben oder weniger als zehn Millionen Euro Jahresumsatz machen.

Welcher EU-Mitgliedsstaat jeweils für die Aufsicht über den Anbieter zuständig ist, richtet sich nach dessen Hauptsitz. Liegt dieser außerhalb der EU, ist der Sitz eines durch den Anbieter benannten Vertreters maßgeblich. Einige große Anbieter fallen daher nicht unter die Zuständigkeit des BSI, obwohl der deutsche Markt für ihr Europageschäft eine zentrale Rolle spielt. Dieser Nachteil wird durch eine engere Vernetzung der zuständigen nationalen Behörden und der Computer Security Incident Response Teams (CSIRT) der Mitgliedsstaaten ausgeglichen.

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Im Mittelpunkt der neuen Regelungen steht das Ziel, Sicherheitsvorfällen vorzubeugen bzw. deren Auswirkungen auf die Digitalen Dienste zu minimieren. Dazu haben die Anbieter dem Risiko angemessene Maßnahmen unter Berücksichtigung des Standes der Technik zu treffen. Die Anforderungen gehen dabei deutlich über die des Telemediendienstgesetzes hinaus, das bereits seit 2015 Schutzvorkehrungen für alle gewerblich genutzten Internetseiten vorschreibt (§ 13 Abs. 7 TMG). Zu berücksichtigen sind die folgenden Aspekte:

1. **Sicherheit der Systeme und Anlagen**
2. **Erkennung, Analyse und Bewältigung von Sicherheitsvorfällen**
3. **Betriebskontinuitätsmanagement (Business Continuity Management)**
4. **Überwachung, Überprüfung und Erprobung**
5. **Einhaltung internationaler Normen**

Die EU-Kommission hat zu den fünf Aspekten konkretisierte Sicherheitselemente per Durchführungsverordnung festgelegt.

Regelmäßige Nachweise der getroffenen Sicherheitsmaßnahmen gegenüber dem BSI sind nicht vorgesehen. Ganz bewusst wurde hier der Ansatz einer Ex-post-Regulierung gewählt, da ein effektives Risiko- und Sicherheitsmanagement für einen Digitalen Dienst ohnehin im Interesse des Anbieters liegt. In begründeten Fällen, z.B. bei Sicherheitsvorfällen, kann das BSI aber entsprechende Unterlagen anfordern und auf der Beseitigung eventueller Sicherheitsmängel bestehen.

MELDUNG VON SICHERHEITSVORFÄLLEN

Ist ein Digitaler Dienst von einer IT-Störung oder einem Cyber-Angriff betroffen, so können dadurch erhebliche Auswirkungen für professionelle oder private Nutzer des Dienstes entstehen. Insbesondere bei Cyber-Angriffen kann oft nicht ausgeschlossen werden, dass auch noch weitere Anbieter im Fokus der Angreifer stehen könnten.

Daher haben Anbieter Digitaler Dienste Sicherheitsvorfälle „mit erheblichen Auswirkungen“ unverzüglich an das BSI zu melden. Die entsprechenden Kriterien und Schwellenwerte zur Definition erheblicher Auswirkungen wurden ebenfalls vorab durch die EU-Kommission festgelegt. Sie berücksichtigen sowohl den für einzelne Nutzer entstandenen finanziellen Schaden als auch die Gesamtdauer von Ausfällen und die Anzahl betroffener Nutzer bei Datendiebstahl oder Sabotage.

AKTIVITÄTEN DES BSI

Das BSI hat auf seiner Webseite ein Informationsangebot für Anbieter Digitaler Dienste eingerichtet. Fragen zur Regulierung beantwortet gerne auch die zuständige Geschäftsstelle im BSI (siehe Infobox).

Zudem sollen die Anbieter – analog zu KRITIS-Betreibern – zukünftig auch die Warn- und Informationsverteiler des BSI beziehen können. Dazu wird eine freiwillige Registrierung notwendig sein. Außerdem ist ein Arbeitskreis geplant, um den Austausch zwischen BSI und Anbietern zu fördern. ■

Weitere Informationen:
https://www.bsi.bund.de/DSP

Kontakt Geschäftsstelle:
digitale.dienste@bsi.bund.de
0228 / 999582 6656

CYBER-SICHERHEIT

Einstieg leicht gemacht

von Katrin Alberts und Holger Schildt, Referat IT-Grundschutz

Basis-Absicherung nach IT-Grundschutz

Das BSI bietet mit der Basis-Absicherung nach IT-Grundschutz kleinen Unternehmen und Behörden sowie Selbstständigen einen einfachen Einstieg in einen Sicherheitsprozess an. Anhand eines Leitfadens können Verantwortliche den Status der Informationssicherheit in ihrer Institution in drei Schritten überprüfen und verbessern.

Umfragen wie zuletzt die Cyber-Sicherheits-Umfrage der Allianz für Cyber-Sicherheit (siehe S. 22/23) zeigen es immer wieder: Awareness für Informationssicherheit ist in der Regel vorhanden – an der Umsetzung von Maßnahmen, um das Sicherheitsniveau zu erhöhen, mangelt es jedoch häufig noch. Der Dialog mit kleinen und mittelständischen Unternehmern sowie Selbstständigen ergibt meist dasselbe Bild: Es fehlt häufig (noch) an geschultem Personal, dem notwendigen Wissen und finanziellen Spielräumen, notwendige Maßnahmen nachhaltig und sinnvoll umzusetzen. Sichere Datenhaltung, grundlegender Schutz der eingesetzten PCs, Tablets und Smartphones gegen unerwünschte Zugriffe von außen sind vielen Verantwortlichen wichtig. Doch die zu überwindende Hürde, um sich mit Sicherheitsaspekten zu befassen, ist häufig noch zu hoch.

PRAXISTAUGLICHE LÖSUNG FÜR INSTITUTIONEN JEDER GRÖSSENORDNUNG

Genau hier setzt die Basis-Absicherung an. Im Rahmen der IT-Grundschutz-Methodik ist sie ein Einstieg für alle Unternehmen und Behörden zur Absicherung ihrer IT-Systeme und Informationen. Sie liefert einen kompakten und übersichtlichen Einstieg zum Aufbau eines Managementsystems für Informationssicherheit (ISMS) in einer Institution. Dabei handelt es sich um ein geplantes und organisiertes Vorgehen, um ein angemessenes Sicherheitsniveau für die Informationssicherheit zu erzielen und aufrechtzuerhalten.

Die Basis-Absicherung basiert auf dem bewährten BSI-Standard 200-2 zur IT-Grundschutz-Methodik und erläutert elementare Schritte, mit denen das Informationssicherheitsniveau in einer Institution überprüft und gesteigert werden kann. Im Vordergrund stehen praxisnahe Sicherheitsanforderungen mit dem Ziel, die Einstiegshürde in den Sicherheitsprozess so niedrig wie möglich zu halten und allzu komplexe Vorgehensweisen zu vermeiden. Neben technischen Aspekten werden im Sinne eines ganzheitlichen Managementsystems zur Informationssicherheit auch infrastrukturelle, organisatorische und personelle Themen betrachtet. Damit ermöglicht die Basis-Absicherung ein Mindestmaß an Informationssicherheit auf Basis des modernisierten IT-Grundschutzes über alle Geschäftsprozesse und Fachverfahren hinweg.

In kleineren Unternehmen oder Behörden – von Selbstständigen ganz zu schweigen – ist es häufig eine besondere Herausforderung, einen Verantwortlichen zu benennen, der sich den Fragen der Informationssicherheit annimmt. Ist

IN DREI SCHRITTEN ZUR INFORMATIONSSICHERHEIT

Der Prozess, mit dem das Informationssicherheitsniveau erhöht wird, ist bei der Basis-Absicherung in drei Schritte aufgeteilt.

1 Zunächst muss festgelegt werden, wer die Verantwortung für den gesamten Prozess übernimmt. Im Fokus der ersten Betrachtungen steht auch, den Geltungsbereich einzugrenzen: Welche Systeme müssen überprüft werden, welche können – aus welchen Gründen – außen vor bleiben?

2 Im nächsten Schritt müssen die Sicherheitsziele benannt und festgeschrieben sowie eine Leitlinie verfasst werden. Die Leitungs- oder Managementebene sollte in jedem Fall frühzeitig eingebunden werden. Zur Organisation des Sicherheitsprozesses zählt primär, ihn zu konzeptionieren und zu planen. Dabei gilt es beispielsweise, Erkenntnisse und Maßnahmen aus dem Prozess in bestehende Abläufe und Prozesse zu integrieren. Anwendungen, die „plötzlich" sicher sind, dafür aber ständig abstürzen, sind wenig hilfreich.

3 Im dritten Schritt wird der Sicherheitsprozess durchgeführt. Kernaufgabe ist dabei die Umsetzung der zuvor festgelegten Sicherheitskonzeption. Je nach Größe der Institution können dazu IT-Grundschutz-Bausteine zu einzelnen Themen aus dem IT-Grundschutz-Kompendium herangezogen werden.

die Institution etwas größer, fällt die Aufgabe in der Regel einem dezidierten Informationssicherheitsbeauftragten (ISB) zu. Diese Rolle muss auch in kleineren Institutionen eingerichtet sein. Hier ist dies aber eine Aufgabe, die ein Mitarbeiter neben anderen Aufgaben übernimmt. Beispielsweise könnten Mitarbeiter aus den Bereichen Finanzen und Controlling, IT-Betrieb oder der betriebliche Datenschutzbeauftragte diese übernehmen.

PRAKTIKABLE HANDLUNGSEMPFEHLUNGEN ZUM NACHLESEN

Mit der Basis-Absicherung können in einem ersten Schritt zeitnah die wichtigsten Sicherheitsanforderungen umgesetzt werden. Darauf aufbauend kann das Sicherheitsniveau zu einem späteren Zeitpunkt weiter erhöht werden, beispielsweise indem alle Bereiche mit der Standard-Absicherung oder kritische Geschäftsprozesse mit der Kern-Absicherung geschützt werden. ■

Die Basis-Absicherung als Einstieg für Institutionen jeder Größenordnung gibt es auch zum Nachlesen in einem handlichen Leitfaden als Printbroschüre und online auf den BSI-Webseiten unter https://www.bsi.bund.de/grundschutz

CYBER-SICHER FAHREN

von Thomas Strubbe und Christian Wieschebrink, Referat Cyber-Sicherheit für die Digitalisierung in Verkehr und Industrie 4.0,
und Prof. Markus Ullmann, Referatsleiter Technologische Grundlagen sicherer elektronischer Identitäten, Chipsicherheit

Automatisierte und vernetzte Fahrzeuge

Die zunehmende Digitalisierung macht auch vor der Automobilindustrie nicht Halt. Assistenzsysteme, die den Fahrer beim Einparken oder Halten der Spur unterstützen, sind längst üblich und auch der WLAN-Hotspot im Fahrzeug ist keine Seltenheit mehr. Mit diesen technischen Entwicklungen steigt auch das Angriffspotenzial aus dem Cyber-Raum.

In vielen heute am Markt verfügbaren Fahrzeugmodellen gehört eine Internetanbindung über Mobilfunk zur Standardausstattung. Durch neue Technologien wie der Fahrzeug-zu-Fahrzeug-Kommunikation und eCall nimmt der Grad der Vernetzung noch zu. Dazu kommen die Ankündigungen der Hersteller, in absehbarer Zukunft hoch automatisierte Fahrzeuge auf den Markt bringen zu wollen.

Im Hinblick auf die Cyber-Sicherheit solcher hochgradig vernetzter Fahrzeuge sieht auch die Politik in diesem Bereich großen Handlungsbedarf. In der „Strategie automatisiertes und vernetztes Fahren“ der Bundesregierung wird explizit darauf hingewiesen, dass klare IT-Sicherheitsstandards, insbesondere im Hinblick auf die Zulassung von Fahrzeugen, notwendig sind. Das BSI wirkt aktiv zusammen mit dem Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) an der Erarbeitung von entsprechenden Kriterien und an der zukünftigen Ausrichtung der Cyber-Sicherheit im Straßenverkehr mit.

FAHRZEUG-HACKS

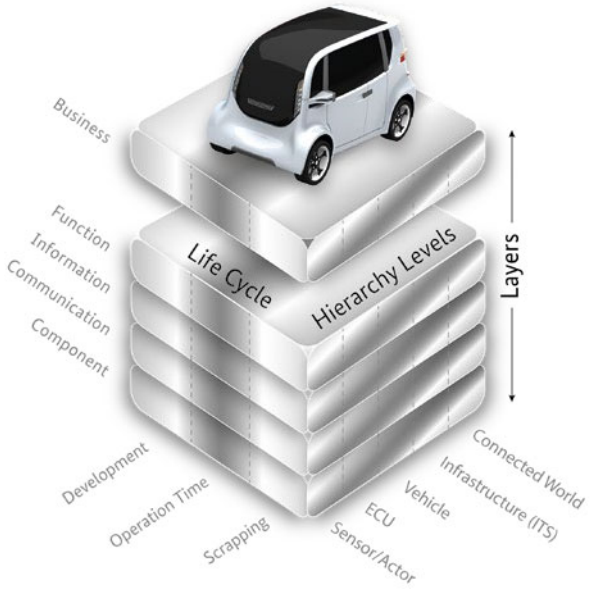
Während Angriffe auf die Fahrzeugelektronik in der Vergangenheit vor allem auf den Diebstahl des Gefährts abzielten, zeigen die Entwicklungen der letzten Jahre, dass mittlerweile das Angriffspotenzial wesentlich weiter geht.

Es ist eine Reihe von weiteren Angriffen auf Fahrzeugsysteme publiziert worden, die die Gefährdung von vernetzten Fahrzeugen aufzeigen. Beispielsweise wurde demonstriert, dass über schlecht gesicherte Infotainment-Module in Fahrzeugen per Internetverbindung in die Fahrfunktionalität eingegriffen werden konnte. Des Weiteren erwiesen sich bestimmte Smartphone-Apps als angreifbar, die Fahrzeugfunktionen, wie z. B. das Öffnen der Türen oder den Abruf von Fahrzeuginformationen, steuerten.

In eigenen Untersuchungen zeigte das BSI Schwachstellen auf, die die Privatsphäre von Fahrern betreffen. Dazu gehört die Identifikation von Fahrzeugen anhand von Bluetooth-Signalen und die Schwächen in den Pseudonymisierungsfunktionen der zukünftigen Fahrzeug-zu-Fahrzeug-Kommunikation.

ABSTRAKTE REFERENZARCHITEKTUR

Um übergreifende Fragestellungen zur IT-Sicherheit in Fahrzeugen untersuchen und diskutieren zu können, wird ein Architekturmodell benötigt, das modell- und



Ergebnis der Zusammenarbeit von Industrie, Verbänden und Behörden: Das Architekturmodell RAMA

herstellerunabhängig ist und keine konkrete IT-Architektur im Fahrzeug voraussetzt. Aus dieser Motivation heraus wurde das „Reference Architecture Model Automotive“ (RAMA) entwickelt (basierend auf RAMI 4.0, DIN SPEC 91345).

RAMA ist ein Ergebnis der Zusammenarbeit von Industrie, Verbänden und Behörden innerhalb der Unterarbeitsgruppe IT-Sicherheit (UAG IT-Sicherheit) des BMVI und BSI.

RAMA betrachtet das Fahrzeug in drei Dimensionen:

- Hierachy Levels: Diese ordnen das Fahrzeug von kleinen Einheiten wie Sensoren, über Computer im Fahrzeug und das Fahrzeug als Ganzes bis hin zur vernetzten Welt ein.

- Layers: Sie beschreiben die Komponenten von der Hardware-Ebene bis zur Anwendung.

- Life Cycle: Hier wird zwischen der Entwicklung, der Nutzung und schließlich der Verschrottung unterschieden.

Die Möglichkeit, RAMA in die benötigten Einzelblöcke zu zerlegen, erlaubt es, herstellerunabhängig IT-Funktionalitäten auf einem abstrakten Niveau zu modellieren und zu untersuchen.

RAMA wurde als Vorschlag in die entsprechenden Arbeitsgruppen der Wirtschaftskommission für Europa der Vereinten Nationen (UNECE) eingebracht, in denen Anforderungen an die Typzulassung von Fahrzeugen mit Gültigkeit in den derzeit 54 Vertragsstaaten des UNECE-Übereinkommens definiert werden.

AUSBLICK

Die Entwicklungen in der Fahrzeugindustrie werden neue Anforderungen sowohl an Automobilhersteller als auch den Gesetzgeber mit sich bringen. Ein Angriff auf ein vollautomatisiertes Fahrzeug hätte nicht nur Folgen für die Insassen, sondern könnte auch seine Umgebung gefährden. Darum muss es entsprechende Zulassungskriterien für Fahrzeuge geben. Dazu kann auch ein passendes Zertifizierungskonzept gehören.

Zurzeit erstellt die Industrie im Kontext der internationalen Standardisierung ein Vorgehensmodell zum Cybersecurity-Engineering in Fahrzeugen (ISO/IEC WD 21434), das die Entwicklungsphase und das Security-Management im Feld beinhaltet.

Eine weitere Forderung des BSI ist die Absicherung von Fahrzeugen über die gesamte Lebensdauer. So sollte etwa die Kryptoagilität, das heißt die Migrierbarkeit von in den Komponenten implementierten kryptografischen Verfahren, früh im Entwicklungsprozess berücksichtigt werden. Dies beinhaltet auch sichere Update-Mechanismen (z.B. für Security-Patches) über den Lebenszyklus des Fahrzeugs. ■

Weitere Informationen:
Strategie automatisiertes und vernetztes Fahren der Bundesregierung: http://www.bmvi.de/SharedDocs/DE/Publikationen/DG/broschuere-strategie-automatisiertes-vernetztes-fahren.html
https://www.bmvi.de/SharedDocs/DE/Artikel/LA/internationale-harmonisierung-der-technischen-vorschriften-fuer-kraftfahrzeuge.html

Sicherheit für Entwickler

von Dr. Peter Birkner und Dr. Aron Gohr, Referat Evaluierung kryptografischer Verfahren und Forschungskoordinierung

Die Technischen Richtlinien zur Kryptografie

Seit 2008 gibt das BSI Richtlinien mit Empfehlungen zur Nutzung kryptografischer Primitive im Rahmen der TR-02102 heraus. Sie enthalten zum einen allgemeine kryptografische Empfehlungen, die die wesentlichen, heute praxisrelevanten Aspekte der Entwicklung kryptografischer Anwendungen umfassen. Zum anderen geben sie konkrete Empfehlungen, wie bestimmte kryptografische Protokolle eingesetzt und konfiguriert werden sollen. Der nachfolgende Artikel beschreibt die Geschichte dieser Technischen Richtlinien (TR) und beleuchtet ihre heutige Rolle im Kontext anderer kryptografischer Standards und Leitlinien.

„Die Richtlinie erleichtert die Entwicklung oder Konfiguration kryptografischer Systeme.“

Die erste Fassung der Technischen Richtlinie TR-02102 aus dem Jahr 2008 gab nur allgemeine kryptografische Empfehlungen zur Wahl von Schlüssellängen und kryptografischen Verfahren. Diese Empfehlungen – der heutige Teil 1 der TR – richteten sich primär an die Entwickler neuer kryptografischer Anwendungen.

Am Anfang des laufenden Jahrzehnts zeigte sich, dass die TR die veränderten Rahmenbedingungen, unter denen kryptografische Techniken eingesetzt wurden, nicht mehr ausreichend widerspiegelte. Dem wurde einerseits mit einer grundlegenden Überarbeitung der TR im Jahr 2012 begegnet und andererseits mit einer inhaltlichen Erweiterung, die zu einer Aufteilung der Richtlinie in zunächst zwei und heute vier Teile führte.

Während die TR-02102-1 weiterhin grundlegende Empfehlungen zur Wahl von kryptografischen Verfahren und Schlüssellängen enthält, geben die anderen Richtlinien der Serie praktische Hinweise zur Einrichtung kryptografischer Protokolle, wie sie zum Beispiel für Systemadministratoren von Interesse sein können. Konkret befasst sich der Teil 2 mit der Nutzung von TLS, der Teil 3 mit IKE/IPsec und Teil 4 mit SSH.

Seit 2016 werden alle Teile dieser Technischen Richtlinie auch in englischer Sprache veröffentlicht und erreichen damit einen internationalen Anwender- und Leserkreis.

ZIELSETZUNG DER TECHNISCHEN RICHTLINIE

Allgemein haben die vier Teile der TR-02102 empfehlenden Charakter. Sie sollen eine Entwicklung oder Konfiguration kryptografischer Systeme erleichtern, die dem jeweiligen Stand der Technik entspricht. Es gibt aber kein institutionalisiertes Prüfschema, das kryptografische Systeme gegen die TR prüft. So sind im Rahmen von Zulassungsverfahren des BSI zum Beispiel Abweichungen von den TR-Empfehlungen möglich, wenn sie notwendig sind und hinsichtlich der in dem jeweiligen Produkt erreichten Sicherheitseigenschaften hinreichend begründet werden können.

Solche Abweichungen sind nicht automatisch nachteilig für die Sicherheit einer Anwendung: Es gibt viele krypto-

grafische Verfahren, die als sicher gelten und die relativ gut untersucht sind, aber die nicht in der TR-02102 empfohlen werden. Die TR behandelt nur solche Verfahren, die vom BSI als besonders relevant eingeschätzt werden. Bildlich ausgedrückt entspricht die TR eher einem kryptografischen Bausatz mit vorgefertigten, als sehr solide bekannten Teilen als einer Enzyklopädie aller derzeit als sicher zu bewertenden Verfahren.

„Als Sicherheitsniveau werden 100 Bit angestrebt – ab 2023 sollen es 120 Bit sein."

WIRKUNG DER TECHNISCHEN RICHTLINIE

Auch wenn die TR-02102 insgesamt lediglich Empfehlungen enthält, gibt es doch Kontexte, in denen diese Empfehlungen verbindlich werden. Ein Beispiel dafür ist der „Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden". Dieser wurde erstmals im Jahr 2014 nach § 8 Abs. 1 Satz 1 BSIG herausgegeben und macht die aktuell gültige Fassung der TR-02102-2 zur Nutzung von TLS für Bundesbehörden verbindlich.

Die TR-02102 hat erheblichen Einfluss auf Zulassungs- und Zertifizierungsverfahren. Für Zulassungen liefert die TR-02102 dem Hersteller eine Richtschnur, etwa zur Parametrisierung von kryptografischen Verfahren. Dies ersetzt aber nicht eine Gesamtwürdigung des Produkts durch Experten im Rahmen des Zulassungsverfahrens. Bei Zertifizierungsverfahren nach den Common Criteria im deutschen Zertifizierungsschema wird kryptografischen Algorithmen und Mechanismen ein Sicherheitsniveau von mindestens 100 Bit zugebilligt (üblicherweise im Zertifizierungsreport), wenn sie den Empfehlungen der TR-02102 folgen.

Eine indirekte Wirkung ergibt sich auch daraus, dass weitere Technische Richtlinien des BSI die TR-02102 referenzieren und selbst in ihrem Anwendungsbereich verbindlich sein können. Dies gilt beispielsweise für die TR-03116, die in vier Teilen verbindliche Vorgaben für die Verwendung kryptografischer Mechanismen in Projekten der Bundesregierung definiert. Für die Bewertung der Sicherheit kryptografischer Verfahren stützt sich die TR-03116 auf die TR-02102.

SICHERHEITSZIELE UND INHALT DER TR

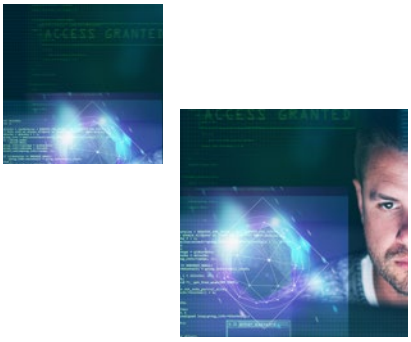
Grundsätzlich wird in der TR-02102-1 ein Sicherheitsniveau von 100 Bit angestrebt. Ab 2023 sollen es 120 Bit sein. Das bedeutet, dass kein bekannter Angriff auf empfohlene Verfahren existieren darf, dessen Aufwand geringer ist als der (klassische) Brute-Force-Angriff auf eine idealisierte Blockchiffre mit der entsprechenden Schlüssellänge. Die empfohlenen kryptografischen Verfahren und die Wahl der Sicherheitsparameter entsprechen diesem Ziel.

In den folgenden Teilen der TR-02102 werden, aufbauend auf den Empfehlungen der TR-02102-1, Vorgaben abgeleitet, wie spezifische kryptografische Protokolle sicher verwendet werden können. Hierbei geht es vor allem darum, die richtigen Schlüssellängen und sonstigen Sicherheitsparameter der implementierten Protokolle sowie sichere Ciphersuiten zu wählen und spezifische Attacken gegen die Protokolle zu verhindern. Grundsätzlich soll zudem verhindert werden, dass isolierte Kompromittierungen eines Systems die Sicherheit der vermittelten Verbindungen langfristig schwächen. Dies wird erreicht, indem konsequent die Nutzung von Ciphersuiten mit Perfect Forward Secrecy empfohlen wird, solange nicht zwingende Gründe für die Nutzung einer Konfiguration ohne diese Eigenschaft sprechen.

ANWENDUNGSMÖGLICHKEITEN

Die Empfehlungen der TR-02102-1 sind in erster Linie als Hilfestellung für Entwickler gedacht, um sichere kryptografische Verfahren auswählen zu können. Soll beispielsweise eine Software eine Funktion zum Erstellen einer elektronischen Signatur erhalten, so kann die TR-02102-1 eine Übersicht über die zurzeit als sicher betrachteten Verfahren geben. Daraus können nun ein konkretes Verfahren und geeignete Sicherheitsparameter, also etwa Schlüssellängen, ausgewählt werden.

Die Teile 2 bis 4 richten sich hingegen eher an Administratoren, die kryptografische Protokolle einsetzen und dazu Software installieren, konfigurieren und betreiben wollen. Ein Beispiel für ein solches Anwendungsszenario ist die Konfiguration eines Webservers für die Nutzung von TLS. Der Administrator kann hierbei eine Vielzahl von Einstellungen vornehmen, die die Sicherheit seiner Nutzer und seiner Seite teils wesentlich beeinflussen können. Die TR-02102-2 listet hierfür konkrete Ciphersuiten und Schlüssellängen auf, gibt aber auch Hinweise zu anderen sicherheitsrelevanten The-



men, etwa zur Wahl von geeigneten Zufallsgeneratoren und bestimmten Attacken.

Grundsätzlich enthält die TR-02102 keine Aussagen zu bestimmten Implementierungen. Dennoch kann natürlich die Kompatibilität von Implementierungen zur TR-02102 geprüft werden. Im Rahmen einer durch das BSI beauftragten Sicherheitsanalyse der OpenSSL-Bibliothek wurden etwa verschiedene Sicherheitsaspekte von OpenSSL auch unter dem Blickwinkel einer TR-Konformität untersucht.

FAZIT

Die kryptografischen Technischen Richtlinien des BSI können dem Nutzer eine grundsätzliche Orientierung geben, um sichere kryptografische Verfahren auszuwählen und kryptografische Lösungen zu konfigurieren. Ihre Ausrichtung hat sich dabei seit ihrer Einführung von einer reinen Orientierung auf Entwickler in Richtung der Bedürfnisse von Administratoren (Konfiguration von Anwendungen) erweitert.

Eine Beachtung der TR kann gleichwohl die Beteiligung von Experten an der Entwicklung oder auch dem Ausrollprozess eines kryptografischen Systems nicht ersetzen. Die Sicherheit eines kryptografischen Gesamtsystems wird von vielen Faktoren beeinflusst, die nicht in den eingesetzten Algorithmen liegen. Zudem können die Sicherheitsziele und Einsatzbedingungen eines bestimmten Systems dazu führen, dass selbst bei Verwendung für sich genommen kryptografisch sicherer Komponenten doch noch Sicherheitslücken etwa auf Protokollebene entstehen.

Eine konsequente Berücksichtigung der TR-02102 durch die Entwickler oder Konfiguratoren eines kryptografischen Systems kann aber die Aufgabe eines Experten sehr erleichtern, weil zumindest die Sicherheit der Grundbausteine und der verwendeten grundlegenden Sicherheitsparameter dann leicht eingeschätzt werden kann. ■

Weitere Informationen:

TR02102, Kryptografische Verfahren: Empfehlungen und Schlüssellängen: https://www.bsi.bund.de/TR

Sicherheitsanalyse der OpenSSL-Bibliothek: https://www.bsi.bund.de/DE/Publikationen/Studien/OpenSSL-Bibliothek/openssl-bibliothek.html

Anlaufstelle und Austauschplattform

von Frauke Greven und Till Kleinert, Referat Cyber-Sicherheit für die Wirtschaft

Allianz für Cyber-Sicherheit

Allianz für Cyber-Sicherheit richtet sich verstärkt an Handwerksbetriebe

Seit 2012 bietet die Allianz für Cyber-Sicherheit großen und kleinen Unternehmen umfangreiches Know-how und Dialogmöglichkeiten zu allen Fragen und Problemen der IT-Sicherheit im digitalen Zeitalter an. 2018 richtet sie ein zusätzliches Augenmerk auf die Handwerksbetriebe in Deutschland.

März 2012: Anlässlich der CeBIT haben der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur gemeinsamen Pressekonferenz in das Convention Center des Messegeländes geladen. Die Allianz für Cyber-Sicherheit ist geboren. Unter Federführung des BSI wird ein Informationsangebot geschaffen, das sich insbesondere an kleine und mittelständische Unternehmen richtet und praktische Hilfe zum Schutz vor Cyber-Angriffen sowie zur Reaktion darauf bietet. Die Inhalte stammen dabei nicht nur vom BSI selbst. Experten aus der Wirtschaft sind herzlich dazu eingeladen, sich als Partner der Allianz für Cyber-Sicherheit zu engagieren und eigene Inhalte bereitzustellen.

Die Teilnehmer der Initiative können so mithilfe der vorgeschlagenen Maßnahmen das eigene Sicherheitsniveau erhöhen. Im Gegenzug liefern sie Erfahrungswerte aus der betrieblichen Praxis sowie Meldungen über tatsächlich beobachtete Vorfälle. Es entsteht eine Zusammenarbeit in Form von Public Private Partnership, von der alle Beteiligten profitieren.

ÜBER 2.600 MITGLIEDER HEUTE

Inzwischen gehören über 2.600 Unternehmen und Institutionen der Allianz für Cyber-Sicherheit an. Täglich neue Anmeldungen zeigen, dass die Idee einer Anlaufstelle für Cyber-Sicherheitsfragen den Puls der Zeit getroffen hat. Neben Informationen auf der Plattform www.allianz-fuer-cybersicherheit.de bieten die Partner der Allianz Seminare und Workshops zu unterschiedlichen Themen an verschiedenen Standorten an. Die Cyber-Sicherheits-Tage der Allianz für Cyber-Sicherheit wurden zunächst quartalsweise, inzwischen im Abstand von zwei Monaten, in ganz Deutschland organisiert. Dabei steht jede Veranstaltung unter einem aktuellen Leitthema der IT-Sicherheit.

DER BLICK NACH VORN GEHT RICHTUNG HANDWERK

Die Digitalisierung ist seit der Gründung der Allianz für Cyber-Sicherheit immer weiter vorangeschritten. Nicht nur in weltweit agierenden Konzernen werden Standorte, Prozesse und Maschinen miteinander vernetzt, auch in teils jahrhundertealten, ursprünglich gänzlich analogen Produktionen und Abläufen haben Computer und programmierbare Steuerungskomponenten längst Einzug erhalten.

Aus diesem Grund wendet sich die Allianz für Cyber-Sicherheit im Jahr 2018 an die zahlreichen Handwerksbetriebe in der Bundesrepublik. Diese stehen nicht nur vor den für die heutige Arbeitswelt fast schon normalen Herausforderungen, wie zum Beispiel dem Gang in die Cloud oder dem Umgang mit mobilen Endgeräten. Zusätzlich müssen sich die Verantwortlichen auch mit Schutzmaßnahmen für computergestützte Spezialmaschinen in den Bereichen wie Produktion und Bau beschäftigen. Die Erfahrungen aus vielfältigen Arbeiten, Konstruktionsplänen oder den Daten von Kunden und Lieferanten machen Handwerksbetriebe zu attraktiven Zielen für Cyber-Angriffe.

Bereits Ende 2017 haben sich der Zentralverband des Deutschen Handwerks (ZDH) und das BSI auf eine verstärkte Zusammenarbeit verständigt. Der 20. Cyber-Sicherheits-Tag am 25. Januar 2018 war dann die erste Veranstaltung, die sich ganz gezielt an die zahlreichen Handwerksbetriebe richtete: Im Rahmen von verschiedenen Vorträgen konnten sich die Teilnehmer über die aktuellen Cyber-Bedrohungen und Schutzmaßnahmen informieren.

Zentrale Bausteine im Kampf gegen Cyber-Angriffe bietet beispielsweise der modernisierte IT-Grundschutz des BSI. Hier werden in den kommenden Monaten sogenannte IT-Grundschutz-Profile erarbeitet, die von den einzelnen Betrieben als Blaupause für die Umsetzung von Sicherheitsmaßnahmen genutzt werden können. Im Laufe des Jahres sind weitere Angebote geplant. Hierzu zählen Informationskampagnen, branchenspezifische Veranstaltungen und Multiplikatoren-Schulungen. Ziel ist es, in den Betrieben das Know-how zu IT- und Datensicherheit zu stärken und wertvolle, praxisnahe Hinweise zu Prävention und Abwehr von Cyber-Angriffen an die Hand zu geben. ■

„Die mehr als eine Million Handwerksbetriebe sind ein bedeutender Faktor für den Wirtschaftsstandort Deutschland. Auch im Handwerk ist die Digitalisierung auf dem Vormarsch, etwa bei der Projektplanung, bei der Steuerung früher manuell bedienter Werkzeuge oder in Verwaltungsabläufen. Aufgrund der zunehmenden Vernetzung sehen sich auch die Handwerksbetriebe mit Hackerangriffen, Schadsoftware, Phishing und anderen Cyber-Risiken konfrontiert, die zu Datenverlust, Produktionsausfällen und finanziellen Schäden führen können. Als nationale Cyber-Sicherheitsbehörde arbeitet das BSI Hand in Hand mit dem ZDH und unterstützt das Handwerk dabei, die Herausforderungen der Digitalisierung zu meistern.“

Arne Schönbohm, Präsident des BSI

Weitere Informationen: https://www.allianz-fuer-cybersicherheit.de

SONDERTHEMA

Industrie 4.0 – Security by Design

von Arne Schönbohm, Präsident des BSI

Die Weltwirtschaft wächst weiter zusammen. Vorangetrieben wird der Globalisierungsprozess der Märkte in erster Linie durch neue Technologien in den Bereichen Kommunikation, Information und Transport. Weltweite Datennetze, Satellitenkommunikation, computergestützte Logistik und fortschrittlichste Verkehrsmittel ermöglichen es Unternehmen, die für sie günstigsten Produktions- und Lieferstandorte auszuwählen. Die größten Marktpotenziale liegen aber nicht in der Standortwahl, sondern in der Steigerung der Effizienz der Produktionsabläufe durch den Einsatz intelligent vernetzter Systeme.

Bereits heute werden zum automatisierten Regeln, Steuern und Messen industrielle Steuerungssysteme verwendet. Der Anwenderkreis reicht vom produzierenden Gewerbe über die chemische Industrie bis hin zu kritischen Infrastrukturen; er umfasst kleine und mittelständische Betriebe ebenso wie Großunternehmen und internationale Konzerne.

Für viele dieser Unternehmen wird es immer wichtiger, Informationen möglichst schnell und direkt innerhalb des Unternehmens, mit anderen Niederlassungen oder Tochtergesellschaften im Ausland, mit Zulieferern oder Kunden auszutauschen. Dafür werden bisher physikalisch voneinander getrennte Bereiche über das Internet miteinander vernetzt – und damit angreifbar. Datenströme sind die Kapitalströme des digitalisierten Wirtschaftens. Werden sie gestört, stehen möglicherweise „alle Räder still".

Umso wichtiger ist es darum, ein nachhaltiges Sicherheitsbewusstsein in der Wirtschaft zu schaffen und damit eine solide Grundlage für die Digitalisierung zu legen. Nur wenn Cyber-Sicherheit schon im Design berücksichtigt wird, können Unternehmen erfolgreich an der Digitalisierung teilhaben und Schaden von Beginn an abwenden.

Wie besonders schützenswert dabei gerade industrielle Steuerungssysteme sind und was Angriffe auf diese Strukturen für Folgen haben können, haben die letzten Jahre mehr als einmal gezeigt. So waren im Dezember 2015 mindestens 225.000 Personen in der Ukraine von einem mehrstündigen Ausfall der Stromversorgung betroffen, der durch einen gezielten Cyber-Angriff verursacht wurde. Im Dezember 2016 gab es einen erneuten Stromausfall in Kiew, der Hauptstadt der Ukraine. Auch hierbei soll es sich, laut Aussage des geschäftsführenden Direktors des staatlichen Energieversorgers, um einen gezielten Cyber-Angriff gehandelt haben. Zwischen 100.000 und 200.000 Einwohner wurden für über eine Stunde nicht mehr mit Strom versorgt. Ein weiteres Beispiel sind die massiven Beeinträchtigungen des dänischen Logistikunternehmens Maersk und verschiedener Produktionsunternehmen durch die Ransomware „WannaCry". Allein bei Maersk wird der Schaden auf ca. 300 Millionen Dollar geschätzt.

Eine digitalisierte Gesellschaft kann nur mit einer durchgängig den Risiken angemessenen Informations-

„Nur wenn Cyber-Sicherheit schon im Design berücksichtigt wird, können Unternehmen erfolgreich an der Digitalisierung teilhaben und Schaden von Beginn an abwenden.“ Arne Schönbohm, Präsident des BSI

und Cyber-Sicherheit nachhaltig funktionsfähig sein. Diese Sicherheit entsteht einmal aus der engen und vertrauensvollen Zusammenarbeit aller Akteure, zum anderen aus dem richtigen Zusammenspiel von technischen und organisatorischen Maßnahmen, die sich gegenseitig von Anfang an ergänzen. Das BSI als die nationale Cyber-Sicherheitsbehörde hat sich darum einmal das Ziel gesetzt, bewährte deutsche und europäische IT- und Sicherheitsstandards zu stärken und zu erhalten. Mit dem BSI IT-Grundschutz als national und international anerkanntes Informationsmanagementsystem und seinem Kompendium existiert ein umfangreiches Arbeitsinstrument und Nachschlagewerk zur Informationssicherheit. Es benennt auch die Anforderungen, um industrielle Steuerungssysteme abzusichern. Das BSI forciert zum anderen die konsequente Anwendung des Konzepts „Security by Design“. Es legt die Basis für sichere Produkte und Technik und schafft somit ein einheitliches transparentes Sicherheitsniveau. Allerdings muss die Umsetzung überprüfbar und nachweisbar sein, beispielsweise durch Zertifizierungen.

Und das BSI beteiligt sich schließlich an nationalen und internationalen Initiativen wie der Plattform Industrie 4.0, um von Beginn an eine sichere Konzeption zu unterstützen. Mit der Allianz für Cyber-Sicherheit und den umfangreichen Informations- und Sensibilisierungsangeboten, wie den Expertenkreisen oder den Cyber-Sicherheitstagen leistet es seinen Beitrag, um die Herausforderungen der Digitalisierung zu meistern und den Erfolg des Wirtschaftsstandorts Deutschland zu sichern. ■

Gemeinsame Verantwortung

von Jens Mehrfeld, Referat Cyber-Sicherheit in Industrieanlagen

Klare Kommunikation von Sicherheitsanforderungen

In Zeiten von Industrie 4.0 ist Cyber-Sicherheit ein wesentliches Kriterium für die Verfügbarkeit von Anlagen und Maschinen. Die steigende Anzahl von Cyber-Angriffen auf Produktionsanlagen verdeutlicht die Notwendigkeit zu handeln, aber häufig fühlt sich niemand so richtig verantwortlich. Um dieser Zwickmühle zu entgehen, sind Eigenverantwortung und eine klare Kommunikation von Anforderungen und Einsatzvorgaben erforderlich.

Auf dem Weg von der Konzeption bis hin zum Betrieb industrieller Anlagen oder Maschinen sind eine Vielzahl unterschiedlicher Unternehmen beteiligt. Dies beginnt bei den Herstellern einzelner Komponenten wie z. B. speicherprogrammierbarer Steuerungen oder Sensoren. Maschinenbauer und Integratoren setzen diese zu Maschinen und Produktionsanlagen zusammen. Diese stehen bei einem Betreiber, der sie nutzt und betreut. Im Zuge von Industrie 4.0 kommen noch weitere Beteiligte, beispielsweise Predicitive Maintenance oder Cloud-Dienste, hinzu. Und jeder dieser Beteiligten hat dabei seine spezifischen Interessen:

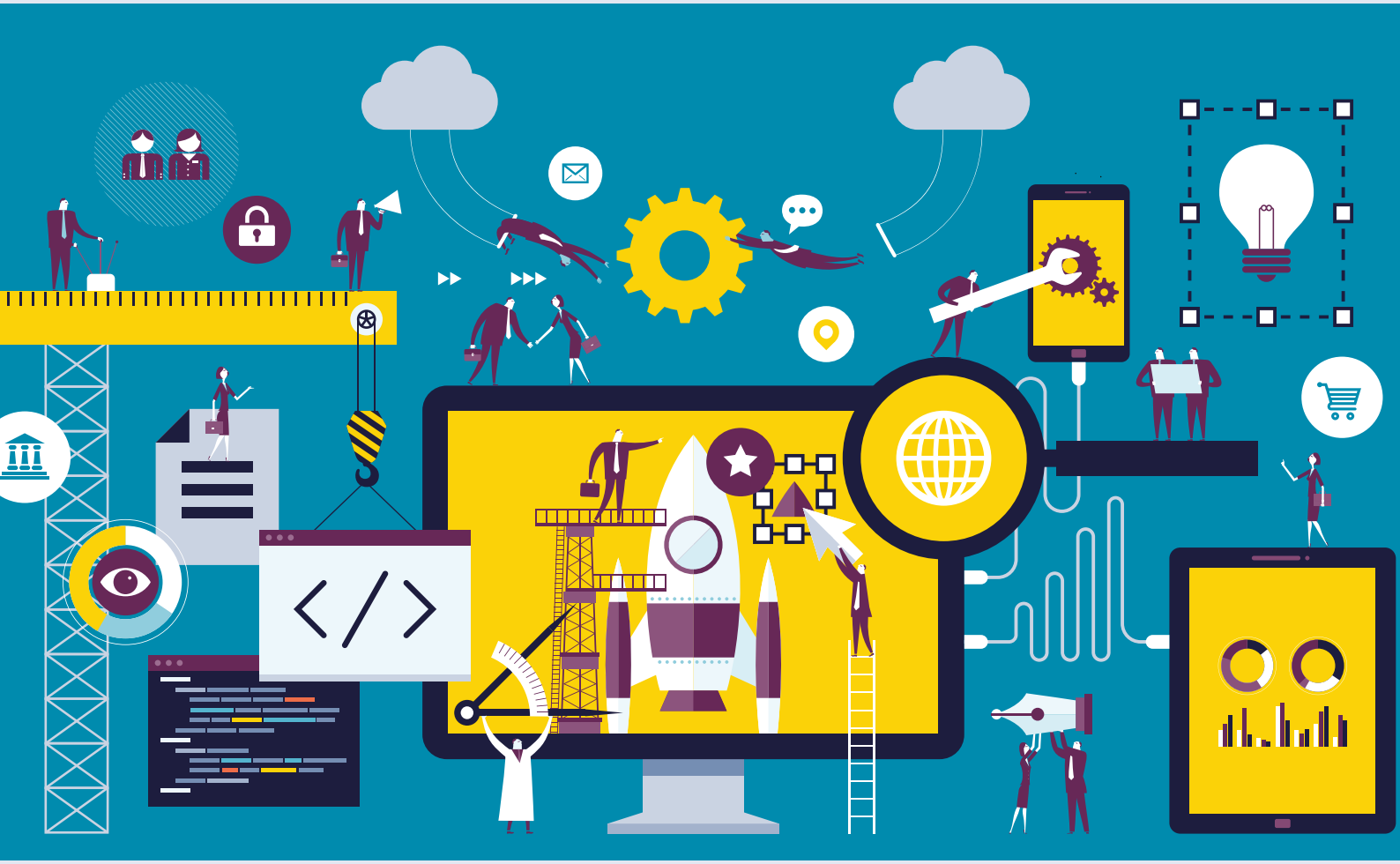
- Betreiber wollen eine kostengünstige, flexible Anlage kaufen, mit einer hohen Lebensdauer, geringen Stillstandzeiten, die generell wenig Aufwand während des Betriebs verursacht.
- Integratoren möchten Anlagen schnell und mit geringem Aufwand planen, programmieren, in Betrieb nehmen und warten. Dazu werden nur die Anforderungen der Betreiber berücksichtigt.
- Hersteller bieten Komponenten mit vielen Funktionen an, um eine breite Verwendbarkeit zu ermöglichen.

Gemeinsam ist allen Beteiligten, dass mit wenig Aufwand an Zeit und Geld ein Maximum erreicht werden soll. Der Fokus liegt dabei auf der eigentlichen Funktionalität der Komponente oder Anlage.

DAS DILEMMA DER CYBER-SICHERHEIT

Cyber-Sicherheit wird dabei oft als lästiger oder unnützer Zusatzaufwand betrachtet und in der Folge vernachlässigt. Hersteller kümmern sich nicht um Schwachstellen in ihren Komponenten, Integratoren nutzen Security-Funktionen nicht und Betreiber, machen sich keine Gedanken über Schutzmaßnahmen. Damit ist die Grundlage für Angriffe auf die Sicherheit der Anlage geschaffen.

Cyber-Sicherheit ist mehr als nur der Schutz der Vertraulichkeit und Integrität von Informationen. Es geht auch um die Verfügbarkeit und Integrität von Systemen bzw. Komponenten und damit die Verfügbarkeit von Anlagen und Maschinen. Das kann dramatische Folgen haben. Denn bei einer Manipulation oder Störung einer Komponente steht die Produktion oder wird negativ beeinflusst. Dies widerspricht dem Interesse des Betreibers. Wenn er mit der Anlage unzufrieden ist, sucht er sich für den Auftrag vermutlich einen anderen Integrator. Gleiches gilt für die Auswahl der Komponenten. Auch hier wird er nach anderen Möglichkeiten



suchen, was der Interessenslage des Herstellers zuwiderläuft. Darum sollten alle Beteiligten eine weitere Gemeinsamkeit entwickeln und pflegen: die Cyber-Sicherheit.

GEMEINSAME AUFGABE

Das Bewusstsein um die Verantwortlichkeit steigt – insbesondere im Bereich der kritischen Infrastrukturen. Der Grund ist das IT-Sicherheitsgesetz mit seinen Pflichten, ein Informationssicherheitsmanagement aufzubauen und Vorfälle zu melden. Zu den Aufgaben zählen Risikomanagement und die gezielte Umsetzung von Schutzmaßnahmen. Auch Hersteller und Integratoren sollten ein ISMS implementieren, um ihre Infrastruktur und damit unter anderem ihre Entwicklungs- und Kundendaten zu schützen. Hersteller und Integratoren müssen zusätzlich bei der Entwicklung Wert auf Cyber-Sicherheit legen. Dies betrifft sowohl die Entwicklung als auch das Design. Bei der Programmierung der Software gilt es, möglichst frühzeitig Fehler zu vermeiden und zu erkennen. Dies kann über Vorgaben für die Entwickler und begleitende Tests erreicht werden. Dies verursacht im ersten Schritt Kosten bzw. verlangsamt die Entwicklung zu einem gewissen Teil, zahlt sich auf lange Sicht aber aus. Denn mögliche Fehler werden vielfach früher erkannt und können deswegen kostengünstiger behoben werden. Wenn der Entwickler vor dem Release einen Fehler findet, ist dieser schneller behoben, als wenn er nach der Veröffentlichung gefunden wird. Dann muss die neue Version erneut komplett durch den Freigabe- und Qualitätssicherungsprozess. Auf lange Sicht können mit Maßnahmen zur Cyber-Sicherheit also Kosten reduziert werden.

OFFENE KOMMUNIKATION

Ähnlich verhält es sich mit der offenen Kommunikation von Anforderungen und Einsatzvorgaben. Anforderungen werden von Betreibern an Integratoren bzw. von Integratoren an Hersteller gestellt. Sie sollten neben den fachlichen Wünschen auch Anforderungen bezüglich der Cyber-Sicherheit enthalten. Dazu wird beschrieben, welche Schutzmaßnahmen bereits in der Anlage ergriffen werden. Die Anforderungen werden im Rahmen des ISMS ermittelt. Vonseiten der Hersteller können auch Einsatzvorgaben an die Integratoren bzw. von den Integratoren an die Betreiber gemacht werden. Darin sind Handlungsanweisungen enthalten, unter welchen Bedingungen ein sicherer Betrieb gewährleistet ist. Diese müssen im ISMS beim Betreiber berücksichtigt werden. So kann sich ggf. eine höhere Investition bei der Beschaffung einer Anlage schnell in erhöhter Cyber-Sicherheit auszahlen, da ein geringerer Aufwand während des Betriebs notwendig ist und die Verfügbarkeit der Anlage nicht durch Angriffe reduziert wird. ■

Cyber-Gefahren für Industrieanlagen

von Andreas Erdrich und Jens Kluge, Referat Cyber-Sicherheit in Industrieanlagen

Mit Security by Design eine höhere Resilienz gegen Angriffe

Cyber-Angriffe auf Industriesteuerungen (Industrial Control Systems, ICS) ähneln häufig den bekannten Angriffen auf IT Systeme, können jedoch im Gegensatz dazu physische Auswirkungen haben. Schlimmstenfalls kommt es zum Produktionsausfall lebensnotwendiger Güter, zur Gefährdung von Mensch und Umwelt oder zur Beeinträchtigung Kritischer Infrastrukturen. Daher sind die potenziell betroffenen Systeme besonders zu schützen. Durch „Security by Design“ muss eine Grundimmunität gegen Cyber-Angriffe im sich immer mehr vernetzenden Umfeld geschaffen werden.

DIE IT ALS ANGRIFFSZIEL – MIT AUSWIRKUNGEN AUF MASCHINEN UND ANLAGEN

Im Bereich der Operational Technology (OT) wird in vielen Systemen wie Industrial-PCs oder Human-Machine-Interfaces (HMI), aber auch auf Entwicklungs- und Projektierungsrechnern, Microsoft Windows als Betriebssystem eingesetzt. Für dieses Betriebssystem gibt es aufgrund seiner hohen Verbreitung eine Vielzahl an Schadsoftware. Aufgrund der hohen Verfügbarkeitsanforderungen werden auf diesen Systemen häufig – im Gegensatz zur IT in Büroumgebungen – Patches und Sicherheitsupdates gar nicht oder nur mit großer Verzögerung eingespielt. Darum ist die in der Abbildung gezeigte Malware Conficker, WannaCry, NotPetya und Copperfield langfristig ein großes Bedrohungspotenzial für diese Anlagen und Systeme.

Diese Schadsoftware-Varianten zielen zwar nicht direkt auf ICS, weshalb die Ausfälle als Kollateralschäden bezeichnet werden. Dennoch können die Auswirkungen auf industrielle Prozesse gravierend sein, wenn Komponenten wie HMIs ausfallen (Verlust der Anzeige) oder auf wichtige Prozessdaten nicht mehr zugegriffen werden kann (Verlust der Kontrolle). Durch WannaCry und NotPetya beispielsweise kam und kommt es bei Unternehmen und Anlagenbetreibern immer noch zu mehrwöchigen Betriebsstörungen oder -ausfällen, was für die Betroffenen mit Imageschäden und Umsatzeinbußen im Millionenbereich verbunden ist.

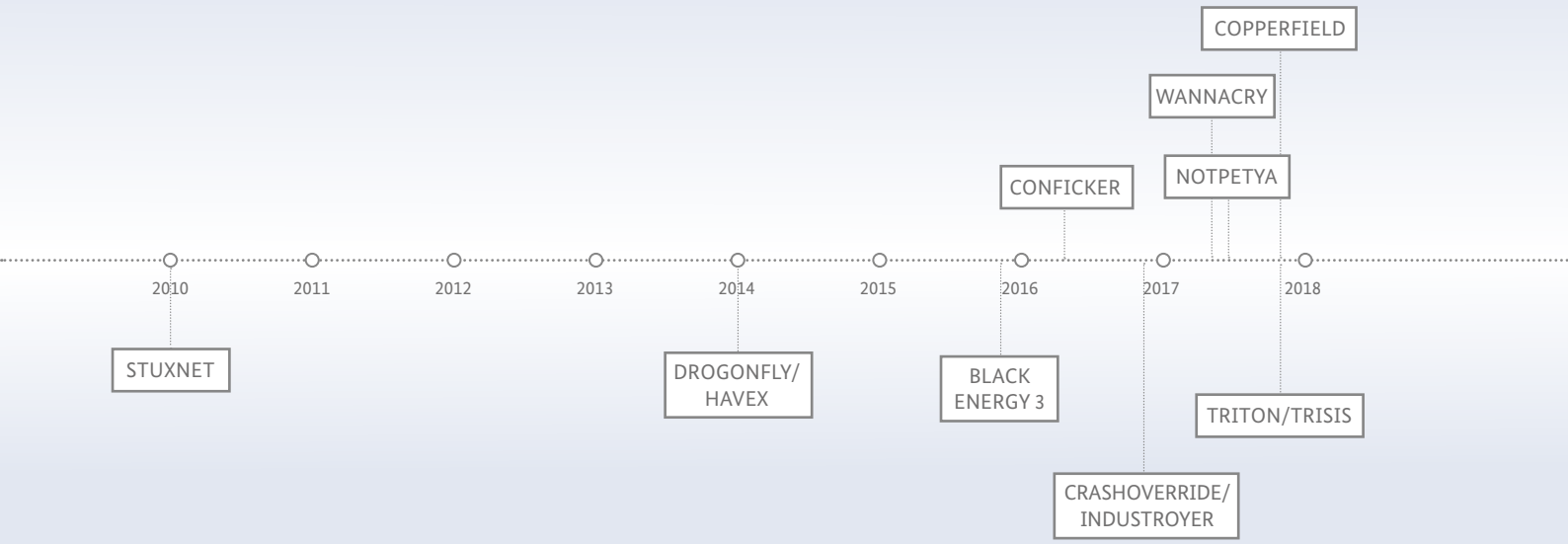
DIE SPITZE DES EISBERGS – GEZIELTE ANGRIFFE GEGEN ICS

Darüber hinaus gab es in den letzten Jahren eine Reihe an bekannt gewordenen Vorfällen, die sich dadurch auszeichneten, dass Schadsoftware gezielt gegen industrielle Prozesse eingesetzt wurde. Dazu waren nicht selten tief gehende Kenntnisse der Anlagenkonfiguration und oft erhebliche Ressourcen für die Vorbereitung und Durchführung erforderlich. Dies lässt kriminelle oder staatlich ausgerichtete Organisationen im Hintergrund vermuten.

- So hatte Stuxnet das Ziel, den Prozess der Urananreicherung einer Anlage im Iran zu sabotieren, indem die für dafür notwendigen Gasultrazentrifugen durch gezielte Veränderung der Drehzahl und der Prozessdrücke mechanisch beschädigt wurden. Die Prozessvisualisierung wurde dabei während der Attacke so weit verändert, dass ein zuvor aufgezeichneter Zeitabschnitt von mehreren Tagen eingespielt wurde. Bemerkenswert an Stuxnet war, dass die Malware eine spezielle Anlagenkonfiguration vorfinden musste, damit sie aktiv wurde. Als Konsequenz fand trotz weltweiter Ausbreitung des Schadcodes nur eine Manipulation in der iranischen Anlage statt. Der Einsatz mehrerer Zero-Day-Exploits spricht für einen hohen finanziellen Mitteleinsatz bei den Angreifern.

- Die Dragonfly-Kampagne sollte vertrauliche Daten aus ICS sammeln und exfiltrieren. Die dort eingesetzte

ZEITSTRAHL DER GEZIELTEN (OBEN) UND UNGEZIELTEN (UNTEN) ANGRIFFE AUF ICS



Schadsoftware Havex war ein Remote-Access-Trojaner, der über drei verschiedene Wege verbreitet wurde: Spear-Phishing-Mails, die die Malware enthielten, Watering-Hole-Attacken, die Besucher auf Webseiten mit Exploit-Kits weiterleiteten, und die Infizierung legitimer Software von drei verschiedenen ICS-Komponentenherstellern. Vom Havex-Trojaner wurden mehr als 50 Varianten gefunden und es gab mindestens 2500 Betroffene. Die Schadsoftware hat u. a. Netzwerke auf Ports von ICS-spezifischen Protokollen gescannt und nach OPC-Servern gesucht. Zusätzlich wurden VPN-Konfigurationsdateien, im Browser gespeicherte Kennwörter, Adressbücher und Nutzer-/Systeminformationen exfiltriert.

- Black Energy 3 war ein Angriff auf die Stromversorgung in der Ukraine, wobei bis zu 700.000 Personen für mehrere Stunden ohne Strom waren. Betroffen waren drei Energieunternehmen, bei denen die Steuersysteme für die Umspannwerke bzw. Schaltanlagen im Abstand von je 30 Minuten koordiniert sabotiert wurden. Dies führte schließlich zum Black-out. Bemerkenswert war, dass die Malware vor dem Angriff fast acht Monate unentdeckt blieb und den Angreifern dadurch viel Zeit gegeben wurde, die Anlagen auszukundschaften und den Angriff weiterzuentwickeln.

- Ein Jahr später soll Industroyer/Crashoverride für einen erneuten kurzzeitigen Black-out in der Ukraine gesorgt haben, diesmal in der Region Kiew. Nach knapp einer Stunde konnte die Stromversorgung durch manuelle Eingriffe in den Schaltstationen wiederhergestellt werden. Spätere Analysen anhand Samples der Malware beschreiben einen modularen Aufbau und eine gezielte Ausrichtung des Schadcodes auf die in der Energieverteilung üblichen Fernwirkprotokolle mit dem Ziel, die Schalter zur Netztrennung in Mittel- und Hochspannungsanlagen über die entsprechenden Steuerungen auszulösen.

WAS KOMMT NOCH AUF UNS ZU?

Die gezielten Vorfälle stellen ungeachtet ihrer Raffinesse nur einen Bruchteil der durch Malware verursachten industriellen Schäden dar. Der größere Teil geht noch von den ungezielten Angriffen aus. Die hier aufgeführten gezielten Angriffe sind also nur die Spitze des Eisbergs.

Den Angreifern kommt dabei zu Gute, dass viele der in den Anlagen genutzten Systeme und Kommunikationsprotokolle bereits seit Jahrzehnten im Einsatz sind. Haben die Angreifer sich einmal Zugang zum OT-System verschafft, weist dieses kaum Schutzmöglichkeiten gegen den Angriff auf. Die fortschreitende Vernetzung der Anlagenkomponenten und die steigende Funktionalität bieten hierbei zusätzliche Angriffsvektoren, um den Zugang zu erlangen. Noch gravierender können die Auswirkungen sein, wenn durch einen Angriff nicht nur der eigentliche Prozess, sondern die funktionale Sicherheit der Anlage beeinträchtigt wird. Dann sind Mensch und Umwelt in Gefahr, wie im nachfolgenden Artikel genauer beschrieben wird. ■

Security for Safety

von Erwin Kruschitz, anapur AG, und Veselina Hensel, Referat Cyber-Sicherheit in Industrieanlagen

Kein Hype, sondern Notwendigkeit

Der 14. Dezember 2017 versprach ein ganz normaler Tag zu werden, bis die Berichte der IT-Sicherheitsdienstleister FireEye und Dragos über eine neue Malware veröffentlicht wurden. In einer digitalisierten Welt sind solche Berichte alltägliche Routine. Nicht aber, wenn industrielle Steuerungssysteme betroffen sind. Das Außergewöhnliche an dieser Malware: Zum ersten Mal wurde ein Safety Instrumented System (SIS) gezielt manipuliert, ein System, das Gefahr von Mensch, Umwelt und technischen Anlagen abwenden soll.

Unbekannten Tätern war es gelungen, ins Netz eines Unternehmens einzudringen und die Kontrolle über einen oder mehrere Entwicklungsrechner (Engineering Workstation) zu erlangen. Auf mindestens einem davon befand sich eine spezielle Software, die für die Programmierung und Parametrierung der eingesetzten SIS verwendet wird. Durch das Laden von Schadcode auf diese Maschine konnten die Täter im Netz gezielt nach einem SIS eines bestimmten Herstellers suchen, Verbindung zu diesem aufbauen und Schadcode einspielen, um die Programmlogik des SIS zu manipulieren. Die Analysen des Angriffs und des Schadcodes laufen noch. Bekannt ist bisweilen, dass die Täter teilweise erfolgreich Änderungen im laufenden Betrieb vorgenommen haben. Eins von den Systemen hat darauf bestimmungsgemäß reagiert, die Anlage in einen sicheren Zustand überführt und schwerwiegendere Auswirkungen verhindert.

SAFETY VS. SECURITY

Diskussionen zwischen IT-Sicherheitsexperten und Automatisierungsingenieuren leiden häufig an dem unterschiedlichen Verständnis darüber, wie das Risiko im jeweiligen Kontext definiert wird.

Im Zusammenhang mit Safety geht es darum, die Risiken, die von Maschinen und Industrieprozessen ausgehen und eine Gefahr für Mensch und Umwelt darstellen, auf ein tolerierbares Maß zu reduzieren. Mit der IT-Sicherheit rücken jedoch zusätzlich Vorsatz sowie gezieltes Handeln in den Mittelpunkt der Betrachtung.

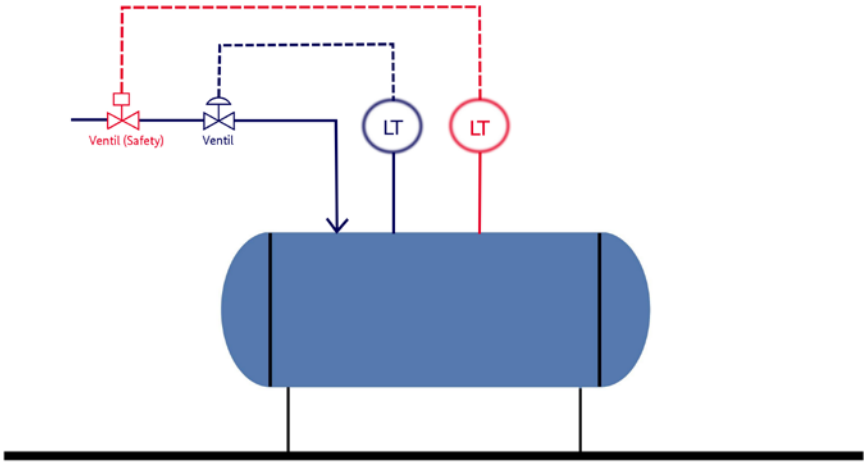
ÜBERLEGTES HANDELN IST GEFRAGT

Seitdem 2010 die Schadsoftware Stuxnet entdeckt wurde, ist Triton/Trisis/HatMan die fünfte zurzeit bekannte Malware, die speziell auf Industriesteuerungssysteme abzielt. Diese Zahl mag klein erscheinen, ist aber kein Grund, sich beruhigt zurückzulehnen. Einerseits sind Industrieanlagen in der Regel einmalig, andererseits ist das Safety Engineering eine Disziplin, die hoch spezialisiertes Wissen voraussetzt, sodass hoch entwickelte, gezielte Angriffe aufwendig und komplex sind. Aber sie sind möglich. Ebenfalls nicht zu

SIS UND SEINE AUFGABEN

Safety Systeme bilden eine Untergruppe der industriellen Steuerungssysteme und werden eingesetzt, um Gefahren für Mensch, Umwelt und technische Anlagen abzuwenden. Ein wesentlicher Unterschied zu konventionellen Automatisierungssystemen besteht in den erhöhten Anforderungen an die Zuverlässigkeit.

SIS (in Rot dargestellt) werden sowohl in Maschinen als auch in verfahrenstechnischen Anlagen eingesetzt. Sie funktionieren unabhängig von den Steuerungssystemen (in Blau dargestellt), die einen physikalischen Prozess oder eine Maschine regeln. Die Grafik zeigt, wie dem Risiko einer Überfüllung des Behälters durch die im SIS implementierte Sicherheitsfunktion (Safety Instrumented Function, SIF) begegnet wird: Solange der Betrieb reibungslos funktioniert, nimmt das SIS eine rein beobachtende Funktion ein. Treten jedoch Störungen oder Abweichungen von vordefinierten Kriterien ein, greift das SIS in den Prozess ein und versetzt die Maschine oder Anlage kontrolliert in einen sicheren Zustand. Im Beispiel wird das Ventil geschlossen, wenn der Füllstandsensor (LT) eine Überfüllung meldet.



vernachlässigen sind ungezielte Angriffe, wie beispielsweise Ransomware, die ein hohes Schadenspotenzial aufweisen.

Handeln ist gefragt, denn auch Safety kann nicht ohne IT-Sicherheit auskommen. Dieser Erkenntnis folgen bereits Standards wie IEC 61511. Auch das BSI beschäftigt sich seit mehreren Jahren mit der Thematik, beispielsweise durch aktive Mitarbeit bei der Erstellung des NAMUR-Arbeitsblattes NA 163. Es gibt auch im Rahmen des IT-Grundschutz des BSI einen Baustein, der die Betreiber bei der Analyse, Auswahl und Implementierung von Maßnahmen zur Absicherung der SISen unterstützt.

Die Herausforderungen an Hersteller und Betreiber sind groß, da klassische Sicherheitskonzepte und -empfehlungen nicht einfach übertragen werden können. Safety-Komponenten durchlaufen spezielle Validierungs- und Zertifizierungsprozesse, sodass Anlagenänderungen oder Produktneuerungen entsprechend selten sind. Die lange Lebensdauer der Maschinen und Anlagen ist ebenfalls ein Grund, warum Hersteller das mit der Vernetzung einhergehende Risiko aktiv in dem gesamten Lebenszyklus mit berücksichtigen und einfließen lassen müssen. Trotz alldem gilt: Der Schutz von Mensch, Umwelt und Anlage muss zuverlässig gewährleistet sein. Erst dann kann Digitalisierung erfolgreich werden. ■

Weiterführende Informationen, eine vereinfachte Risikoanalyse sowie Empfehlungen und Maßnahmen zur Absicherung von SIS für Betreiber:

NA 163 „IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen“ sowie die dazugehörige Checkliste: http://www.namur.net/de/publikationen/news-archiv/detail/article/na-163-ist-neu-erschienen.html

IT-Grundschutz-Kompendium des BSI, Baustein „Safety Instrumented Systems“: https://www.bsi.bund.de/IT-Grundschutz-Drafts

„Sichere Identitäten sind die Ausgangsbasis fast aller Geschäftsprozesse.“

Interview mit Michael Jochem,
Leiter der Arbeitsgruppe „Sicherheit vernetzter Systeme“

Wie will der Produktionsstandort Deutschland mit Industrie 4.0 seine Wettbewerbsfähigkeit weiter steigern? Welche Rolle spielt Deutschland bei der Setzung von Standards? Wie kann die Arbeitswelt mit Industrie 4.0 zum Nutzen der Menschen gestaltet werden? Mit diesen Fragen beschäftigt sich die Plattform Industrie 4.0. Eine Arbeitsgruppe hat sich des Themas IT-Sicherheit für die Industrie 4.0 angenommen. Das BSI-Magazin sprach mit Michael Jochem, Robert Bosch GmbH, Leiter der Arbeitsgruppe „Sicherheit vernetzter Systeme“.

Herr Jochem, welche Ziele verfolgt die Plattform Industrie 4.0?

Dort erarbeiten Unternehmen, Verbände, Politik, Wissenschaft und Gewerkschaften gemeinsam Konzepte sowie Handlungsempfehlungen, geben Orientierungshilfen für kleine und mittlere Unternehmen und prägen den internationalen Austausch – alles für einen erfolgreichen Übergang zur Industrie 4.0. Wir wollen dazu beitragen, dass Deutschland auch in Zukunft führend in der Fabrikausrüstung bleibt und seine Wettbewerbsfähigkeit weiter steigert. Relevante Trends und Entwicklungen im Bereich der produzierenden Industrie werden identifiziert und im Sinne eines einheitlichen Gesamtverständnisses von Industrie 4.0 zusammengeführt. IT-Sicherheit spielt dabei eine zentrale Rolle.

Warum?

Daten sind das Öl des 21. Jahrhunderts. Ihre Speicherung und Verarbeitung erzeugt Wertschöpfung. Aber im Gegensatz zu Öl sind Daten sehr volatil. Es muss sichergestellt sein, dass die gespeicherten und übertragenen Daten korrekt und vollständig sind. Dazu liefert die IT-Sicherheit Maßnahmenkataloge, z.B. zum Schutz vor unberechtigtem Zugriff, Veränderungen oder unerlaubtem Kopieren.

Eine entscheidende Rolle spielen dabei Organisation und Prozesse. Anders als im analogen Zeitalter erfordert Industrie 4.0 einen ganzheitlichen Ansatz, der die Office-IT, die Produktentwicklung und die Produktions-IT beinhaltet. Ein Informationssicherheitsmanagementsystem (ISMS) unterstützt das Management in der Umsetzung und dient dazu, das Unternehmensrisiko zu minimieren und regulatorische Anforderungen zu erfüllen. IT-Sicherheit trägt also wesentlich zum Geschäftserfolg bei.

Können Sie das Thema „Sichere Identitäten“ näher erläutern?

Gern. Wenn Unternehmensabläufe flexibilisiert werden, sind sichere Identitäten – allein schon aus rechtlichen Gründen – die notwendige Ausgangsbasis fast aller Geschäftsprozesse. Flexibilisierung wäre ohne Sichere Identitäten in der Industrie 4.0 de facto nicht zu leisten. Nur wer sich vertraut (Menschen und Maschinen), sollte miteinander kommunizieren.

Was heißt in diesem Zusammenhang Vertrauen?

Es meint, wie gut man sich auf seinen Geschäftspartner oder auch ein Produkt verlassen kann. Tut der Geschäftspartner oder das Produkt das, was er oder es soll? Vertrauenswürdigkeit im Produktkontext bedeutet, dass keine versteckten Funktionen enthalten sind und ein angemessener Schutz vor Fehlfunktionen und Angriffen gewährleistet ist. Bisher gibt es keine Kriterien oder Bewertungsskalen, um dies zu beurteilen oder automatisch für ein Produkt zu bestimmen. Zunehmend automatisierte Prozesse mit einer Ad-hoc-Vernetzung untereinander erfordern Methoden, mit denen die Vertrauenswürdigkeit der Beteiligten ermittelt und bewertet werden kann.

„Anders als im analogen Zeitalter erfordert Industrie 4.0 einen ganzheitlichen Ansatz, der Office-IT, Produktentwicklung und Produktions-IT beinhaltet.“

Kurzprofil Michael Jochem

Michael Jochem ist aktuell im Business Chief Digital Office Industry für IT Security Governance und Services zuständig. Er bringt mehr als 30 Jahre Erfahrung im Bereich Automationstechnik in unterschiedlichen Funktionen (Entwicklung, Produktmanagement, Vertrieb) bei Bosch Rexroth AG und Robert Bosch GmbH in die Arbeitsgruppe bei Plattform Industrie 4.0 ein.

Damit gewinnen doch Sichere Identitäten eine zentrale Bedeutung für den Gesamtprozess?

Richtig. Ein bekanntes Beispiel sind alle Arten des Fernzugriffs. Dies kann für die Zustandsüberwachung einer Maschine oder für Wartung und Service nötig sein. In allen Fällen muss sichergestellt werden, dass nur der berechtigte Servicetechniker oder die überwachenden Systeme Zugriff erhalten. Sichere Identitäten können auch zum Schutz vor Produktfälschungen beitragen, indem sie ermöglichen. die Herkunft und Authentizität einer Komponente zu validieren. Es gibt daher ein breites Spektrum an Einsatzgebieten. In der Publikation „Sichere Identitäten“ der Plattform Industrie 4.0 werden die Bedeutung sicherer Identitäten aufgezeigt, die wesentlichen Elemente für den vertrauensvollen Aufbau von Wertschöpfungsnetzwerken zusammengestellt und Handlungsempfehlungen abgeleitet. Denn gerade organisatorische Aufgaben wie Identitäten zu verwalten oder ein Informationssicherheitsmanagement zu implementieren stellen für viele Unternehmen eine Herausforderung dar.

Haben Sie sich hierzu auch schon Gedanken gemacht?

Ja, der Leitfaden „IT-Security in der Industrie 4.0 - Handlungsfelder für Betreiber“ beschreibt neben den technischen Schutzmaßnahmen insbesondere die organisatorischen Rahmenbedingungen einer digitalisierten Produktion. Mit der Umsetzung der beschriebenen Maßnahmen und praktischen Hinweise, beispielsweise zu möglichen Anforderungen beim Einkauf von Maschinen und Anlagen, können bekannte Risiken reduziert werden. Das schafft die Voraussetzungen, um als vertrauenswürdiger Partner in Wertschöpfungsnetzwerken mitwirken zu können.

Prozesse und Maßnahmen werden von Menschen umgesetzt. Wie stellen Sie das entsprechende Know-how bei den Mitarbeitern sicher?

Das ist in der Tat ein wichtiges Anliegen. Wir haben darum in der Arbeitsgruppe notwendige IT-Security-Kompetenzen in der Aus- und Weiterbildung identifiziert und in einer Publikation dargestellt. Dort werden Kompetenzen über alle Wertschöpfungspartner und Hierarchieebenen beschrieben und das Anforderungsprofil eines Industrial-Security-Officers als zentraler Ansprechpartner für die IT-Security in der Produktion herausgearbeitet.

Die Erkenntnisse der Publikation sind aktuell in die vom ZVEI-begleiteten Ausbildungsberufe der Elektroindustrie einbezogen worden. Sie sollen bis August 2018 umgesetzt werden. Damit werden bereits in der Ausbildung erste Grundlagen vermittelt.

Wie adressieren Sie denn bei Bosch, also in Ihrem Unternehmen, die IT-Sicherheit bei Industrie 4.0?

IT-Security muss von Anfang an mitgedacht werden. Der die Produktentwicklung begleitende „Bosch Security Engineering Prozess (SEP)“ beschreibt die notwendigen Aktivitäten im Kontext der IT-Security und des Datenschutzes und sorgt damit für „Security-by-Design“. Ein etabliertes Netzwerk sichert den Austausch von Daten in der Fertigung und zu anderen Organisationseinheiten. Und zukünftig wird eine standardisierte Fernwartungslösung für mehr als 100.000 vernetzte Maschinen und Anlagen dazu beitragen, die Servicetechniker sowohl intern als auch extern sicher anzubinden und die Angriffsfläche zu reduzieren. Denn angemessene IT-Security und ein hohes Maß an Datenschutz sehen wir als Bestandteil des Bosch-Qualitätsversprechens. ■

DAS BSI

Vorteil Diversität

BSI fördert Frauen in MINT-Berufen

Um qualifizierte Nachwuchskräfte bemühen sich öffentliche und private Arbeitgeber gleichermaßen – vor allem, wenn sie in den sogenannten MINT-Berufen ausgebildet wurden. Noch immer sind Mathematik, Informatik, Naturwissenschaften und Technik (MINT) in den Augen mancher „Männersache“. Damit das nicht so bleibt, hat sich das BSI dem „Nationalen Pakt für Frauen in MINT-Berufen" angeschlossen.

Knapp unter 15 Prozent: So niedrig war 2016 laut Statistischem Bundesamt der Anteil der weiblichen Erwerbstätigen in der IT- und IKT-Branche in Deutschland. Eine Zahl, mit der eigentlich niemand zufrieden sein kann – weder die Politik noch die Wirtschaft und genauso wenig das BSI als Arbeitgeber.

Die Ursachen dafür sind vielfältig, und doch sticht ein Grund immer wieder heraus: Stereotype. Als typische Männer-Domäne wird zum Beispiel oftmals die Informatik bezeichnet. Die genannten Zahlen scheinen dies auch zu bestätigen. Und doch gibt es immer wieder weibliche Vorbilder (siehe nebenstehende Interviews), die zeigen: Informationstechnik und Informationssicherheit sind auch Frauensache.

Das BSI möchte Schülerinnen, Studentinnen und auch bereits erwerbstätige Frauen ermutigen, sich beruflich für eine hochspannende Aufgabe zu begeistern: Ganz gleich ob Mathematik, Physik, Elektrotechnik, Informatik oder auch Politik- und Wirtschaftswissenschaft – viele Fachrichtungen tragen beim BSI gemeinsam zur sicheren Gestaltung der Digitalisierung bei. Eine große Aufgabe für engagierte Fachleute, egal welchen Geschlechts, deren Herz auf der digitalen Seite schlägt.

FRAUEN IM BSI

Auf das gesamte BSI betrachtet beträgt die Quote der weiblichen Beschäftigten aktuell circa 27 Prozent. Demgegenüber sind 35 Prozent der 2017 neu eingestellten Beschäftigten Frauen. Bei den neu besetzten Referatsleitungen betrug der Frauenanteil im zurückliegenden Jahr sogar 50 Prozent. Eine positive Tendenz ist also erkennbar und der Anteil der weiblichen Beschäftigten mag, verglichen mit dem Branchendurchschnitt, auch viel erscheinen – ausruhen will sich darauf beim BSI aber niemand.

komm mach MINT
NATIONALER PAKT FÜR FRAUEN IN MINT-BERUFEN

Um Frauen gezielter für die Aufgaben des BSI erreichen zu können, hat sich die nationale Cyber-Sicherheitsbehörde im Jahr 2016 dem „Nationalen Pakt für Frauen in MINT-Berufen“ angeschlossen. Dabei handelt es sich um eine Initiative des Bundesministeriums für Bildung und Forschung mit dem Motto „Komm, mach MINT“. Mittelfristig soll durch die Mitgliedschaft der Anteil an weiblichen Beschäftigten und Führungskräften im BSI gesteigert werden, unter anderem durch Maßnahmen wie ein gendersensibles Personalmarketing oder Kooperationen mit ortsansässigen Hochschulen zur Förderung des Frauenanteils in technischen Studiengängen. ■

Weitere Informationen: https://www.bsi.bund.de/karriere


Yona Raekow


Ayse Yenigün

VIER FRAGEN AN: YONA RAEKOW

Wie sind Sie ins BSI gekommen?
Ich bin 2012 auf das BSI aufmerksam geworden, habe mich dort beworben und arbeitete anschließend in den Bereichen „Kryptografie in Anwendungen“ sowie „Evaluierung von sicheren mobilen Lösungen“. Ich habe dann das hausinterne Führungskräfte-Nachwuchsprogramm durchlaufen und mich vor Kurzem erfolgreich für die Position als Referatsleiterin im Bereich „Zertifizierung von IT-Sicherheitsdienstleistungen" beworben.

Frauen gelten oftmals noch als „Exoten“ in der Informationstechnik. Was hat Sie damals begeistert, trotzdem diesen Weg einzuschlagen?
Als es um meine Studienwahl ging, wurde gerade der Studiengang Bioinformatik angeboten. Da dachte ich „Bio kann ich“ und „Informatik ist spannend und komplettes Neuland“. Ich war dann gar nicht so eine Exotin, da sich auch einige andere Frauen von der Bioinformatik angesprochen fühlten. Hinterher hat sich herausgestellt, dass mir Informatik viel leichter fällt als Biologie. Deshalb habe ich mein Studium in den USA mit einem Master of Computer Science and Engineering abgeschlossen.

Sie sind verheiratet, zweifache Mutter und haben nun eine Führungsfunktion im Bereich der Zertifizierung. Wie bringen Sie das alles in Einklang?
Mein Mann arbeitet ebenfalls im BSI, das hilft uns sehr bei der Koordination von Familie und Beruf. Insbesondere die flexiblen Arbeitszeiten und die Möglichkeit, Teilzeit zu arbeiten, ermöglichen es, Berufliches und Privates in Einklang zu bringen. Darüber hinaus habe ich die Erfahrung gemacht, dass die Kollegen und Vorgesetzten sehr verständnisvoll sind, wenn es zu Hause mal schwierig ist.

Was geben Sie Schülerinnen, Studentinnen und Berufseinsteigerinnen, die sich für die Informationstechnik interessieren, mit auf dem Weg?
Dass sie sich für ein spannendes und vielseitiges Berufsbild interessieren, von dem sie möglichst viel ausprobieren sollten. Denen, die sich (noch) nicht interessieren, möchte ich auch gerne etwas mitgeben: Schaut es euch einfach mal an, es macht wirklich Spaß und es ist kein Hexenwerk.

VIER FRAGEN AN: AYSE YENIGÜN

Wie sind Sie ins BSI gekommen?
Auf Umwegen. Ich habe zunächst eine Ausbildung als Arzthelferin absolviert und mich dann entschlossen, Informatik zu studieren. Über die Betreuung meiner Masterarbeit habe ich dann den Weg ins BSI gefunden und mich nach dem Studienabschluss beworben. Seit 2016 arbeite ich im Nationalen IT-Lagezentrum.

Von der Arztpraxis ins Nationale IT-Lagezentrum – wie kam es dazu?
Ein Wunschtraum von mir war es, Teil eines großen Ganzen zu sein und etwas Gutes zu tun. Aus diesen und weiteren Gründen kam ich zunächst zu einer Ausbildung als Arzthelferin. Computer waren meine ständigen Begleiter. Dabei hat sich mein ursprüngliches Interesse verwandelt. Mit dem Informatikstudium kam ich meinem Ziel näher, mit meinem Wissen etwas bewegen zu können. Nun zum „Happy End“ bin ich Teil eines großen Teams und kann meine Fähigkeiten für die nationale Cyber-Sicherheit einsetzen. Weiterhin habe ich die Möglichkeit, im Rahmen eines spannenden Jobs und in einem tollen Umfeld mein Wissen jeden Tag zu erweitern.

Nach dem Abschluss des Studiums stehen Studierenden der Informatik derzeit viele Türen offen – was hat Sie für das BSI begeistert?
Für mich war die IT-Sicherheit das interessanteste unter all den Themengebieten. Es ist mir auch wichtig, da zu arbeiten, wo es spannend und abwechslungsreich ist. Weiterhin sollte dort, wo ich arbeite, kein Konkurrenzkampf herrschen, sondern ein Teamgefühl, sodass alle an einem Strang ziehen und für dasselbe Ziel arbeiten. Ich persönlich entwickle mich zusammen mit der IT-Sicherheit weiter und wo wäre ich da besser aufgehoben als beim BSI?

Das Informatikstudium gilt als sehr anspruchsvoll – welchen Tipp haben Sie für Studienanfängerinnen und Schülerinnen, damit sie dieses erfolgreich bewältigen?
Learning by doing. Alles Theoretische ausprobieren und keine Quantensprünge herbeiwünschen. Informatik funktioniert am besten, indem man sie anwendet und Schritt für Schritt erlernt. Dadurch ergibt sich eine höhere Anzahl an Erfolgserlebnissen für die Motivation und das Erlernte bleibt einem ein Leben lang erhalten.

Zusammenarbeit mit den Ländern wird ausgebaut

von Stefanie Euler, Referat Informationssicherheitsberatung für Behörden und Fabienne Middeke, Referatsleiterin Nationales Verbindungswesen

Einheitliches IT-Sicherheitsniveau schaffen

Durch die Sicherheitsberatung und das Verbindungswesen baut das BSI die Zusammenarbeit mit den Bundesländern kontinuierlich aus. Übergeordnetes Ziel ist dabei, ein einheitliches IT-Sicherheitsniveau zu schaffen. Angesichts der fortschreitenden Digitalisierung der Verwaltung und einer zunehmenden Vernetzung von IT-Strukturen zwischen Bund und Ländern gewinnt dies immer mehr an Bedeutung. Mit Rheinland-Pfalz und Hessen wurden im letzten Jahr erste Absichtserklärungen unterzeichnet, mit Nordrhein-Westfalen in diesem Jahr.

Das BSI als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Um diesen gesamtstaatlichen Ansatz umfassend verfolgen zu können, wurde in der Cyber-Sicherheitsstrategie für Deutschland 2016 festgelegt, die Bund-Länder-Zusammenarbeit zu stärken. Die rechtliche Grundlage dafür bildet der § 3 BSIG. Danach kann das BSI die Länder in Fragen der Informationssicherheit beraten und warnen sowie auf deren Ersuchen bei der Sicherung ihrer Informationstechnik und Abwehr von Gefahren unterstützen.

> Die Zusammenarbeit zwischen den Bundesländern und dem BSI wird auch durch das Gesetz zur Umsetzung der EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-RL) gestärkt. Gemäß § 3 Abs. 1 S. 2 Nr. 13a BSIG kann das BSI nunmehr zuständige Stellen der Länder auf deren Ersuchen bei der Abwehr von Gefahren für die Sicherheit in der Informationstechnik unterstützen und technische Expertise zur Verfügung stellen. Das BSI ist damit die Bundesbehörde, die die Länder bei der Gefahrenabwehr im Bereich der Cyber-Sicherheit unterstützt.
>
> Auch um regionale Konzepte zum Schutz der Wirtschaft zu erarbeiten, können die Länder mit dem BSI zusammenarbeiten.

DIE STRUKTUREN DER ZUSAMMENARBEIT

Im BSI bestehen auf beratender, strategischer und operativer Ebene folgende Strukturen, um die Bund-Länder-Zusammenarbeit im Bereich der IT-Sicherheit zu gestalten:

Die Sicherheitsberatung des BSI ist die zentrale Anlaufstelle für Beratungsanfragen aus den Bundes- und Landesverwaltungen im Kontext des Informationssicherheitsmanagements (ISMS). Sie ist der zentrale Point-of-Contact für die Informationssicherheitsbeauftragten der jeweiligen Behörden und erhält durch Gremienarbeiten, enge Behördenkontakte und einen effizienten Austausch von IT-sicher-

Seit September 2017 unterzeichnete BSI-Präsident Arne Schönbohm Absichtserklärungen mit Rheinland-Pfalz (Staatssekretär Randolf Stich, oben links), Hessen (Staatsminister Peter Beuth, unten links) und Nordrhein-Westfalen (Wirtschafts- und Digitalminister Prof. Dr. Andreas Pinkwart, oben rechts).

heitsrelevanten Informationen einen guten Einblick in die Lage der Informationssicherheit vor Ort. Die Sicherheitsberatung unterstützt die Informationssicherheitsbeauftragten der Behörden, wenn es darum geht, ein ISMS einzuführen oder ausgewogene Lösungsansätze in Fragen der Informationssicherheit zu finden.

Das Nationale Verbindungswesen des BSI gestaltet die Beziehungen des BSI zu nationalen Partnern in den Bereichen Staat, Wirtschaft und Gesellschaft. Sein besonderes Merkmal ist die regelmäßige Präsenz in ausgewählten Regionen Deutschlands. Dadurch wird der unmittelbare Austausch erleichtert und eine konkrete Erreichbarkeit des BSI vor Ort geschaffen. Der Ausbau der Kooperation mit den relevanten Ansprechpartnern in den Bundesländern ist ein wichtiger Tätigkeitsschwerpunkt der Verbindungspersonen des BSI. Regelmäßige Treffen, die Teilnahme an Veranstaltungen vor Ort sowie Vortragstätigkeiten gehören hierbei zum Angebotsspektrum.

Die operative Zusammenarbeit mit den Ländern erfolgt über den VerwaltungsCERT-Verbund (VCV). Über den VCV sollen die CERTs des Bundes und der Länder den Informationsaustausch verbessern, um effektiver und schneller auf IT-Angriffe reagieren zu können. Der IT-Planungsrat hat ab 2018 ein verbindliches Meldeverfahren zum Informationsaustausch über Cyber-Angriffe eingeführt und somit eine Meldeverpflichtung zwischen Bund und Ländern geschaffen. Das BSI stellt über CERT-Bund Warnungen, Lageberichte sowie Gefährdungsindikatoren bereit. Von Länderseite sind Beiträge zum Lagebild und Vorfallsmeldungen von elementarer Bedeutung und müssen sichergestellt sein.

DAS ZIEL: EIN EINHEITLICHES IT-SICHERHEITSNIVEAU

Neben dem Auftrag aus der Cyber-Sicherheitsstrategie wurde auch auf Ebene der Innenminister und -senatoren von Bund und Ländern 2017 ein Beschluss mit großer Tragweite für die BSI-Länder-Kooperation gefasst. Die Notwendigkeit der Verbesserung der institutionalisierten Zusammenarbeit zwischen Bund und Ländern für den Bereich IT-Sicherheit wurde betont und dem BSI „mit seiner anerkannten Kompetenz und den dort zur Verfügung stehenden Ressourcen“ eine besondere Bedeutung beigemessen.

Übergeordnetes Ziel einer besseren Zusammenarbeit ist die Schaffung eines einheitlichen IT-Sicherheitsniveaus, das angesichts der fortschreitenden Digitalisierung der Verwaltung und einer zunehmenden Vernetzung von IT-Strukturen zwischen Bund und Ländern an Bedeutung gewinnt. Die Sicherheitsberatung und das Verbindungswesen gestalten gemeinsam den Ausbau der Zusammenarbeit des BSI mit den Ländern.

KOOPERATIONSVEREINBARUNGEN MIT DEN LÄNDERN

Im Rahmen von Sondierungsgesprächen werden seit Mitte 2017 der individuelle Kooperations- und Unterstützungsbedarf der Länder erfasst und Modelle für die Umsetzung diskutiert. Ziel der Gespräche sind konkrete Vereinbarungen, um die Zusammenarbeit zu stärken. Mit den Ländern Hessen und Rheinland-Pfalz hat das BSI bereits im Jahr 2017 Modellpartnerschaften initiiert, im Februar 2018 folgte Nordrhein-Westfalen. Ausgangspunkt war die Unterzeichnung von Absichtserklärungen, in denen konkrete Kooperationsfelder festgelegt wurden.

Diese Form der Kooperation bietet das BSI allen Bundesländern gleichermaßen an, wobei die Schwerpunkte und Unterstützungsleistungen individuell und bedarfsgerecht angepasst werden. In diesem Zuge wird mithilfe der BSI-Expertise der Auf- und Ausbau von IT-Sicherheitsstrukturen in den Ländern gezielt zur Stärkung der IT-Sicherheit unterstützt. Auch die Kommunen müssen bei der Stärkung der Bund-Länder-Zusammenarbeit mit einbezogen werden. Sie sollten aus BSI-Sicht an die Allianz für Cyber-Sicherheit angebunden werden. Denn aufgrund der hohen Anzahl an Kommunen ist bei der Festlegung von Schnittstellen zwingend eine Bündelung bzw. Einbindung von Multiplikatoren erforderlich.

DAS ANGEBOT DES BSI

Das Leistungsangebot des BSI wurde in einem Produkt- und Dienstleistungsportfolio zusammengestellt und bedarfsspezifisch aufbereitet (siehe Abb. 1). Ausgehend von der Kategorie „Information“, die u. a. Standards wie den IT-Grundschutz, aber auch Lageberichte und Warnungen umfasst, nimmt der Bereitstellungsaufwand gemäß der dargestellten Pyramide mit jeder Kategorie weiter zu. Neben „Aus- und Fortbildungsangeboten“ und „Kooperationsplattformen“ wie z. B. der Allianz für Cyber-Sicherheit bietet das BSI auch „Beratungsleistungen“ zu verschiedenen Fragestellungen der Umsetzung von IT-Sicherheit. Konkrete „technische Leistungen“, wie die Unterstützung bis hin zur „Übernahme technischer Schutzmaßnahmen“, kann das BSI aufgrund des hohen Ressourcenaufwands nur auf Anfrage anbieten, zum Teil müssen auch entsprechende rechtliche Voraussetzungen erst noch geschaffen werden.

Die Bundesbehörden als traditionelle Kunden des BSI können derzeit auf alle Leistungen des BSI zurückgreifen. Um ein einheitliches und hohes IT-Sicherheitsniveaus in Bund und Ländern zu realisieren, wird angestrebt, dass das BSI den Bundesländern die gleichen operativen Unterstützungsleistungen zur Verfügung stellt wie aktuell der Bundesverwaltung. Dafür fehlen aber bislang entsprechende rechtliche Grundlagen. ■

DAS PRODUKT- UND DIENSTLEISTUNGSPORTFOLIO DES BSI

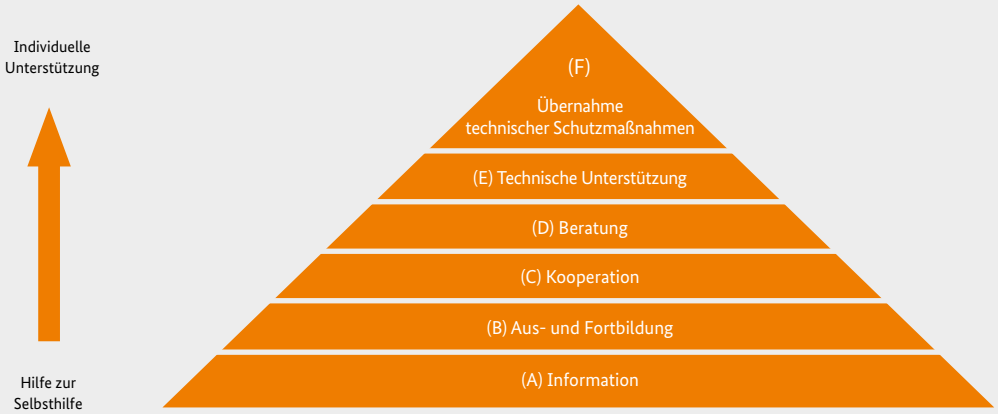


Abb. 1

Randolf Stich, Staatssekretär im Ministerium des Innern und für Sport Rheinland-Pfalz

Interview mit Randolf Stich

„Informationssicherheit ist mehr als das Betreiben von Firewalls."

Wie ist Rheinland-Pfalz im Bereich Cyber-Sicherheit aktuell aufgestellt?

Die rheinland-pfälzische Landesregierung nimmt die aktuelle Bedrohungslage durch Cyber-Angriffe sehr ernst. Die Gewährleistung der Informationssicherheit in der Landesverwaltung ist ihr entsprechend ein wichtiges Anliegen, das auch im Koalitionsvertrag verankert ist. Unter anderem wird derzeit eine bereits verabschiedete Leitlinie zur Informationssicherheit weiter vertieft und umgesetzt. Außerdem hat das Land einen CISO (Chief Information Security Officer) bestellt, der landesweit die Cybersicherheit koordiniert und eine Organisation rund um das Thema aufbaut.

Das rheinland-pfälzische CERT (Computer Emergency Response Team) betreibt die zentralen Angriffserkennungssysteme des Landes, die pro Tag mehr als 20 Millionen sicherheitsrelevante Ereignisse erkennen und abwehren. Die Dienste werden auch von den Kommunen und dem Saarland genutzt.

Welche Herausforderungen sehen Sie in diesem Bereich für Ihr Land?

Neben immer neuen Bedrohungsarten, denen wir täglich begegnen müssen, und zielgerichteten Angriffen auf unsere Infrastruktur ist der Fachkräftemangel eine große Herausforderung. Wir konkurrieren nicht nur mit dem Bund und anderen Ländern, sondern auch mit der Wirtschaft des Rhein-Main-Gebiets um extrem begehrte Fachkräfte.

In den zentralisierten Bereichen haben wir bereits ein gutes Sicherheitsniveau erreicht. Wichtig ist jedoch auch die weitere Ausdehnung in die Fläche. Für nachgeordnete Behörden und noch nicht zentralisierte Dienste ist Informationssicherheit genauso essenziell wie für alle anderen.

Wie planen Sie diese Herausforderungen anzugehen?

Informationssicherheit ist mehr als das Betreiben von Firewalls: Wir betrachten Informationssicherheit aus einem ganzheitlichen Ansatz heraus. Wichtig sind hier vor allem Kooperationen und der Aufbau einer Sicherheitsorganisation für das ganze Land. Die CISO-Geschäftsstelle hat hierfür bereits ein Konzept entwickelt.

Um dem existierenden Fachkräftemangel zu begegnen, setzen wir auch auf einen kooperativen und agilen Ansatz. Nicht jeder Sicherheitsbeauftragte im Land muss das Rad neu erfinden. Aber ein größtmöglicher Austausch muss stattfinden. Das ermöglicht es auch, flexibel und schnell auf neue Bedrohungen zu reagieren.

In welchen Bereichen werden Sie mit dem BSI künftig stärker zusammenarbeiten?

Die Arbeit im CERT-Verbund soll weiter intensiviert werden, unter anderem mit dem Einsatz einer MISP (Malware Information Sharing Platform). Hier leisten wir schon einen großen Beitrag im Bereitstellen von Informationen zu Schadsoftware. Mit den Spezialisten des BSI wollen wir gerade mit Blick auf zielgerichtete Angriffe auf Behörden im Land verstärkt zusammenarbeiten. In schwerwiegenden Fällen werden die rheinland-pfälzischen Kräfte durch Mobile Incident Response Teams (MIRTs) unterstützt, Spezial-Task-Forces des BSI zur Bewältigung von Cyber-Angriffen.

Was sind aus Ihrer Sicht die Vorteile einer Kooperation mit dem BSI?

Cyber-Sicherheit ist eine gesamtstaatliche Aufgabe, die die Zusammenarbeit von Bund, Ländern und Kommunen erfordert. Rheinland-Pfalz will hier seinen Beitrag leisten, um für alle Beteiligten eine höhere Sicherheit zu erreichen.

Zudem ist der Zugang zu Expertenwissen des BSI von großem Vorteil für uns, genauso wie wir unsere Informationen mit dem BSI teilen. Der gegenseitige Austausch bringt beide Partner voran.

Welche Kooperationen gibt es derzeit bereits im Bereich Cyber-Sicherheit und wie bewerten Sie diese?

Gemeinsam mit den Kommunen arbeiten wir an einem umfassenden Konzept, wie wir diese in eine gesamtstaatliche Strategie zur Cyber-Sicherheit einbinden können. Auch länderübergreifend kooperiert Rheinland-Pfalz bereits: Unser CERT übernimmt Leistungen für die Verwaltung des Saarlands. Für die Zukunft streben wir weitere Kooperationen an.

Was wünschen Sie sich als Vertreter einer Landesregierung vom Bund hinsichtlich der künftigen Ausgestaltung der Kooperation?

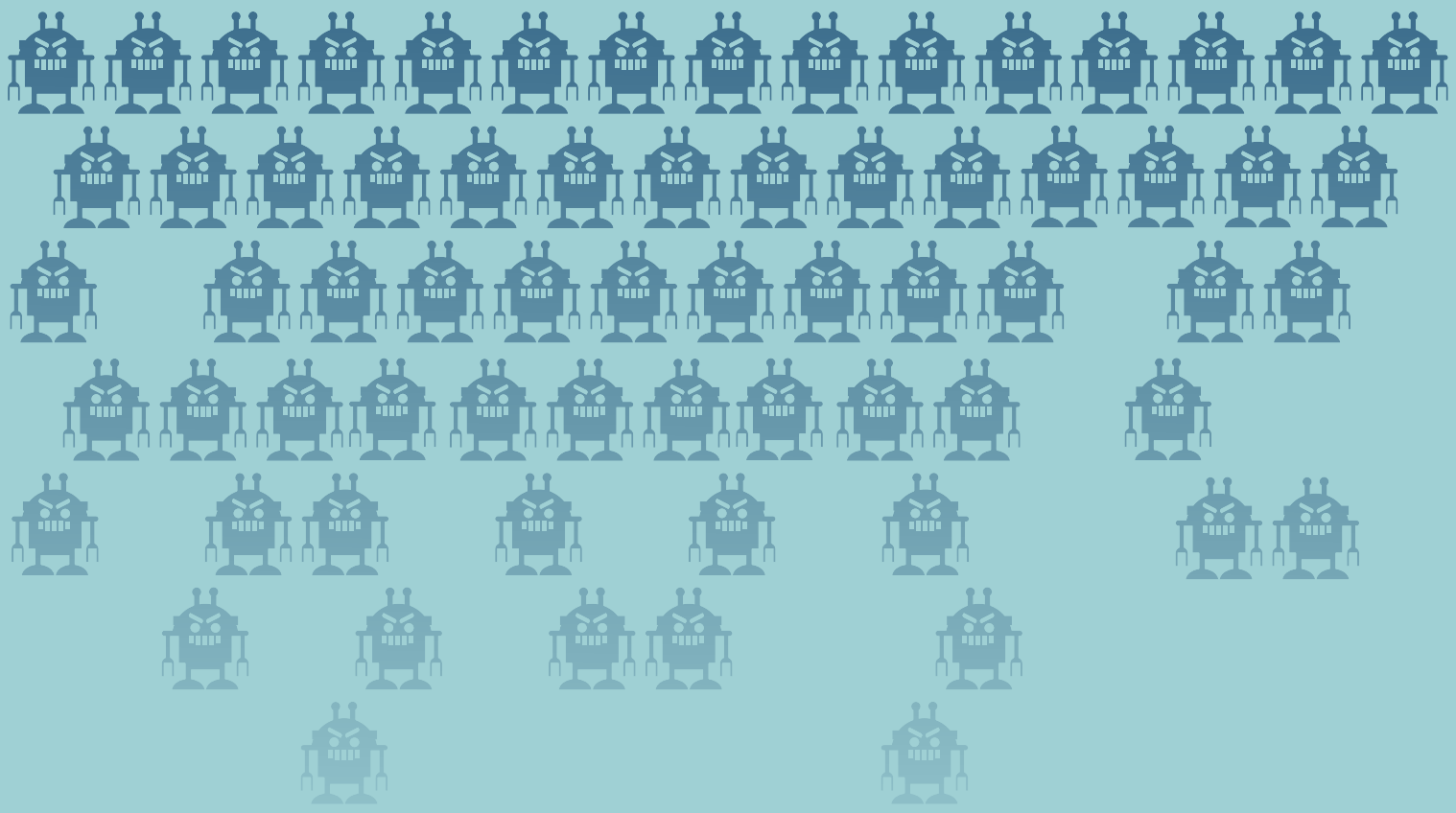
Von der nationalen Cyber-Sicherheitsbehörde wünschen wir uns Zugang zu den ohnehin vorhandenen Produkten und Dienstleistungen, die das BSI bisher nur für die Bundesverwaltung erbringt. Jetzt freuen wir uns aber erst einmal über einen schnellen Start der Zusammenarbeit mit dem BSI.

IT-SICHERHEIT
IN DER PRAXIS

AVALANCHE SINKHOLING

Viele Systeme sind noch infiziert

Vor über einem Jahr hoben die Zentrale Kriminalinspektion Lüneburg und die Staatsanwaltschaft Verden mit maßgeblicher Unterstützung des BSI in einer internationalen Operation erfolgreich die Botnetz-Infrastruktur Avalanche aus. Das BSI traf damals umfangreiche Informations- und Schutzmaßnahmen für betroffene Anwender. Dennoch sind heute noch viele Systeme infiziert. Bürger sollten aus eigenem Interesse aktiv werden und ihre Systeme bereinigen.



Es war eine spektakuläre Aktion: Insgesamt waren an der Operation 30 Länder beteiligt. Als Resultat gab es fünf Festnahmen, 37 Hausdurchsuchungen und die Beschlagnahme von 39 Servern in verschiedenen Ländern – 221 weitere Server wurden durch die Hosting-Provider abgeschaltet. Über 830.000 Botnetz-Domänen wurden beschlagnahmt oder auf sogenannte Sinkhole-Server umgeleitet. Opfer konnten in über 180 Ländern identifiziert werden. Am Ende stand fest: Bei Avalanche handelte es sich um die bis dahin größte bekannte Botnetz-Infrastruktur. Mehr als 20 Botnetz-Familien konnten identifiziert werden. Eine international agierende Tätergruppe hatte hunderttausendfach private und geschäftliche Computersysteme mit unterschiedlicher Schadsoftware infiziert.

BÜRGER MÜSSEN HANDELN

Für das BSI, das als nationale Cyber-Sicherheitsbehörde die Operation maßgeblich unterstützt hatte, stand von Beginn an der Schutz der Bürger an erster Stelle. Durch den Einsatz der Sinkhole-Server konnte die Schadsoftware auf infizierten Rechnern nicht mehr mit den Servern der Urheber kommunizieren – die Kontrolle über die Schadsoftware auf befallenen Rechnern wurde ihnen auf diese Weise entrissen. Da aber weiterhin die IP-Adressen nebst Zugriffszeit der befallenen Rechner registriert wurden, war es bei deutschen IP-Adressen möglich, den jeweils zuständigen Internet-Provider und über diesen den betroffenen Nutzer zu informieren.

Zur Vorsorge vor Infektionen stellte das BSI Signaturen, die aus der Analyse der ermittelten Schadcode-Varianten gewonnen wurden, den Herstellern von Antiviren-Software zur Verfügung.

Doch Ende 2017, rund ein Jahr nach der Aushebung von Avalanche, zeigten Analysen der Infektionszahlen, dass noch immer eine große Anzahl infizierter Systeme vorhanden ist. Zwar hat sich die Zahl in Deutschland nach einem Jahr um 61 Prozent reduziert, was verglichen mit der weltweiten Entwicklung – einer Reduzierung um 45 Prozent – ein großer Erfolg ist. Andererseits bedeutet das, dass viele betroffene Anwender ihre Systeme noch immer nicht bereinigt haben.

Hier besteht dringender Handlungsbedarf. Das BSI hat daher die Schutz- und Informationsmaßnahmen verlängert und ausgeweitet. Aktuell werden so täglich rund 4.800 deutsche IP-Adressen von infizierten Rechnern erkannt und über die Provider benachrichtigt.

GEFÄHRDUNGSPOTENZIAL

Anwender mit infizierten Rechnern müssen davon ausgehen, dass die Täter Informationen, die auf dem befallenen Rechner gespeichert waren, abgegriffen und beispielsweise Kennungen und Kennwörter ausgespäht haben. Zudem wurden Bürger beim Internet-Banking betrogen, Ransomware installiert und die Rechner für den Versand von Spam-E-Mails verwendet. Die identifizierte Schadsoftware wurde überwiegend auf Windows-Rechnern eingesetzt, in einigen Fällen auch auf Smartphones unter Android, beispielsweise um SMS-TANs abzufangen. ■

WERDEN SIE AUS EIGENEM INTERESSE AKTIV!

Sollten Sie eine Benachrichtigung durch Ihren Provider bekommen, dass Rechner an Ihrem Internetanschluss infiziert sind, sollten Sie unmittelbar aktiv werden. Sie müssen davon ausgehen, dass das Schadprogramm Passwörter und Zugangsdaten ausgespäht hat. Auf **www.bsi-fuer-buerger.de/botnetz** finden Sie umfangreiche Informationen, wie Sie die Infektion beseitigen können.

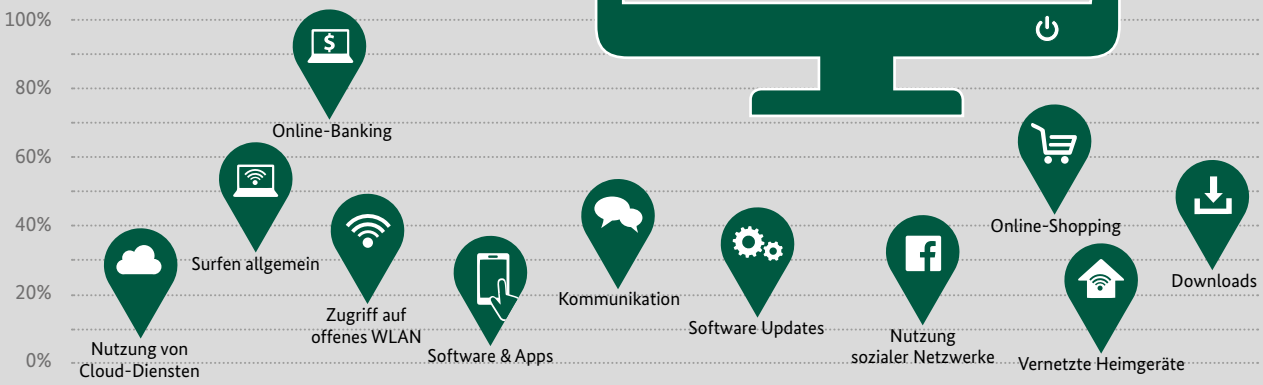
Wichtig ist, dass Sie umgehend nach der Benachrichtigung und der Bereinigung des Rechners alle wichtigen Passwörter ändern. Prüfen Sie weiterhin Ihre Kontoauszüge auf fehlende oder falsche Buchungen. Ähnlich sollten Sie bei allen Kundenkonten, beispielsweise bei Online-Händlern und Auktionshäusern verfahren, um auszuschließen, dass ein Unberechtigter in Ihrem Namen Geschäfte getätigt hat.

Weitere Informationen: https://www.bsi-fuer-buerger.de/botnetz

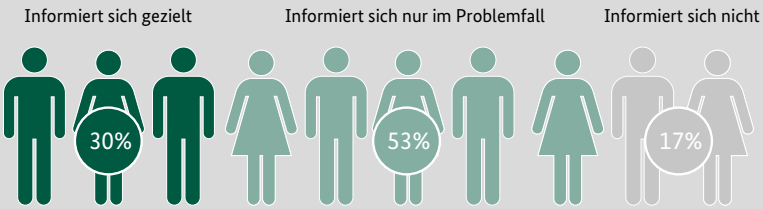
IT-Sicherheit in die Tat umsetzen

Die Digitalisierung sicher zu gestalten ist ein zentrales Anliegen des BSI. Doch wie wichtig ist Bürgerinnen und Bürgern in Deutschland Sicherheit bei der Internetnutzung? Wie schützen sie sich vor Gefahren im Internet? Antworten gibt eine repräsentative Umfrage der Kooperationspartner BSI und Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK).

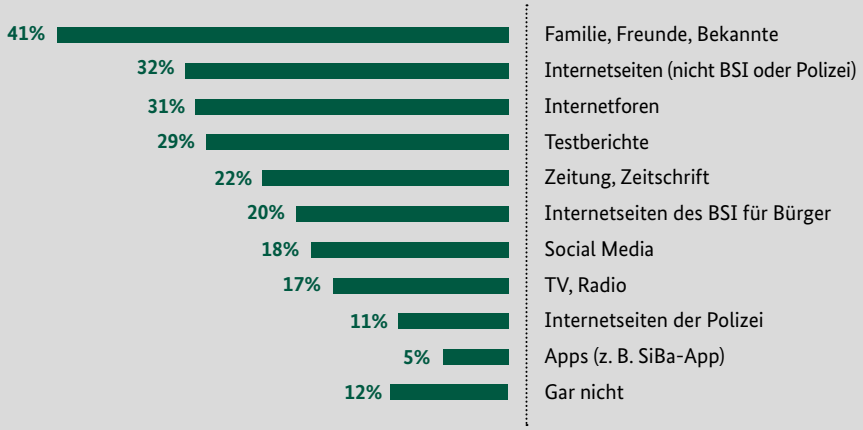
BEI DIESEN TÄTIGKEITEN IST DEN BEFRAGTEN SICHERHEIT BEI DER INTERNETNUTZUNG BESONDERS WICHTIG

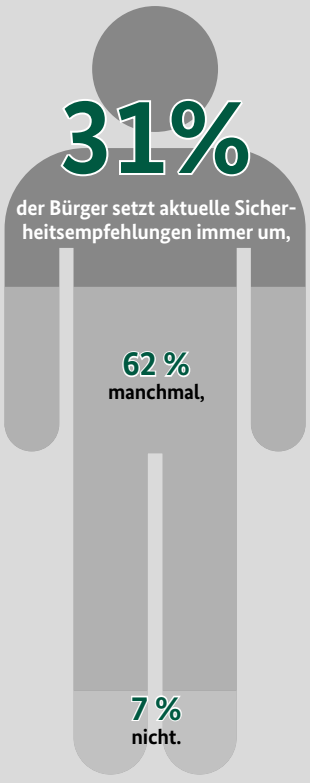


EIN DRITTEL DER BÜRGER INFORMIERT SICH GEZIELT ZU IT-SICHERHEIT



Bürger informieren sich zum Thema IT-Sicherheit über ...





OPFER VON INTERNETKRIMINALITÄT

4 von 10 Bürgern sind schon einmal Opfer von Internetkriminalität geworden.

Ich habe mir selbst geholfen

Ich habe Familie, Freunde oder Bekannte um Hilfe gebeten

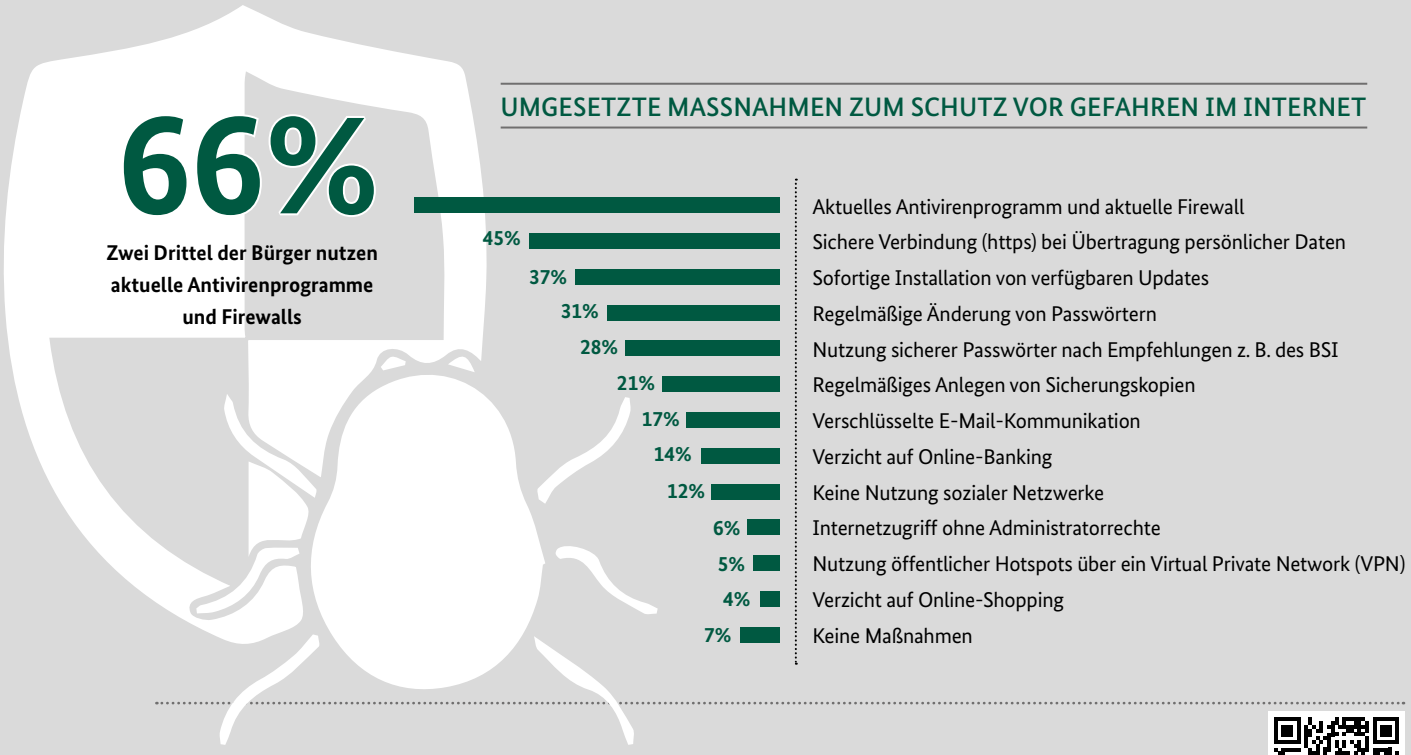
Rund jeder vierte Bürger sieht sich nicht in der Lage, Straftaten im Internet zu erkennen

6 von 10 Bürgern verlassen die Internetseite oder löschen die E-Mail, wenn eine Straftat vermutet wird.

UMGESETZTE MASSNAHMEN ZUM SCHUTZ VOR GEFAHREN IM INTERNET

66%

Zwei Drittel der Bürger nutzen aktuelle Antivirenprogramme und Firewalls



Weitere Informationen: https://www.bsi.bund.de/Umfrage_Internetsicherheit_2018

Quelle: Bundesamt für Sicherheit in der Informationstechnik / Programm Polizeiliche Kriminalprävention der Länder und des Bundes. Repräsentative Onlinebefragung der deutschsprachigen Bevölkerung im Alter von 14 bis 66 Jahren, durchgeführt von Ipsos Public Affairs, Befragungszeitraum 28.09.-09.10.2017, n=2.010.

MIT DEN FOLGEN LEBEN

von Joachim Gutmann, Glücksburg Consulting AG

Lukaskrankenhaus: Gerüstet gegen Cyber-Angriffe

Vor gut zwei Jahren wurde die Städtische Kliniken Neuss – Lukaskrankenhaus – GmbH von einem Cyber-Angriff kräftig durchgeschüttelt und wäre beinahe Opfer einer Erpressung geworden. Doch das Lukaskrankenhaus zahlte nicht, sondern ging digital vorübergehend auf Tauchstation und verstärkte seine Abwehrmechanismen gegen Cyber-Attacken. Freiwillig und bis heute erfolgreich.

„Der Cyber-Angriff an Aschermittwoch hat eine wochenlange digitale Fastenzeit eingeläutet.“

Aschermittwoch, 10. Februar 2016. Ab 09.00 Uhr laufen in der IT-Abteilung des Lukaskrankenhauses die Telefone heiß. Einige Rechner fahren nicht hoch, auf anderen erscheint ein in geschliffenem Englisch verfasster Brief, viele zeigen Fehlermeldungen an. Der Grund: Ein Verschlüsselungs-Trojaner, eingeschleust über den infizierten Anhang einer E-Mail. Sein Ziel: Lösegeld zu erpressen. Alle Daten des Rechners seien verschlüsselt worden, heißt es in dem Brief, und man solle sich an eine bestimmte E-Mail-Adresse wenden.

ERNSTFALL AM ASCHERMITTWOCH

Genau das machte die Klinikleitung aber nicht, sie schaltete stattdessen das Landeskriminalamt (LKA) ein und erstattete Anzeige. Die Techniker der Klinik fuhren alle Systeme herunter und versetzten die Klinik ins vordigitale Zeitalter. Zwei Tage nach dem Angriff wurde auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) eingeschaltet und schickte Experten nach Neuss.

„Der Cyber-Angriff an Aschermittwoch hat eine wochenlange digitale Fastenzeit eingeläutet“, erinnert sich der Kaufmännische Geschäftsführer Dr. Nicolas Krämer. Um die sensiblen Patientendaten zu schützen und ein Ausbreiten des Virus zu verhindern, wurden Boten statt Bits eingesetzt, Laborwerte auf Papier notiert, per Telefon und nicht per Tablet kommuniziert. Geplante große Operationen wurden verschoben, die Klinik meldete sich von der Notfallversorgung ab und nahm keine Schwerverletzten mehr auf. Glück im Unglück: Das Back-up der Nacht zuvor war nicht befallen. Dennoch war das Wiederhochfahren mühsam, und ein Zurück zur alten IT-Infrastruktur, obgleich vor dem Crash auf gutem Niveau, erschien nicht ratsam. Stattdessen wurden eine neue IT-Netzwerkstruktur und eine Citrix-Technologie eingesetzt, die deutlich sicherer sind. „Wir haben unter anderem ein Sandboxsystem zur Entschärfung verseuchter E-Mail-Anhänge eingeführt und unter dem Motto ‚Prävention ist besser als Rehabilitation‘ eine Kooperation mit einem niederländischen Cyber Defense Center abgeschlossen“, erzählt Krämer. Begleitet werden die technischen Sicherheitsmaßnahmen von einer Awareness-Kampagne für die Mitarbeiter. Sie erhalten einmal im Monat einen kurzen Videoclip zur IT-Sicherheit.

„Der Schritt, die IT-Systeme herunterzufahren, war der einzig richtige. Kein Patient kam zu Schaden, keine Patientendaten wurden kompromittiert und das Krankenhaus konnte die Krise als Chance nutzen."

WIEDER BETRIEBSBEREIT

Mehr als einen Monat nach dem Angriff waren die Systeme wieder einsatzbereit. Rund eine Million Euro hat das Krankenhaus dafür aufwenden müssen, zum überwiegenden Teil für die Honorare externer IT-Berater. „Doch der Schritt, die IT-Systeme herunterzufahren, war der einzig richtige", ist der Geschäftsführer überzeugt. „Kein Patient kam zu Schaden, keine Patientendaten wurden kompromittiert und das Krankenhaus konnte die Krise als Chance nutzen."

Zweifel an der Notwendigkeit, die Digitalisierung im Gesundheitswesen und auch im Lukaskrankenhaus voranzutreiben, hat der Cyber-Angriff in Neuss nicht ausgelöst. „Fortschritt im Gesundheitswesen ist ohne Digitalisierung nicht möglich", meint Krämer. „Der Supercomputer IBM Watson enthält das Lehrbuchwissen aller medizinischen Fachbücher dieser Welt und wird Ärzte künftig dabei unterstützen, eine treffsichere Diagnose zu stellen. Mittels weltweiter Big-Data-Analysen werden wichtige Fortschritte in der Krebsforschung zu erzielen sein. Und bereits in wenigen Jahren wird es nicht nur möglich sein, für hundert Euro die individuelle menschliche DNA zu sequenzieren, sondern auch aufzuzeigen, mit welcher Wahrscheinlichkeit dieser Mensch in einem bestimmten Alter eine bestimmte Krankheit erleiden wird."

Datensicherheit und Digitalisierung sind keine feindlichen Brüder – im Gegenteil: Im Prinzip sind digitale Daten besser geschützt als analoge, ist man in Neuss sicher. Derzeit werden Patientendaten an niedergelassene Ärzte noch immer am häufigsten per Fax übermittelt und sind oft genug auch für nicht autorisierte Personen einsehbar oder zugänglich. Auch die gesetzlich vorgeschriebene 30-jährige Archivierung von Patientenakten auf Papier in unzureichend gesicherten Lagern ist ein Sicherheitsproblem. Demgegenüber schreibt das E-Heath-Gesetz Sicherheitsstandards wie doppelte Verschlüsselung und Protokollierung der Datenzugriffe fest. Und die europäische Datenschutzgrundverordnung regelt ab Mai 2018, wie der Datenschutz mit dem Verwenden großer Datenmengen zusammengebracht werden kann.

ERHÖHTE SICHERHEITS-ANFORDERUNGEN

Seit Juli 2017 gelten Krankenhäuser mit mindestens 30.000 vollstationären Patienten pro Jahr als Kritische Infrastruktur und müssen ihre IT-Infrastruktur nach den Vorschriften des IT-Sicherheitsgesetzes ausrichten. Die neuen Regeln gelten für insgesamt 110 Krankenhäuser und Kliniken. Sie müssen ab dem Inkrafttreten der entsprechenden Verordnung gem. § 8b Absatz 3 BSIG

- dem BSI als zentraler Meldestelle für die IT-Sicherheit Kritischer Infrastrukturen einen Ansprechpartner benennen und erhebliche Störungen ihrer IT melden, sofern sie Auswirkungen auf die Verfügbarkeit kritischer Dienstleistungen haben können,
- innerhalb von zwei Jahren dem BSI nachweisen, dass sie angemessene organisatorische und technische Vorkehrungen getroffen haben, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit maßgeblich sind, zu vermeiden,
- die Einhaltung von IT-Sicherheit nach dem Stand der Technik auch danach regelmäßig gegenüber dem BSI nachweisen (§ 8a BSIG).

Im ersten Schritt müssen die Krankenhäuser dazu die zugrunde liegenden

Prozesse feststellen und entsprechende Sicherheitsmaßnahmen planen, umsetzen und dokumentieren. Im zweiten Schritt muss die Umsetzung der Maßnahmen durch eine geeignete prüfende Stelle zertifiziert werden. Deren Prüfbericht wird zu guter Letzt mit Angaben zur geprüften Kritischen Infrastruktur und zum Ansprechpartner alle zwei Jahre beim BSI eingereicht.

Sofern Sicherheitsmängel aufgedeckt werden, darf das BSI im Einvernehmen mit den Aufsichtsbehörden deren Beseitigung anordnen und erforderlichenfalls auch die Hersteller der entsprechenden IT-Produkte und -systeme gemäß § 8b BSIG zur Mitwirkung verpflichten. Umgekehrt hat das BSI sämtliche für die Abwehr von Angriffen auf die IT-Sicherheit Kritischer Infrastrukturen relevanten Informationen zu sammeln, zu bewerten und an die Betreiber sowie die zuständigen (Aufsichts-)Behörden weiterzuleiten.

ATTACKE KANN JEDEN TREFFEN

Das Lukaskrankenhaus in Neuss zählt nicht zu den Einrichtungen, die unter das IT-Sicherheitsgesetz fallen. Denn die Grenze von mindestens 30 000 vollstationären Patienten im Jahr erreichen nach Angaben der Deutschen Krankenhausgesellschaft nur rund zehn Prozent aller Klinken. Diese großen Einrichtungen haben schon von jeher viel in IT-Sicherheit investiert und verfügen in der Regel über eigene Notfallpläne. Dass kleinere Einrichtungen nicht berücksichtigt würden, sei „mit der Versorgungsrealität nicht in Einklang zu bringen", kritisierte zuletzt auch der Marburger Bund.

Auch das BSI hatte 2013 eine Risikoanalyse „Krankenhaus-IT“ veröffentlicht. Sie kam zu dem Ergebnis, dass es um die IT-Sicherheit von Krankenhäusern sehr unterschiedlich bestellt sei: „Während große Häuser, insbesondere Universitätskliniken, um die Bedeutung des Themas wissen", heißt es dort, „wird es gerade bei kleineren Krankenhäusern in ländlichen Gebieten aus Budget- und Personalmangel eher mit untergeordneter Priorität behandelt."

Das könnte fatale Folgen haben, denn die Gefahren sind real, und selbst zufällige Angriffe können erhebliche Schäden verursachen. Die massiven Angriffe mit der Erpressungssoftware „Wannacry“ und „Petya“ im Jahr 2017 haben dies wieder einmal gezeigt. Sie trafen diesmal Krankenhäuser in Großbritannien und den USA. Aber, so weiß man in Neuss: „Der Angriff hat uns klar gemacht, dass Cyber-Attacken jeden treffen können, nicht nur die großen Häuser“, resümiert Krämer. „Und darum sollte sich jeder bestmöglich absichern.“ ■

Joachim Gutmann ist freiberuflicher Journalist und Buchautor. Er ist für die Glücksburg Consulting AG als Kommunikationsexperte tätig.

DIGITALE GESELLSCHAFT

BLOCKCHAINS IM EINSATZ

von Dr. Christian Berghoff und Dr. Ute Gebhardt, Referat Technologische Grundlagen sicherer elektronischer Identitäten, Chipsicherheit

Passende Anwendungsmodelle für geeignete Schutzziele

Das Interesse vieler Unternehmen an Blockchains und ihren Einsatzmöglichkeiten ist ungebrochen. Auch im Koalitionsvertrag wird die Erprobung dieser Technologie angekündigt. Bei der Konzeption von Lösungen sollte allerdings bedacht werden, dass das ausgewählte Blockchain-Modell für die geplante Anwendung und die angestrebten Schutzziele geeignet sein muss.

Blockchains realisieren eine Technologie zur verteilten Datenhaltung (siehe dazu auch BSI-Magazin 02/2017). Dabei werden neue Datenblöcke an eine stetig wachsende Kette angehängt und mit ihrem Vorgänger durch eine kryptografische Hash-Funktion verkettet. Die so entstehende Blockchain wird in einem dezentralen Peer-to-Peer-Netzwerk verteilt. Ein sogenannter Konsensmechanismus sorgt dafür, dass die Daten von allen Netzwerkknoten übereinstimmend anerkannt und konsistent gehalten werden.

Die Wahl dieses Mechanismus hat direkten Einfluss auf die Skalierbarkeit der Blockchain. Der bekannteste Ansatz („Proof-of-Work"), den auch die bekannte Kryptowährung Bitcoin verwendet, erlaubt nur einen geringen Datendurchsatz und ist zudem extrem energieintensiv.

Wesentlich effizientere, nachrichtenbasierte Verfahren können in privaten bzw. „permissioned" Blockchains verwendet werden, in denen – im Gegensatz zu öffentlichen „unpermissioned" Blockchains wie Bitcoin – nicht alle Nutzer über die gleichen Zugriffs- bzw. Zugangsrechte verfügen. Sie sind aufgrund ihrer Beschränkungen auch in IT-sicherheitstechnischen und rechtlichen Fragen weniger problematisch. Die Wahl des passenden Blockchain-Modells ist daher wichtig, und in der Praxis basieren jenseits der Kryptowährungen die meisten Anwendungen auf privaten Blockchains.

EINSATZSZENARIEN

Der Mehrzahl der Blockchain-Anwendungen liegt eine der folgenden Ideen zugrunde:

Zum einen können sie die Eigentumsübertragung von Werten dokumentieren. Dabei verspricht man sich eine sichere Abwicklung von Transaktionen, die ohne Vertrauen auf eine zentrale Instanz auskommt. Zu nennen sind hier Kryptowährungen, vor allem Bitcoin, aber z. B. auch im Energiebereich gibt es Pilotprojekte. Bei einem von ihnen wird bei Transportengpässen im Stromnetz die überschüs-

Blockchain sicher gestalten – Eckpunkte des BSI

von Dr. Manfred Lochter und Dr. Sarah Maßberg,
Referat Kryptografische Vorgaben und Entwicklungen

Für das BSI als die nationale Cyber-Sicherheitsbehörde stehen die technisch-gestalterischen Aspekte von Blockchain mit Bezug zur IT-Sicherheit im Vordergrund. Dazu wurden im Februar 2018 fünf Eckpunkte des BSI veröffentlicht und auf einer Veranstaltung der Reihe „BSI im Dialog“ erstmals vorgestellt. Eine weitere „BSI im Dialog“-Veranstaltung mit speziellem Fokus auf die Finanzbranche ist für Herbst 2018 geplant. Die Eckpunkte sollen für die Herausforderungen der IT-Sicherheit in Blockchains sensibilisieren und den Dialog mit Wirtschaft, Wissenschaft und Verwaltung anregen.

Folgende Kernaussagen sieht das BSI als Eckpunkte zum Thema „Blockchain und IT-Sicherheit“:

Blockchain allein löst keine IT-Sicherheitsprobleme

Die Zielcharakteristika von Blockchain wie Unveränderbarkeit, Nachvollziehbarkeit und Dezentralität sowie die starke kryptografische Fundierung können sich grundsätzlich positiv auf die Sicherheitseigenschaften von IT-Lösungen auswirken, es muss aber gleichzeitig die Sicherheit der verwendeten Hard- und Software sowie der zugrunde liegenden Protokolle gewährleistet werden. Ebenso ist die Sicherheit von externen Schnittstellen der Blockchain, insbesondere für das authentische Einfügen oder Auslesen von Daten, zu beachten. Eine vertrauenswürdige zentrale Stelle wird auch beim Einsatz von Blockchains in vielen Anwendungen nicht vollständig überflüssig werden.

Die Wahl des passenden Blockchain-Modells ist wichtig

Je nach Anwendung muss ein geeigneter Konsensmechanismus zur Herstellung einer Einigkeit über den korrekten Zustand der Blockchain gewählt werden. Außerdem kann sowohl der Zugang zum Netzwerk (unpermissioned – permissioned) als auch der Zugriff auf die Daten (public – private) sowie ein allgemeines Rollen- und Rechtemanagement individuell definiert werden. Die bei Bitcoin verwendete „unpermissioned public“ Blockchain mit „Proof-of-Work“-Konsens ist dabei für viele Anwendungen ungeeignet.

sige Energie in einer Vielzahl räumlich verteilter Batterien gespeichert und später, wenn sich die Lage normalisiert hat, wieder abgegeben. Die Dokumentation der Abrechnung erfolgt über eine Blockchain.

Andere Anwendungen planen, die Technologie zur Integritätssicherung von Dokumenten zu nutzen, indem sie deren elektronische Fingerabdrücke (Hashwerte) in einer Blockchain ablegen. Die Integrität eines Dokuments kann später durch Vergleich seines Hash-Wertes mit dem hinterlegten Hash-Wert zweifelsfrei geprüft werden. Durch die dezentralen Zugriffsmöglichkeiten erhofft man sich Effizienzsteigerungen bei der Integritätssicherung und den Abbau redundanter Strukturen. Dieser Anwendungsfall wird beispielsweise von einer Lösung realisiert, mit der digitale Zeugnisse und Zertifikate verwaltet werden können.

Wieder andere Anwendungen wollen Blockchains bei der Kontrolle von Geschäftsprozessen einsetzen, deren Abläufe in den Datenblöcken gespeichert werden. Transparenz und Unveränderbarkeit der Blockchain versprechen eine nachvollziehbare, fälschungssichere Dokumentation der Prozessschritte. Ein Beispiel ist die Lieferkettenverfolgung im globalen Handel.

VERTRAUENSMODELL

Für die Blockchain-Technologie wird seit ihrem Aufkommen im Zuge von Bitcoin postuliert, dass sie ohne jedes Vertrauen in Intermediäre auskommt und nur auf kryptografischen Beweisen beruht. Es lassen sich jedoch einige Akteure identifizieren, denen ein gewisses Maß an Vertrauen entgegengebracht werden muss. Bei Kryptowährungen sind hier Mining-Pools, die theoretisch die Blockchain manipulieren können, sowie Tauschbörsen zu nennen, in denen Bitcoins gegen Währungen wie Euro und US-Dollar gehandelt werden. Auch wenn diese selbst sich ehrlich verhalten, stellen sie doch lohnende Angriffsziele dar, auf deren angemessenen Schutz die Nutzer vertrauen müssen. Gleiches gilt für die Implementierungssicherheit der Wallets (digitale Geldbörsen). Eine wichtige Machtposition haben – auch bei Open-Source-Projekten – die Programmierer der verwendeten Blockchain-Software inne.

Diesem eher diffusen Vertrauensmodell öffentlicher Blockchains steht das hierarchische Modell privater Blockchains gegenüber, insbesondere wenn es sich um „permissioned“ Blockchains handelt. Es ähnelt dem klassischer Lösungen – zum Beispiel auf Basis von Datenbanken – insofern, als Nutzer dabei Inhabern gewisser Rollen stärker vertrauen müssen.

Bei der Konstruktion von Blockchains müssen Sicherheitsaspekte frühzeitig berücksichtigt werden

Entsprechend den angestrebten Sicherheitszielen sind Aspekte wie Vertraulichkeit, Integrität und Authentizität der Transaktionsdaten, die sichere Ausführung von Smart Contracts und das Identitätsmanagement der Nutzer passend zu modellieren und in der Blockchain umzusetzen. Insbesondere Vertraulichkeit ist bei Blockchain-Anwendungen ein anspruchsvolles Ziel. Bei der Auswahl von Algorithmen und Protokollen sollte man sich nach den Vorgaben des BSI richten.

Sensible Daten mit langfristigem Schutzbedarf müssen in einer Blockchain besonders geschützt werden

Aufgrund der langen Verfügbarkeit (bei gleichzeitig potenziell hoher Sensibilität) von Daten in der Blockchain stellt die Erreichung von Langzeitsicherheit eine besondere Herausforderung dar. Es ist sicherzustellen, dass die Sicherheitsmechanismen der Blockchain bei Bedarf ausgetauscht werden können. Dabei sind insbesondere Anforderungen, die sich aus der Gefährdung durch potenzielle Quantencomputer und technische Fortschritte in der Kryptoanalyse ergeben, zu beachten.

Einheitliche Sicherheitsniveaus für Blockchains müssen definiert und durchgesetzt werden

Die Standardisierung von Blockchains muss weiter vorangetrieben werden und dabei die Aspekte der IT-Sicherheit angemessen berücksichtigen. Auch eine Sicherheitszertifizierung ausgewählter Komponenten nach allgemein anerkannten Kriterien kann für bestimmte Anwendungen sinnvoll sein. Bei Blockchains, die transnational betrieben werden, ist eine internationale Abstimmung erforderlich. Das BSI wird die Entwicklung der Blockchain-Technologie weiter beobachten und fachgerecht bewerten und im Rahmen seiner Zuständigkeiten an Empfehlungen und Anforderungen für Sicherheitsmechanismen von Blockchains mitwirken.

EINORDNUNG DER EIGENSCHAFTEN

Ausgestattet mit geeigneten kryptografischen Algorithmen, können Blockchains Integrität und Verfügbarkeit sicherstellen. Aufgrund der immanenten Transparenz ist Vertraulichkeit jedoch ein anspruchsvolles Ziel. Auch Authentizität muss in der Regel durch zusätzliche Maßnahmen erzielt werden.

Bei der Konstruktion von Lösungen ist der angestrebte Schutzbedarf frühzeitig zu analysieren und zu prüfen, ob die Sicherheitseigenschaften des ausgewählten Blockchain-Modells diesem entsprechen. So kann Transparenz für die Dokumentation von Geschäftsprozessen entscheidend sein, fehlende Vertraulichkeit ist bei der Speicherung sensibler Daten hingegen inakzeptabel. Dezentralität ist dort interessant, wo keine vertrauenswürdigen Instanzen existieren. Wo es sie hingegen gibt, können private Blockchains mit ihrem hierarchischen Vertrauensmodell und ihrer deutlich höheren Effizienz vorzuziehen sein.

Ebenso ist ein Vergleich mit bestehenden Technologien zu empfehlen, um zu entscheiden, wie die gewünschte Funktionalität am sinnvollsten umgesetzt werden kann. Gegenüber Datenbanken bieten Blockchains etwa intrinsische Vorteile in der Verfügbarkeit und Transparenz und erfordern weniger Vertrauen in eine zentrale Stelle. Deutliche Nachteile ergeben sich in den Punkten Vertraulichkeit und Verarbeitungsgeschwindigkeit. ■

„Blockchain sicher gestalten – Eckpunkte des BSI“ unter https://www.bsi.bund.de/Blockchain-Eckpunktepapier

Datensicherheit für vernetzte Mobilität

von Dr. Joachim Damasky, Geschäftsführer des Verbands der Automobilindustrie e. V. (VDA)

Das Auto ist kein Smartphone

Die deutsche Automobilindustrie treibt die Entwicklung von vernetzten Fahrzeugen voran, um Sicherheit, Komfort und Umweltfreundlichkeit der Fahrzeuge weiter zu verbessern. Doch das Auto ist kein Smartphone.

Dr. Joachim Damasky, Geschäftsführer VDA

Fahrzeuge benötigen viel höhere Sicherheitsstandards als Tablets oder Handys. Der Schutz des Kunden und seiner Daten ist im Fahrzeug von ganz besonderer Bedeutung. Auf der einen Seite werden durch die Konnektivität von Fahrzeugen neue Anwendungen für den Kunden ermöglicht, auf der anderen Seite könnte diese Entwicklung das Fahrzeug auch verwundbar gegenüber Cyberattacken machen. Das Fahrzeug ist für seinen Nutzer von hoher Sicherheitsrelevanz. Daher haben Integrität und Sicherheit des Fahrzeugs und Fahrers oberste Priorität und müssen jederzeit garantiert sein.

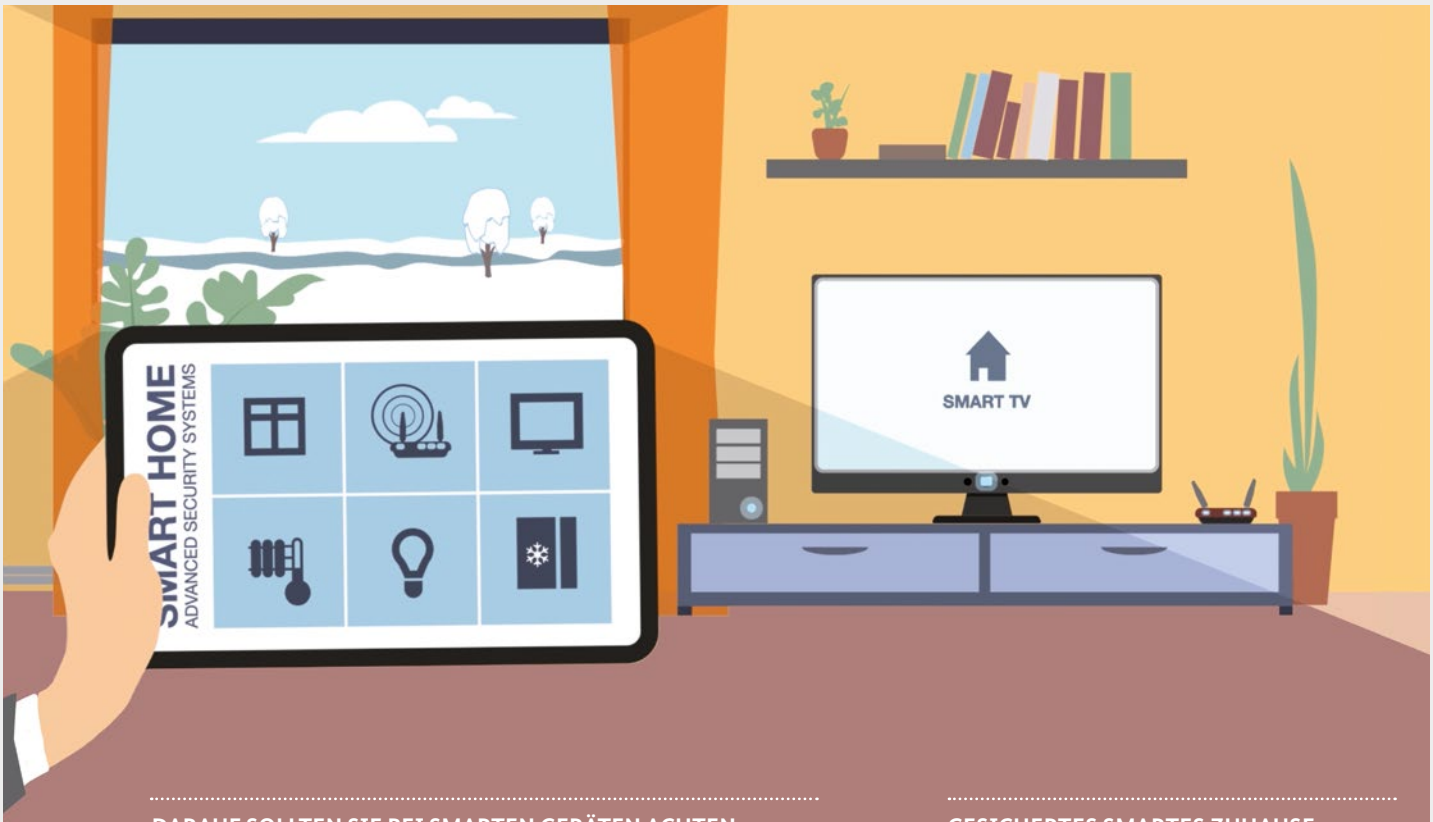
Die deutsche Automobilindustrie hat die Anforderungen an die Fahrzeugsicherheit erkannt und investiert entsprechend in die Absicherung ihrer Produkte, um den Schutzanforderungen gerecht zu werden. Zur Sicherstellung eines Security-Schutzniveaus neuer Produkte wird ein einheitliches methodisches Vorgehen bei der Entwicklung von Fahrzeugsystemen sowie deren Vernetzung beschrieben und in der Industrie angewandt.

Mit „NEVADA-Share & Secure" hat die deutsche Automobilindustrie ein Konzept entwickelt, das die sichere Weitergabe von im Fahrzeug generierten Daten ermöglicht und für öffentliche Stellen und Industrie nutzbar macht. So wird ein Beitrag zur weiteren Verbesserung der Straßenverkehrssicherheit geleistet und die Entwicklung digitaler Innovationen und neuer Geschäftsmodelle unterstützt. Mit der Nutzung der im Fahrzeug generierten Daten durch öffentliche Stellen wie Feuerwehr und Polizei kann die Straßenverkehrssicherheit deutlich erhöht werden. Durch die Auswertung dieser Daten in Verbindung mit Daten der Verkehrsinfrastruktur können Staus schon beim Entstehen identifiziert, Glatteis effizienter lokalisiert oder Unfälle erkannt werden. Die Infrastrukturdaten müssen jedoch von öffentlichen Stellen eingebracht werden. Die Vielzahl der Analysemöglichkeiten bietet einen entscheidenden Mehrwert für die zukünftige Sicherheit auf unseren Straßen. ■

Smart Home

BSI-Basistipp

Vom smarten Fernseher über fernregulierbare Heizungen und Sicherheitskameras bis hin zum intelligenten Kühlschrank: Das vernetzte Zuhause, in dem sich alle Geräte per Smartphone oder Tablet überwachen und steuern lassen, ist längst keine Fiktion mehr. Wer unbeschwert und risikobewusst von den Möglichkeiten eines smarten Zuhauses profitieren möchte, sollte einige einfach zu befolgende Hinweise und Maßnahmen beachten. So schützen Sie Ihr Smart Home vor den Angriffen Cyber-Krimineller.



DARAUF SOLLTEN SIE BEI SMARTEN GERÄTEN ACHTEN

- Die Geräte sollten eine verschlüsselte Kommunikation unterstützen.
- Der Hersteller sollte über einen längeren Zeitraum Softwareupdates bereitstellen und Sicherheitslücken schließen.
- Lokale Nutzung des Geräts ohne Cloud- oder Internetanbindung ist möglich.
- Umgang des Herstellers mit anfallenden Nutzungsdaten prüfen.
- Das voreingestellte Passwort durch ein sicheres, individuelles ersetzen.

GESICHERTES SMARTES ZUHAUSE

Eine Verbindung vernetzter Geräte mit dem Internet ist nur empfehlenswert, wenn ein Zugriff von außen für die Funktion unbedingt notwendig ist. Oft reicht es aus, wenn ein Zugriff auf die Geräte ausschließlich innerhalb des Heimnetzes möglich ist. Zudem sollten mobile Endgeräte das Heimnetzwerk über ein virtuelles privates Netzwerk (VPN) ansteuern.

Weitere Informationen: https://www.bsi-fuer-buerger.de/SmartHome

Verbraucher in der digitalen Welt

von Hanna Heuer, Referat Cyber-Sicherheit für den Bürger und Öffentlichkeitsarbeit, Florian Schumacher, Referat Cyber-Sicherheit für die Gesellschaft und Helga Zander-Hayat, Leiterin des Bereichs Markt & Recht und Mitglied der Geschäftsleitung, Verbraucherzentrale NRW e. V.

Ein Jahr Kooperation zwischen BSI und Verbraucherzentrale NRW

Die Verbraucherzentrale Nordrhein-Westfalen und das BSI blicken auf ein erstes erfolgreiches Jahr der Zusammenarbeit zurück. Zukünftig soll die gemeinsame Arbeit an einer breiten Auswahl von Themen fortgesetzt und weiter ausgebaut werden.

Am 01. März 2017 unterzeichneten der Vorstand der Verbraucherzentrale NRW, Wolfgang Schuldzinski, und BSI-Präsident Arne Schönbohm ein Memorandum of Understanding zur Förderung der Informationssicherheit von Verbrauchern. Als Ziel wurde festgelegt, im Rahmen einer kontinuierlichen vertrauensvollen Arbeit gemeinsam an konkreten Themen der Informationssicherheit zu arbeiten und so von der gegenseitigen Expertise und rechtlichen Befugnissen und Fähigkeiten zu profitieren.

Durch die zunehmende Vernetzung verbinden sich immer mehr Lebenswelten unseres alltäglichen Lebens untrennbar mit dem Digitalen. Das neueste Kleidungsstück wird über das Internet bestellt, die Überweisung per Smartphone getätigt, das smarte Zuhause über die App gesteuert oder die Vitaldaten mit einem Tracker digitalisiert. In vielen Situationen erleichtert uns diese Entwicklung unser tägliches Handeln und bietet Chancen. Gleichwohl gehen hiermit auch Risiken vor allem der Cyber-Sicherheit einher. Dies erfordert resiliente Verbraucher, die in einer sicheren Infrastruktur und mit der Fähigkeit zum kompetenten Handeln agieren. Denn gerade mit Blick auf diese Gruppe wird deutlich, dass Cyber-Sicherheit eine unverzichtbare Bedingung ist, wenn die Digitalisierung gelingen soll.

THEMEN DES ERSTEN JAHRES DER ZUSAMMENARBEIT

Um Gefährdungen zu begegnen und gemeinsam einen Betrag zur Steigerung der Informationssicherheit zu leisten, haben die Verbraucherzentrale NRW und das BSI die Zusammenarbeit im vergangenen Jahr vereinbart. Die Kombination aus den beidseitigen Kompetenzen hat sich bereits im ersten Jahr als sehr fruchtbar erwiesen. Dies wird anhand der folgenden vier Beispiele der Zusammenarbeit erkennbar:

1

UPDATE-FÄHIGKEIT VON SMARTPHONES

Im Handel werden Smartphones mit einem veralteten Betriebssystem als neu angeboten, für die aber keine Sicherheitsupdates mehr durch den Hersteller zur Verfügung gestellt werden. Hierdurch bestehen bei der Nutzung teils gravierende Sicherheitslücken. Ein Beispiel dafür sind die im Juli 2015 unter dem Namen „Stagefright“ bekannt gewordenen Sicherheitslücken im gleichnamigen Multimedia-Framework des Betriebssystems Android von Google. Für Verbraucher sind die Aktualität der Software und fehlende Update-Möglichkeiten kaum zu erkennen. Für eine informierte Kaufentscheidung sind aber transparente Informationen notwendig. Diese liefern die Verkäufer allerdings oftmals nur unzureichend. Nachdem das BSI bei einem Smartphone Sicherheitslücken festgestellt hatte, nutzte die Verbraucherzentrale NRW ihre Befugnis zur Verbandsklage und leitete ein gerichtliches Unterlassungsverfahren gegen den Verkäufer des betroffenen Geräts wegen unzureichender Verbraucherinformation ein. Das Verfahren ist noch nicht abgeschlossen.

2

PHISHING-RADAR

Mit Phishing-Nachrichten versuchen Betrüger Nutzer dazu zu bewegen, ihre Zugangsdaten, beispielsweise zum Online-Banking, auf gefälschten Seiten zu offenbaren. Die Verbraucherzentrale NRW sammelt bereits seit dem Jahr 2010 Informationen zum Internetbetrug. Verbraucher können betrügerische E-Mails direkt an die eigens dafür eingerichtete E-Mail-Adresse phishing@verbraucherzentrale.nrw senden. Diese langjährigen Erkenntnisse werden nun mit dem BSI ausgetauscht und als Beitrag für die Lagebewertung genutzt.

3

GEMEINSCHAFTSREDAKTION DER VERBRAUCHERZENTRALEN

Informations- und Sensibilisierungsmaßnahmen leisten einen wichtigen Beitrag, um die Handlungskompetenz bei Nutzern zu steigern. Hier bietet das BSI mit „BSI für Bürger“ ein etabliertes Angebot. Die Verbraucherzentralen sind eine anerkannte Anlaufstelle im Internet und in den überregionalen Beratungsstellen. Inhalte für die Webseiten werden über eine zentrale Gemeinschaftsredaktion produziert, angegliedert an die Verbraucherzentrale NRW. Die technische Expertise des BSI für Bürger kann in diese Arbeit einfließen, sodass sich die Verbraucher fundiert zu Cyber-Sicherheitsthemen online informieren können.

4

VERNETZTES SPIELZEUG

Die Vernetzung hält auch im Kinderzimmer Einzug. Immer mehr Spielzeuge haben unmittelbare beziehungsweise mittelbare Schnittstellen zum Internet. Damit gewinnen auch Aspekte des Datenschutzes und der Datensicherheit für diesen Produktbereich an Relevanz. Gemeinsam mit der Verbraucherzentrale NRW untersucht das BSI daher die Sicherheit von vernetztem Spielzeug und überprüft beispielhaft einen Spielzeugroboter auf Schwachstellen bei der Datensicherheit. Der Roboter wird mittels einer App via WLAN gesteuert und arbeitet mit einer Gesichtserkennungstechnologie. Er soll mit dem spielenden Kind interagieren können und filmt dazu laufend seine Umgebung.

FAZIT & AUSBLICK

Die Verbraucherzentrale NRW und das BSI können auf ein erfolgreiches Jahr der Kooperation zurückblicken. Insbesondere die gerichtliche Prüfung der Informationspflicht der Verkäufer über nicht mehr updatefähige Smartphones könnte eine große Signalwirkung entfalten. Hieraus könnten zusätzliche Fragestellungen sowie Handlungsbedarfe entstehen. Auch in anderen Feldern möchten beide Partner die Kooperation weiter mit Leben füllen, um gemeinsam die Informationssicherheit für Verbraucher zu steigern. Hierfür kommen die Sicherheit von Hard- und Software im Bereich Smart-Home sowie die verbraucherrelevanten Fragestellungen rund um die Aktivierung privater WLAN-Hotspots in Betracht. Aber auch aktuelle Sicherheitslücken werden wohl immer wieder auf der Agenda stehen. ■

ZU GUTER LETZT

VERANSTALTUNGEN 2018/19

CeBIT

11.–15. Juni 2018 in Hannover

Das BSI stellt auch 2018 auf der CeBIT aus, die in diesem Jahr erstmals mit neuem Konzept im Juni stattfindet. Unter dem Titel „Europas Business-Festival für Innovation und Digitalisierung" plant die Messe Hannover einen Dreiklang aus Ausstellung, Konferenz und Festival. Thema der „neuen CeBIT" ist die Digitalisierung von Unternehmen, Verwaltung und Gesellschaft.

Free and Open Source Software Conference (FrOSCon)

25.–26. August 2018 in Sankt Augustin

Das BSI ist auf der Free and Open Source Software Conference (FrOSCon) 2018 vertreten, die vom 25. bis 26. August 2018 in Sankt Augustin stattfindet. Der Fachbereich Informatik der Hochschule Bonn-Rhein-Sieg veranstaltet dort mit Hilfe des FrOSCon e.V. ein interessantes Programm mit Vorträgen und Workshops für Entwickler und Anwender Freier Software. Auf den Projektständen des BSI können sich die Messebesucher über einige BSI-Projekte im Bereich Freier Software informieren.

IFA 2018

31. August – 5. September 2018 in Berlin

Anfang September stellt das BSI auf der Internationalen Funkausstellung in Berlin aus. Auf der globalen Leitmesse für Consumer Electronics und Home Appliances versammeln sich mehr als 1.800 Aussteller, die ihre neusten Produkt-Highlights auf einer vermieteten Ausstellungsfläche von 159.000 m² präsentieren.

it-sa

9.–11. Oktober 2018 in Nürnberg

Im Oktober 2018 ist das BSI mit einem Stand und verschiedenen Vortragsaktivitäten auf der it-sa in Nürnberg vertreten. Die it-sa ist die einzige IT-Security-Messe im deutschsprachigen Raum und eine der bedeutendsten weltweit. Das BSI fungiert gemeinsam mit dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom e. V.) als ideeller Träger der Messe.

2018 findet zur it-sa erstmals das Symposium „Verwaltung integriert sichere Informationstechnologie (ViS!T)“ statt, zu dem das BSI in diesem Jahr einlädt. Am 8. und 9. Oktober diskutieren Fachleute aus Deutschland, Österreich, der Schweiz und Luxemburg aktuelle Herausforderungen bei der sicheren Gestaltung von IT-Prozessen.

16. Deutscher IT-Sicherheitskongress

19.–23. Mai 2019 in Bonn-Bad Godesberg

Im Mai 2019 richtet das BSI erneut den Deutschen IT-Sicherheitskongress in Bonn aus. Mit mehr als 600 Fachbesuchern ist der alle zwei Jahre stattfindende Kongress eine feste Größe im Veranstaltungskalender der IT-Sicherheitsbranche. Drei Tage lang diskutieren die Teilnehmer über den Stand der nationalen und internationalen Entwicklung zur IT-Sicherheit. Ziel des Kongresses ist es, das Thema IT-Sicherheit aus unterschiedlichen Blickwinkeln zu beleuchten, Lösungsansätze vorzustellen und weiterzuentwickeln. Eine begleitende Ausstellung ergänzt das Vortragsprogramm.

Ab Mai 2018 startet der Call for Papers, mit dem das BSI Fachreferenten um ihre Einreichungen für Vortragsthemen bittet. Ein Beirat prüft die Einsendungen und entscheidet, welche Themen auf dem 16. Deutschen IT-Sicherheitskongress vorgestellt werden. Mehr Informationen erhalten Sie ab Mai unter **www.bsi.bund.de/sicherheitskongress** oder per Mail an **papers2019@bsi.bund.de**.

Eine aktuelle Vorschau zu Veranstaltungen mit BSI-Beteiligung finden Sie unter: https://www.bsi.bund.de/Veranstaltungen

Bestellen Sie Ihr BSI-Magazin!

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Referat Cyber-Sicherheit für den Bürger und Öffentlichkeitsarbeit

Postfach 20063
53133 Bonn
Telefon: +49 (0) 228 99 9582 0
Telefax: 0228 99 9582-5455
E-Mail: bsi-magazin@bsi.bund.de

Zweimal im Jahr gibt das BSI-Magazin „Mit Sicherheit“ Einblick in nationale und internationale Cyber-Sicherheitsthemen, die digitale Gesellschaft sowie IT-Sicherheit in der Praxis. Lassen Sie sich jetzt direkt nach Erscheinen zur Hannover Messe im April und zur it-sa im Oktober die aktuellste Ausgabe bequem per Post zusenden, indem Sie sich mit unten stehendem Formular für den Abo-Verteiler anmelden.

Wählen Sie hier aus, welche BSI-Publikation Sie im Abo erhalten wollen:

☐ BSI-Magazin „Mit Sicherheit“ (2 x im Jahr, Print)
☐ Die Lage der IT-Sicherheit in Deutschland (1 x im Jahr, Print)

Einwilligung in die Speicherung Ihrer Kontaktdaten

Name, Vorname

Organisation

Straße

PLZ, Ort

E-Mail

Einfach das Formular per Fax oder E-Mail einsenden:
Telefax: 0228 99 9582-5455 | E-Mail: bsi-magazin@bsi.bund.de

Oder Sie melden sich direkt online an:
https://www.bsi.bund.de/DE/Publikationen/BSI-Magazin/BSI-Magazin_node.html

Wenn Sie die Speicherung Ihrer persönlichen Daten widerrufen und die BSI Publikationen nicht mehr erhalten möchten, schicken Sie uns einfach eine E-Mail an **bsi-magazin@bsi.bund.de**. Ihre Daten werden dann unverzüglich gelöscht.

Folgen Sie dem BSI auch auf Facebook und Twitter!
www.facebook.com/bsi.fuer.buerger | twitter.com/bsi_presse
Weitere Informationen sowie Checklisten und Tipps rund um Cyber-Sicherheit finden Sie unter:
www.bsi.bund.de | www.bsi-fuer-buerger.de | www.allianz-fuer-cybersicherheit.de

Datenschutzhinweis: Ihre personenbezogenen Daten werden unter Berücksichtigung des Bundesdatenschutzgesetzes und der EU-Datenschutz-Grundverordnung elektronisch gespeichert, verarbeitet und genutzt. Verantwortliche Stelle für diese Daten sowie deren Verarbeitung ist das BSI. Eine Weitergabe an Dritte erfolgt nur für Versandzwecke. Eine Verwendung zu anderen Zwecken findet ohne Ihre Zustimmung nicht statt.

IMPRESSUM

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI) 53175 Bonn
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Referat B23 – Cyber-Sicherheit für den Bürger und Öffentlichkeitsarbeit Godesberger Allee 185–189 53175 Bonn Telefon: +49 (0) 228 999582-0 E-Mail: bsi-magazin@bsi.bund.de Internet: www.bsi.bund.de
Stand:	April 2018
Texte und Redaktion:	Stephan Kohzer, Nora Basting und Mark Schulz, Bundesamt für Sicherheit in der Informationstechnik (BSI); Joachim Gutmann, GLC Glücksburg Consulting AG; Fink & Fuchs AG
Konzept, Redaktion und Gestaltung:	Fink & Fuchs AG, Berliner Straße 164 65205 Wiesbaden Internet: www.finkfuchs.de
Druck:	Druck- und Verlagshaus Zarbock GmbH & Co KG Sontraer Str. 6 60386 Frankfurt a.M. Internet: www.zarbock.de
Artikelnummer:	BSI-Mag 18/707-1
Bildnachweise:	Titel/S. 25: GettyImages©enot-poloskun, GettyImages©FredFroese, GettyImages©Guido Mieth Moment, GettyImages©yoh4nn; S. 2: Stephan Kohzer/BSI; S. 4: Bundesministerium des Innern (o.), Mesago/Thomas Geiger (u.); S. 5: Fink & Fuchs, iStock.com/Grafissimo; iStock.com/Krasyuk (o. l.), BSI (o. r.), GSMA (u.); S. 6: NCSC; S. 9: NCSC; S. 10: NürnbergMesse it-sa; S. 12: GettyImages©Talaj; S. 14/15: GettyImages©Mehau Kulyk/ Science Foto Library; S. 16/17: GettyImages©Dong Wenjie; BSI, GettyImages©3alexd; S. 18-21: GettyImages©Andrzej Wojcicki, GettyImages© Andrzej Wojcicki/GettyImages©PeopleImages; S. 22: GettyImages©bubaone; S. 23: BSI; S. 27: GettyImages©akindo; S. 31: Anapur AG; S. 33: Robert Bosch GmbH; S. 35: BSI; S. 37: BSI (o. l.), BSI (u. l.), Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen (rechts); S.39: Ministerium des Innern und für Sport Rheinland-Pfalz; S. 40, 42, 43: R. Winkler; S. 44-47: Städtische Kliniken Neuss - Lukaskrankenhaus - GmbH; S. 48, 50/51: GettyImages©a-r-t-i-s-t; S. 52: ©VDA 2018; S. 53: junge meister GmbH; S. 54, 55: R. Winkler; S. 56, 57: GettyImages©Ragnar Schmuck

Das BSI-Magazin erscheint zweimal im Jahr. Es ist Teil der Öffentlichkeitsarbeit des BSI.
Es wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

Für die digitale Version des BSI-Magazins scannen Sie den QR-Code
https://www.bsi.bund.de/BSI-Magazin

www.bsi.bund.de