Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Magazin 2018/02

Mit Sicherheit

Verschlüsselung als Grundlage für eine sichere Digitalisierung

CYBER-SICHERHEIT

Quantencomputer – eine BSI-Studie zum Entwicklungsstand

DAS BSI

Deutschland.Digital.Sicher. BSI – Positive Resonanz auf erstes BSI-Symposium

IT-SICHERHEIT IN DER PRAXIS

E-Mails einfach verschlüsseln – EasyGPG erleichtert den Schlüsselaustausch

EDITORIAL

Ein hohes Gut

„Verschlüsselte Kommunikation ist eine wichtige Grundlage für den Erfolg einer sicheren Digitalisierung in Staat, Wirtschaft und Gesellschaft.“

Das Briefgeheimnis ist ein hohes Gut. Durch das Grundgesetz geschützt, ist es ebenso wie das Post- und Fernmeldegeheimnis unverletzlich.

Wir nehmen dieses Grundrecht ganz selbstverständlich in Anspruch. Wir protestieren, wenn es verletzt wird. Aber wir halten uns auch an die einfachen Regeln, die es bewahren helfen. Kaum jemand würde auf die Idee kommen, vertrauliche Informationen auf einer Postkarte zu verschicken.

Tatsächlich ist eine unverschlüsselte E-Mail aber nichts anderes – jeder, dem sie in die Hände fällt, kann sie lesen. Doch der Umgang mit vertraulichen Informationen sieht in der digitalen Welt oft ganz anders aus: Häufig gehen wir – im Privatleben genauso wie im Beruf – mit E-Mails um, als würden wir ausschließlich Urlaubsgrüße per Postkarte versenden.

Dabei ist verschlüsselte Kommunikation eine wichtige Grundlage für den Erfolg einer sicheren Digitalisierung in Staat, Wirtschaft und Gesellschaft. Doch obwohl Provider mittlerweile eine Vielzahl von Verschlüsselungslösungen anbieten, werden diese bislang kaum genutzt. Hauptgrund hierfür ist, dass die Anwendung im Alltag für viele Menschen zu kompliziert ist. Vor allem die Komplexität von Schlüsselbeantragung und –management steht einer breiten Nutzung im Wege. Hier setzt das Projekt easyGPG des BSI an, das wir Ihnen in der vorliegenden Ausgabe des BSI-Magazins ab Seite 36 ausführlich vorstellen. Auch europaweit bringt sich das BSI zum Thema E-Mail-Sicherheit ein: Wie wir gemeinsam mit europäischen Partnern moderne Sicherheitsstandards beim E-Mail-Transport etablieren, lesen Sie ab Seite 10.

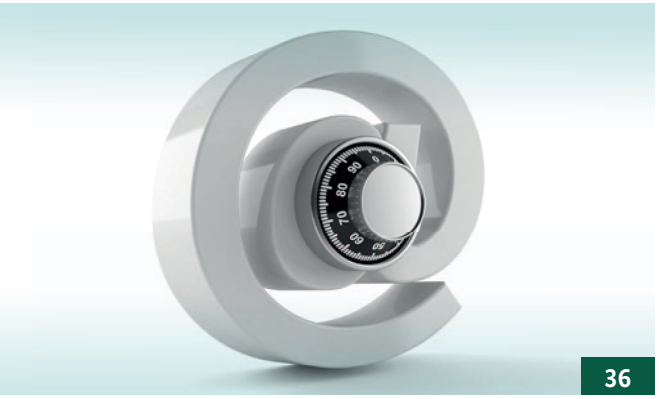
Parallel zur Erhöhung der Nutzerfreundlichkeit muss das Vertrauen in die Sicherheit der E-Mail-Kommunikation stabilisiert werden. Die 2018 entdeckten Schwachstellen in S/MIME und OpenPGP, den beiden am weitesten verbreiteten Standards für E-Mail-Verschlüsselung, haben viele Anwender verunsichert. Langfristig werden eine Anpassung der bekannten Verschlüsselungsstandards und neue Investitionen in die Kryptografie nötig sein. Das BSI als nationale Cyber-Sicherheitsbehörde hat dazu seine Unterstützung angeboten. Am Ziel, Deutschland zum Verschlüsselungsstandort Nummer 1 zu machen, halten wir ausdrücklich fest. Wie wir uns beispielsweise mit Public-Key-Kryptografie für das Zeitalter der Quantencomputer beschäftigen, lesen Sie ab S. 22.

Der Ausbau des BSI als nationale Cyber-Sicherheitsbehörde und zentrales Kompetenzzentrum für Informationssicherheit, wie ihn die Bundesregierung vorgesehen hat, ist auch Voraussetzung dafür, dass wir uns im Bereich der Verschlüsselung noch stärker einbringen können.

Über das Thema E-Mail-Sicherheit hinaus stellen wir Ihnen in dieser Ausgabe des BSI-Magazins wieder ein breites Spektrum an Themen des BSI vor: Die Sicherheit onlinebasierter Zahlungsdienste zählen ebenso dazu wie die Zusammenarbeit mit unseren niederländischen Partnern vom NCSC und der digitale Verbraucherschutz.

Ich wünsche Ihnen eine anregende Lektüre
Ihr

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik



INHALT

AKTUELLES

4 Kurz notiert

BSI INTERNATIONAL

6 NCSC und BSI – Interview mit Hans de Vries
10 Sicherer E-Mail-Transport für Europa
12 ViS!T-Symposien – Drei Länder, eine Idee
14 KRITIS in Europa

CYBER-SICHERHEIT

16 Im Visier – Cyber-Angriff auf die deutschen Hidden Champions
20 Das Jahr im Rückblick – Erkenntnisse aus dem BSI-Lagebericht 2018
22 Public-Key-Kryptografie zukunftssicher machen
24 Quantencomputer – eine BSI-Studie zum Entwicklungsstand
26 VS-Anforderungsprofile

DAS BSI

28 Deutschland.Digital.Sicher.BSI – Positive Resonanz auf erstes BSI-Symposium
30 Binden, motivieren, entwickeln – Das BSI fördert Nachwuchs-Führungskräfte aus den eigenen Reihen
34 Cyber Competence Center Hessen

IT-SICHERHEIT IN DER PRAXIS

36 E-Mails einfach verschlüsseln – EasyGPG erleichtert den Schlüsselaustausch
40 Praktikable Lösung – Schablonen für Informationssicherheit
42 Signaturen bekämpfen Steuerbetrug im Einzelhandel

DIGITALE GESELLSCHAFT

44 Digitaler Verbraucherschutz
46 Digitale Transformation – Den Menschen mitnehmen
48 Elektronische Identitäten europaweit nutzen
50 Starke Kundenauthentifizierung nach PSD2
52 PSD2 – Aufsichtliche Regelungen für mehr Sicherheit und Wettbewerb im Zahlungsverkehr
54 Hilfe bei Cyber-Angriffen – Unterstützung von KRITIS-Unternehmen durch Fachexperten
56 Basis-Tipp: Back-up

ZU GUTER LETZT

57 16. Deutscher IT-Sicherheitskongress
59 Bestellen Sie Ihr BSI-Magazin!
63 Impressum

AKTUELLES

Konferenz

HPI Potsdam

Am 21. und 22. Juni 2018 veranstaltete das Hasso-Plattner-Institut (HPI) die „6. Potsdamer Konferenz für Nationale CyberSicherheit" am Potsdamer Campus Griebnitzsee. Neueste Erkenntnisse und Trends aus dem Bereich der Cyber-Sicherheit wurden von hochrangigen Vertretern deutscher und internationaler Sicherheitsbehörden, der Politik sowie aus Wirtschaft und Gesellschaft vorgestellt. Auch Arne Schönbohm Präsident des BSI, sprach zum Thema „Gefährdungslage, und was das BSI als nationale Cyber-Sicherheitsbehörde tut".

Weitere Informationen: https://www.potsdamer-sicherheitskonferenz.de/konferenz.html

Handbuch

Cyber-Risiko-Management für Entscheider

Damit Cyber-Sicherheit zur Chefsache werden kann, ist auch bei Unternehmenslenkern ein Grundverständnis für die Risiken im Bereich Informationssicherheit nötig. Nur so können diese die potenziellen wirtschaftlichen Schäden durch Cyber-Vorfälle informiert bewerten und über die Validität von IT-Sicherheitsstrategien entscheiden. Genau an diese Zielgruppe richtet sich das jetzt für den deutschen Markt überarbeitete Handbuch „Management von Cyber-Risiken" der US-amerikanischen Internet Security Alliance (ISA). Darin werden fünf grundlegende Prinzipien formuliert, die Vorstände und Aufsichtsräte bei der Betrachtung von Cyber-Risiken unterstützen, ergänzt durch mehrere Anhänge u. a. mit Ressourcen des BSI für die Wirtschaft. Unterstützt wurde die Erstellung der deutschen Version durch die Allianz für Cyber-Sicherheit (ACS) und das ISA-Mitglied AIG.

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

Treffen

3. Treffen der deutschen Cyber-Sicherheits-Initiativen

Bereits zum dritten Mal kamen am 13. Juni 2018 zahlreiche Cyber-Sicherheits-Initiativen aus Deutschland zusammen, um über mögliche Synergien zwischen ihren Sensibilisierungsaktivitäten zu sprechen. Eingeladen hatte die Allianz für Cyber-Sicherheit, Gastgeber des Treffens war das Niedersächsische Ministerium für Inneres und Sport. Vertreterinnen und Vertreter der Initiativen präsentierten in Hannover die ersten Ergebnisse ihrer Kooperation für mehr Cyber-Sicherheit in Deutschland – darunter die Durchführung gemeinsamer Veranstaltungen, die Bekanntmachung von Projekten anderer Initiativen in den eigenen Netzwerken oder das Engagement als Multiplikator der Allianz für Cyber-Sicherheit (ACS). Im Hinblick auf den weiteren Ausbau der Kooperation wurden unter anderem gemeinsame Aktivitäten im Rahmen des European Cyber Security Month (ECSM) im Oktober 2018 geplant.

Weitere Informationen:
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/infos/20180614_CS_Initiativen_Treffen.html

Beste Behörde

BSI als Arbeitgeber

Deutschlands attraktivste Arbeitgeber 2018 TOP 1 ÖFFENTLICHER SEKTOR trendence ABSOLVENTEN

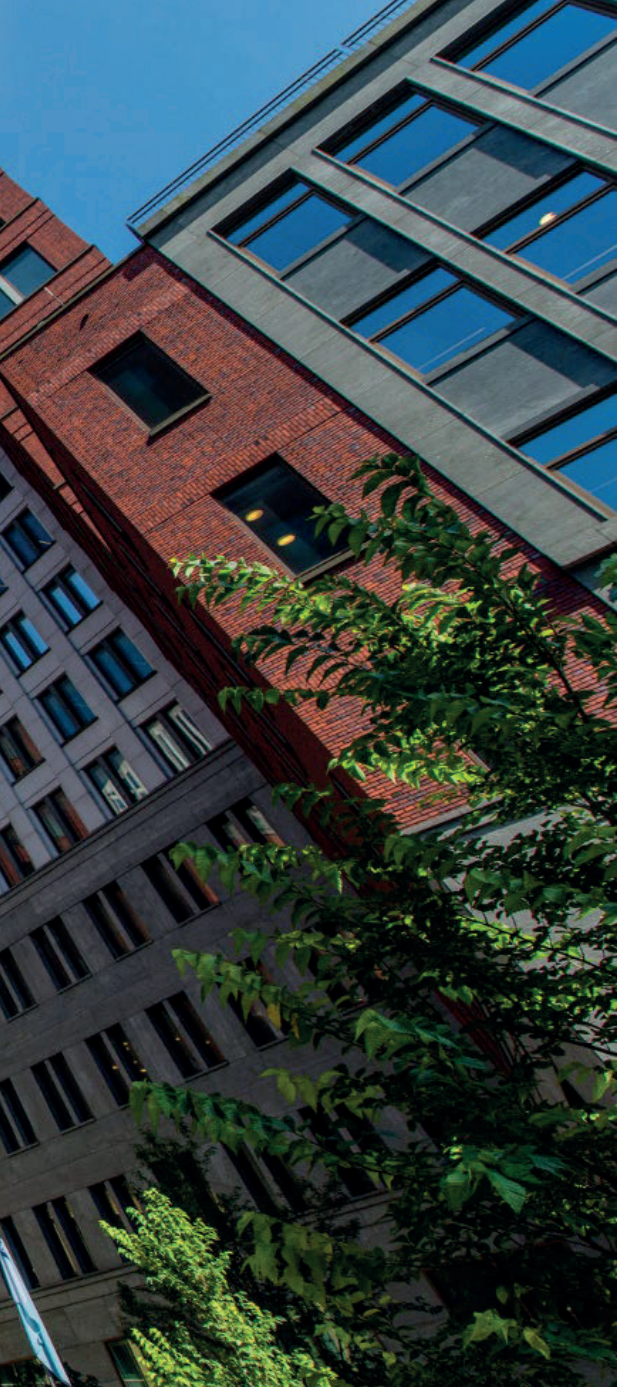
Auch 2018 gehört das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu den Top 100 Arbeitgebern im Bereich Informationstechnologie in Deutschland. Das Forschungs- und Beratungsunternehmen trendence hat im Rahmen des „Graduate Barometer – IT Edition“ rund 6.000 deutsche Studierende an 59 Hochschulen befragt. Das BSI rückte im Vergleich zum Vorjahr zwei Plätze nach vorne und wurde auf Rang 14 der Gesamtliste gewählt: Damit ist das BSI als beste Behörde die Nummer eins im Bereich des öffentlichen Dienstes.

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

BSI INTERNATIONAL

NCSC & BSI

Interview mit Hans De Vries, Leiter des Nationalen Cybersicherheitszentrums der Niederlande, Stellvertretender Direktor Cyber Security



Das Nationaal Cyber Security Centrum (NCSC) ist die zentrale Informationsdrehscheibe und das Kompetenzzentrum für Cyber-Sicherheit in den Niederlanden. Aufgabe des NCSC ist es, zur Stärkung der Resilienz der niederländischen Gesellschaft im digitalen Bereich beizutragen und so eine sichere, offene und stabile Informationsgesellschaft zu schaffen. Auf internationaler Ebene ist das NCSC die niederländische Anlaufstelle für IKT-Bedrohungen und Cyber-Sicherheitsvorfälle. Zudem übernimmt es im Fall einer größeren IKT-Krise eine zentrale Rolle bei der operativen Koordination und dient als Computer Emergency Response Team (CERT) für die Regierung und die Kritischen Infrastrukturen der Niederlande.

NCSC wurde 2012 gegründet. Welche Meilensteine wurden seitdem erreicht?

Ein wichtiger Meilenstein in der kurzen Geschichte des NCSC ist die Zusammenarbeit sowohl mit öffentlichen als auch mit privaten Organisationen. Auf diese Weise soll die Resilienz der Niederlande im digitalen Bereich insgesamt erhöht werden. Zielsetzung ist, durch Wissensaustausch und die Bereitstellung von Erkenntnissen und angemessenen Handlungsmöglichkeiten eine sichere, offene und stabile Informationsgesellschaft zu verwirklichen. Um Cyber-Attacken vorzubeugen, konzentriert sich das NCSC nicht nur auf die Infrastruktur einer Organisation, sondern auch auf ihre Abhängigkeiten innerhalb einer Prozesskette. Der Hafen von Rotterdam (Europas größter Seehafen) zum Beispiel ist ein komplexes Netzwerk verschiedener Organisationen mit jeweils eigener Cyber-Infrastruktur. Durch seinen Fokus auf die komplette Prozesskette kann das NCSC Sicherheitslücken erkennen und so das gesamte Netzwerk stärken – denn eine Kette ist immer nur so stark wie ihr schwächstes Glied.

In den letzten sechs Jahren hat das NCSC bei der Prävention und Reaktion auf Cyber-Angriffe große Fortschritte gemacht. Ein gutes Beispiel ist der Ausbau des National Detection Network (NDN). Öffentliche und private Organisationen tauschen in diesem Rahmen Informationen aus, um digitale Gefahren und Risiken besser und schneller zu erkennen. Im Rahmen ihrer eigenen Verantwortung können die einzelnen Parteien dann rechtzeitig geeignete Maßnahmen ergreifen, um mögliche Schäden zu begrenzen oder zu verhindern. So arbeiten alle Hand in Hand, um die digitale Resilienz der Niederlande zu stärken.

Auf welche Hauptaufgaben konzentriert sich Ihre Organisation heute?

Die Hauptaufgabe des NCSC ist und bleibt der Fokus auf IT-Bedrohungen und Cyber-Sicherheitsvorfälle. Das Sammeln von – automatischen – Bedrohungs- und Ereignisinformationen von unseren Partnern im öffentlichen und privaten Sektor ist ein wichtiger Ansatz, um die Resilienz der niederländischen Gesellschaft im digitalen Bereich zu erhöhen. Daher konzentrieren wir uns auch weiterhin auf die Zusammenarbeit mit diesen Organisationen, aber auch auf die Kooperation mit unseren internationalen (CERT) Partnern, wie dem BSI.

Wie sehen die nächsten Schritte in der Entwicklung Ihrer Organisation aus?

Kernaufgabe des NCSC ist die Zusammenarbeit mit öffentlichen und privaten Organisationen. Dabei geht es um zahlreiche und in vielen Fällen sehr unterschiedliche Cyber-Bedrohungsinformationen. Eine wichtige Aufgabe des NCSC ist es, so viele nützliche Informationen wie möglich zu sammeln, zu ergänzen und zu verteilen, damit

„Ich würde es eine Premium-Partnerschaft nennen."

die Beteiligten ihre Cyber-Sicherheit auf Basis der neuesten Trends verbessern können. So kann ein Vorfall in einer Organisation als gute Warnung für andere dienen.

Der nächste Schritt wird sein, den Informationsaustausch und die bestehende Zusammenarbeit strukturell zu gewährleisten und gleichzeitig das Angebot zu erweitern, beispielsweise durch die Förderung sektorübergreifender Analysen. Bei Behörden und Anbietern kritischer Dienste besteht zum Beispiel noch Verbesserungsbedarf bei den Fähigkeiten zur Detektion und Reaktion. Indem wir daran arbeiten, können wir die digitalen Möglichkeiten dieser Organisationen insgesamt erhöhen.

Wie arbeitet das NCSC mit anderen Agenturen und Interessengruppen auf nationaler und internationaler Ebene zusammen?

Die Cyber-Sicherheit ist zu komplex, um von einem einzigen Bereich verwaltet zu werden. In der digitalen Welt sind IT-Strukturen heute eng miteinander verknüpft. Daher ist Zusammenarbeit auf operativer, taktischer und strategischer Ebene unerlässlich. Die Cyber-Sicherheit betrifft alle Bereiche einer Gesellschaft und für eine angemessene Reaktion müssen die Beteiligten wissen, wie sie sich gegenseitig schnell finden können. Eine gleichberechtigte und vertrauensvolle Zusammenarbeit ist daher ein wesentlicher Grundsatz des NCSC bei der engen Zusammenarbeit mit öffentlichen und privaten Organisationen. Unser Schwerpunkt liegt dabei vor allem auf Bereichen, die für die Gesellschaft entscheidend sind: die sogenannten Kritischen Infrastrukturen. Dazu gehören Energieunternehmen, Telekommunikation und der Finanzsektor. Wir konzentrieren uns auf individuelle Kontakte, die Beteiligung an Information Sharing and Analysis Centres (ISACs) und auf die Zusammenarbeit mit unseren sogenannten „Liaisons". Letztere dienen als wichtige Anlaufstelle für unsere Organisation und unsere Partner. Darüber hinaus arbeiten wir eng mit Fachleuten aus dem Bereich Cyber-Sicherheit sowie mit Experten aus dem Bildungs- und Hochschulbereich zusammen. International ist unser Netzwerk breit gefächert. Durch die bilaterale Zusammenarbeit mit unseren CERT-Partnern und internationalen Netzwerken wie dem International Watch and Warning Network (IWWN) behält das NCSC einen aktuellen Überblick über mögliche Bedrohungen weltweit.

Wie beurteilen Sie die Zusammenarbeit zwischen NCSC-NL und BSI?

Ich würde es eine Premium-Partnerschaft nennen. NCSC-NL und BSI arbeiten in verschiedenen Bereichen eng zusammen. Das betrifft sowohl die operative Zusammenarbeit als auch die Entwicklung von Maßnahmen, und zwar nicht nur bilateral, sondern auch im Rahmen der EU und international wie in der Kooperationsgruppe zur NIS-Richtlinie sowie im EGC und im CSIRT-Netzwerk. Deutschland ist ein wichtiger strategischer Partner und da es immer Raum für Verbesserungen gibt, stehen wir in engem Kontakt, um unsere Zusammenarbeit weiter zu stärken. Wir sind gleichgesinnte Länder und deshalb ist es gut, auf europäischer Ebene zum Beispiel bei der Reaktion auf mögliche Cyber-Krisen, beim Aufbau von Kapazitäten und bei Übungen intensiver zusammenzuarbeiten. Durch die Geschwindigkeit, mit der sich der Bereich der Cyber-Sicherheit entwickelt, und unsere grenzüberschreitenden Verflechtungen gibt es viele Bereiche, auf denen wir unsere Zusammenarbeit verstärken können, unter anderem bei öffentlich-privater Zusammenarbeit, Zertifizierung und Cloud.

Die Niederlande und Deutschland sind hinsichtlich Größe und Regierungsstruktur sehr unterschiedlich. Wo sehen Sie Gemeinsamkeiten hinsichtlich der Cyber-Sicherheit und der allgemeinen Situation? Wo sehen Sie die wesentlichen Unterschiede?

Unsere Kultur, Ansichten und Ansätze sind große Gemeinsamkeiten, die zur engen Zusammenarbeit zwischen NCSC-NL und BSI beitragen. Die Unterscheidung zwischen CERTs und NCSC-Aufgaben und die Unabhängigkeit von den Nachrichten- und Sicherheitsdiensten sind ebenfalls Gemeinsamkeiten unserer staatlichen Strukturen. Der Hauptunterschied besteht in der relativen Autonomie der deutschen Bundesländer, die jeweils ihre eigenen Zuständigkeiten und CERTs haben. Das BSI hat hier ein übergreifendes Mandat und eine zentralere Position in Deutschland. Das ist ein Unterschied zur niederländischen Regierungsstruktur, da die Niederlande nicht nur ein kleineres Land sind, sondern auch nur ein einziges nationales CERT haben. Bisher war unser NCSC eng mit der Direktion für Cyber-Sicherheit verbunden. Ab 2019 wird das NCSC-NL jedoch eine unabhängigere Position einnehmen und sich auf ein ähnlicheres Modell wie die deutsche BSI-BMI-Struktur zubewegen. Wir sind überzeugt, dass ein enges Verhältnis zwischen operativen und politischen Elementen wichtig ist, bei dem beide als Partner agieren. Die deutsche BSI-BMI-Struktur ist ein solches Beispiel, das wir sehr schätzen.

Was sind die zukünftigen Trends in der Cyber-Sicherheit, auf die sich das NCSC-NL national vorbereitet?

Die digitale Resilienz der Niederlande ist nach wie vor ein Problem. Nicht alle Organisationen ergreifen grundlegende

„NCSC-NL und BSI arbeiten in verschiedenen Bereichen eng zusammen.“

Kurzprofil Hans de Vries

Hans de Vries ist seit 2002 für die Zentralregierung tätig, zuletzt im Ministerium für Inneres und Königreichsbeziehungen, wo er als Leiter der Abteilung ICT-Management und Leiter der Koordination des operativen Managements tätig war. In den letzten Jahren hat er im Bereich der IKT-Sicherheit auf interministerieller und internationaler Ebene gearbeitet.

Maßnahmen, um Cyber-Angriffe zu verhindern. So können auch ohne ausgeklügelte Methoden wertvolle Informationen oder Daten gestohlen werden. Vor dem Hintergrund, dass die zunehmende Komplexität der niederländischen IT-Landschaft eine große Herausforderung für uns ist und sein wird, ist das für uns ein wichtiges Thema. In unserer kürzlich veröffentlichten National Cyber Security Agenda (NCSA) haben wir Maßnahmen festgelegt, um solchen zukünftigen Trends zu begegnen. Dazu gehört unter anderem ein landesweites Netzwerk mit Cyber-Sicherheitspartnerschaften, in dem öffentliche und private Parteien Informationen zur Cyber-Sicherheit austauschen können. In diesem Zusammenhang fördern wir die Einrichtung und Weiterentwicklung von Partnerschaften, wie die ISACs, regionale und sektorale CERTs und regionale Cyber-Sicherheitsinitiativen innerhalb einer Region oder eines wirtschaftlichen Ökosystems. Ein solches Netzwerk stärkt die Fähigkeiten sowohl öffentlicher als auch privater Organisationen in den Niederlanden und trägt dazu bei, die Niederlande auf zukünftige Trends in der Cyber-Sicherheit vorzubereiten.

Auf welche zukünftigen Trends in der Cyber-Sicherheit bereitet sich das NCSC-NL international vor?

Es ist kein Geheimnis, dass staatliche Stellen heute mehr digitale Spionage betreiben und Sabotageangriffe auf Organisationen weltweit zumindest vorbereiten. Sicherheitslücken in der IT-Infrastruktur ermöglichen Angriffe und mehrere Vorfälle zeigen, dass Abhängigkeiten innerhalb von Ökosystemen und Lieferketten ein erhebliches Risiko für die digitale Sicherheit darstellen. Um diesen Entwicklungen Rechnung zu tragen und die Cyber-Resilienz zu stärken, ist eine Zusammenarbeit zwischen den Ländern erforderlich. Das im September 2017 angekündigte Cyber-Paket der EU, unter anderem mit der NIS-Richtlinie und dem Konzept für eine schnelle Notfallreaktion, bietet hier eine Möglichkeit.

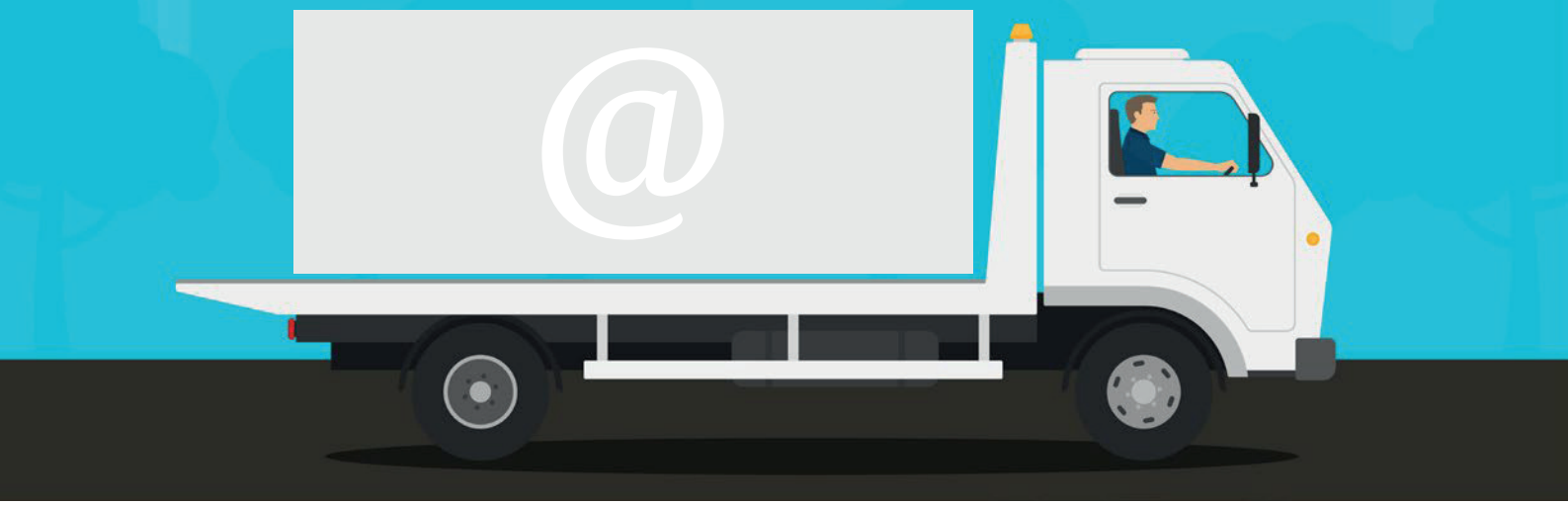
Was müssen Ihrer Meinung nach die nächsten Schritte sein, um die Cyber-Sicherheit in Europa weiter zu verbessern?

Die Niederlande unterstützen eine intensive Zusammenarbeit bei der Cyber-Sicherheit in Europa und hoffen, diese gemeinsam mit Deutschland weiter zu verbessern. Insbesondere im Hinblick auf das CSIRT-Netzwerk ist eine intensive Zusammenarbeit erforderlich. Zielsetzung ist, das Netzwerk weiter zu professionalisieren und zu entwickeln, um die gesamte europäische Zusammenarbeit zu fördern und zu unterstützen. Die zunehmende Bedrohung durch staatliche und nicht staatliche Akteure im digitalen Bereich und die zunehmende Abhängigkeit der Bürger von diesen Technologien erfordern eine weitere Verbesserung der Cyber-Sicherheit in Europa. Maßnahmen wie die Zertifizierung von IoT-Produkten in Europa, wie sie von einem niederländischen Abgeordneten im März 2018 initiiert wurde, gehören zu den Themen, die weiter diskutiert werden sollten. Der deutsche Zertifizierungsansatz bietet hier einige interessante Beispiele, auf denen wir sowohl im niederländischen als auch im europäischen Kontext aufbauen können.

Weitere Informationen: https://www.ncsc.nl

Sicherer E-Mail-Transport für Europa

Europa übernimmt Vorreiterrolle



von Florian Bierhoff, Referat Cyber-Sicherheit für die Digitalisierung von IoT mit Smart Services

Trotz der wachsenden Bedeutung von (mobilen) Instant Messengern bleibt die E-Mail ein bedeutendes Medium zum Austausch von Nachrichten in der digitalen Kommunikation. Speziell im Businessbereich erfreut sie sich nach wie vor großer Beliebtheit. Durch intensive europäische Zusammenarbeit soll die Sicherheit bei der E-Mail-Kommunikation erhöht und die Verbreitung moderner Sicherheitsstandards gefördert werden. Europa kann hierbei eine Vorreiterrolle bei der nachhaltigen Steigerung der Cyber-Sicherheit einnehmen.

Das BSI hat bereits 2015 mit dem Vorhaben zur Technischen Richtlinie (TR) „Sicherer E-Mail-Transport (BSI TR-03108)“ begonnen, Basissicherheitsanforderungen an den Transport von E-Mails zu definieren und damit zur weiteren Verbreitung sicherer E-Mail-Technologien beizutragen.

Der Fokus wurde auf Technologien gelegt, die ausschließlich vom E-Mail-Diensteanbieter (EMDA) umgesetzt werden müssen und somit auch ohne ein Zutun der Nutzer ihren sicherheitstechnischen Mehrwert entfalten. Dieser ergibt sich vor allem aus der konsequenten Verwendung bereits in der Praxis erprobter und etablierter Standards. Neben BSI-eigenen Standards, wie den TR zu kryptografischen Vorgaben für Projekte der Bundesregierung (BSI TR-03116-4) und zum sicheren Betrieb von Zertifizierungsstellen (BSI TR-03145), spielen in diesem Zusammenhang einige internationale Standards eine tragende Rolle.

Besonders positiv wurde in der Öffentlichkeit die Verwendung von DNS-Based Authentication of Named Entities (DANE) in der Verbindung mit DNSSEC aufgenommen. Dieser Standard ermöglicht es Internet-Diensteanbietern, ihre für die Authentisierung und Verschlüsselung notwendigen Zertifikate über die Veröffentlichung auf DNS-Servern bekannt und abrufbar zu machen. Mithilfe der über DANE bereitgestellten Zertifikate kann jeder, der mit einem Diensteanbieter kommunizieren möchte, die Verbindung verschlüsseln und authentisieren. Zudem ist die Nutzung von DANE ein verbindliches Statement, dass der Diensteanbieter in der Lage ist, eine verschlüsselte Verbindung anzubieten. Auch das BSI bietet seine Dienste schon seit einiger Zeit mit DANE und DNSSEC abgesichert im Internet an.

Internetverbindungen, die mithilfe von Transport Layer Security (TLS) abgesichert werden, genießen im Gegensatz zu DANE schon jetzt weite Verbreitung. Sicherheitslücken, wie BEAST oder Poodle, haben gezeigt, dass für die Sicherheit vor allem der Einsatz zeitgemäßer Kryptoverfahren von essenzieller Bedeutung ist. Das BSI veröffentlicht aus diesem Grund jährlich und anlassbezogen aktualisierte kryptografische Vorgaben, die ebenfalls beim sicheren E-Mail-Transport angewandt werden. Durch die Kombination von DNSSEC zur sicheren Abfrage beim DNS-Server, DANE zum Abruf und zur Bereitstellung von Zertifikatsinformationen und durch den Einsatz von sicheren Algorithmen bei TLS wird mithilfe von Standard-Technologien ein Basissicherheitsniveau nach dem aktuellen Stand der Technik erreicht.

TRAGFÄHIGES KONZEPT

In Verbindung mit den Anforderungen an das vom EMDA verpflichtend zu erstellende Sicherheitskonzept und den in Europa geltenden hohen Anforderungen an den Datenschutz ergibt sich damit ein tragfähiges Konzept. Dieses adressiert die Sicherheit einer E-Mail vom Sender bis zum Empfänger auf operativer und technischer Ebene. Dabei wird die Übertragung der E-Mail jeweils von Punkt-zu-Punkt abgesichert. Diese lässt sich bei Bedarf jederzeit um Ende-zu-Ende-Sicherheit, z. B. durch die Nutzung von PGP oder S/MIME, auf der Anwendungsebene ergänzen. Zudem werden bei dieser Kombination auf Transportebene zusätzlich die Verbindungsdaten aus dem E-Mail-Header, wie Informationen zum Sender und Empfänger der E-Mail, verschlüsselt.

Ergänzend zu der Technischen Richtlinie wurde vom BSI ein Zertifizierungsverfahren etabliert, das auf Basis von Prüfspezifikationen von geprüften Auditoren durchgeführt wird. Durch dieses Verfahren wird die Sicherheit von E-Mail-Diensten nachweisbar und vergleichbar. Bereits 2016 konnte das erste Zertifikat an einen EMDA vergeben werden. Für die Zertifizierung müssen die prüfenden Auditoren für eine bei der DAkkS (Deutsche Akkreditierungsstelle GmbH) akkreditierte Prüfstelle tätig sein und erfolgreich eine Zertifizierung als Auditor im Bereich „Sicherer E-Mail Transport“ beim BSI durchlaufen haben. Diese sogenannte Personenzertifizierung beinhaltet neben dem Nachweis der Fachexpertise auch den Nachweis über den korrekten Umgang mit den vom Auditor gewählten Prüftools. Dies wird bei der beispielhaften Prüfung eines fiktiven E-Mail-Diensteanbieters (EMDA) in einer virtuellen Umgebung beim BSI nachgewiesen.

EINE EUROPÄISCHE CHANCE

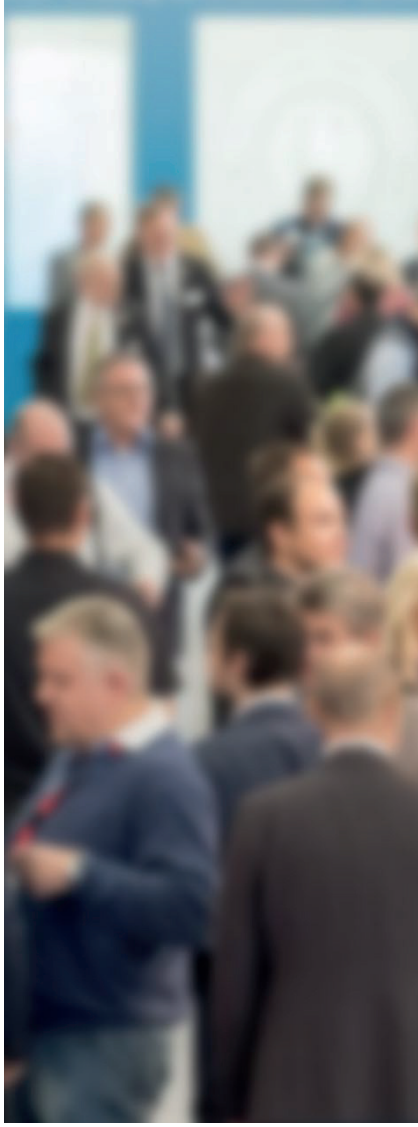
Schon im Rahmen der TR-Erstellung fanden Abstimmungsgespräche mit europäischen Partnerbehörden des BSI statt. Dabei stellte sich heraus, dass es auch in anderen Ländern ähnliche Ansätze gab, die Transportsicherheit zu erhöhen. Sie lagen inhaltlich nah beieinander, unterschieden sich jedoch in der Methodik. So gibt es in Frankreich eine, von der Agence nationale de la sécurité des systèmes d’information (ANSSI) erstellte, Charta zur E-Mail-Sicherheit, die von Regierungsvertretern und Vertretern der fünf größten EMDAn in Frankreich unterzeichnet wurde. In den Niederlanden wurde vom Nationaal Cyber Security Centrum (NCSC) ein Fact Sheet zu dem Thema veröffentlicht, welches für niederländische Behörden auf allen Ebenen nach der Comply-or-Explain-Methodik (sinngemäß: erfülle oder erkläre, warum du nicht erfüllst) verbindlich ist.

Um diese Kompetenzen in Zukunft zu bündeln und möglichst geschlossen auf dem Markt, z. B. gegenüber E-Mail-Softwareherstellern, auftreten zu können, haben die Niederländische NCSC und das BSI am 8. Juni 2018 Vertreter europäischer Behörden, der Kommission sowie Industrievertreter zu einem gemeinsamen Workshop nach München eingeladen. Hierbei stand, neben einem Erfahrungsaustausch zu den Standards und Technologien, die Abschätzung des Potenzials einer weiteren Zusammenarbeit im Vordergrund. Diese Initiative wurde auch von der Europäischen Agentur für Netz-und Informationssicherheit (ENISA) begrüßt, die für die weitere Zusammenarbeit ihre Unterstützung zugesichert hat. Auf diese Weise soll Schritt für Schritt die Sicherheit bei der E-Mail-Kommunikation erhöht und die Verbreitung moderner Sicherheitsstandards gefördert werden. Europa kann hierbei eine Vorreiterrolle bei der nachhaltigen Steigerung der Cyber-Sicherheit im Bereich der E-Mail einnehmen. ■

Technische Richtlinie03108:
https://www.bsi.bund.de/TR03108

Zertifizierung als Auditor „Sicherer E-Mail Transport“ für BSI TR-03108:
https://www.bsi.bund.de/auditor-emailtransport

ViS!T-Symposien



Drei Länder, eine Idee

EINE IDEE WIRD REALITÄT

Seit nunmehr 16 Jahren treffen sich Mitarbeiter der öffentlichen Verwaltung aus Deutschland, Österreich und der Schweiz (seit 2010 auch aus Luxemburg) im Abstand von jeweils 24 Monaten zum ViS!T-Symposium. Das Akronym steht für „Verwaltung integriert sicher Informationstechnologie“ und referiert eine ebenso einfache wie einleuchtende Idee: Die Sicherheitsherausforderungen an die öffentliche Verwaltung sind eigentlich in allen Ländern mehr oder weniger die gleichen. Man setzt ähnliche Infrastrukturen ein, hat dezentralisierte Verwaltungseinheiten zu betreuen und muss neue Technologien (PKI, Server-Infrastrukturen, Arbeitsplatzsysteme mit größerer Rechnerkapazitäten etc.) sicherheitsseitig integrieren.

Naheliegend also, darüber Informationen auszutauschen, über praktische Erfahrungen zu berichten und anhand von Projektergebnissen aufzuzeigen, wie die unterschiedlichsten Anwendungen und Technologien die Verwaltungen bzw. deren Mitarbeiter unterstützen können. Und natürlich sich gegenseitig kennenzulernen. So entstand 2001 auf dem 7. Deutschen IT-Sicherheitskongress in Bonn die gemeinsame Idee „ViS!T“.

WAS DARAUS GEWORDEN IST

Daraus entstand eine Erfolgsgeschichte, die bis heute anhält. Das erste Symposium fand am 20./21. Juni 2002 im Technischen Museum von Wien statt. Symbolträchtig, da sich so durch den Tagungsort moderne IT-Technologie mit Geschichte verband. Rund 100 Mitarbeiter aus den verschiedenen Verwaltungen der drei deutschsprachigen europäischen Länder Deutschland, Österreich und der Schweiz nahmen an der Tagung teil. Interessante Vorträge vermittelten einen ersten guten Überblick über den Stand der eingesetzten IT-Sicherheitsmethoden in den drei Ländern und machten die Tagung zu einem Erfolg.

Was nicht zuletzt auch daran sichtbar wird, dass die Veranstaltung von nun an alle zwei Jahre alternierend in den beteiligten Ländern durchgeführt wurde. Jedes Symposium steht dabei unter einem Leitgedanken.

2004 fand ViS!T in Bern statt. „Mensch und Technik“ sollte als Leitgedanke die Vielfältigkeit der Herausforderungen an die IT und die IT-Sicherheit zeigen, und viele Vorträge konnten dies an konkreten Anwendungen sehr gut aufzeigen.

2006 konnte das Symposium in Bonn durchgeführt werden. Der Leitgedanke war „Vernetzte Identitäten – Herausforderung an die öffentliche Verwaltung“. Die Beiträge legten umfassend dar, wie die Anwendungen in den beteiligten Ländern konkret aussahen.

Zwei Jahre später waren wiederum die österreichischen Kollegen mit der Organisation betreut. Dieses Symposium wurde zusammen mit einer E-Government-Konferenz in Mautern an der Donau durchgeführt. Durch die Verbindung

konnten den Teilnehmern sehr interessante Einblicke in artverwandte Themen gegeben werden.

Beim folgenden Symposium, 2010 in Bern, wurden die Teilnehmer durch den Leitgedanken aufgefordert, den Blick nach vorn zu richten: Wohin entwickelt sich die Informations- und Kommunikationstechnologie (IKT) der öffentlichen Verwaltung in den nächsten zehn Jahren, unter besonderer Berücksichtigung der immer wichtiger werdenden Sicherheitsaspekte? Wie arbeiten und kommunizieren wir im Jahr 2020? Im Rückblick kann dabei festgestellt werden, dass sich durch die sich enorm schnell verändernde IKT-Landschaft viele der damals prognostizierten Aspekte nicht nur realisiert, sondern bereits übertroffen wurden (Entwicklungen von Apps, Bezahlsystemen mit dem Mobiltelefon etc.).

AUS DREI MACH VIER

An dieser Tagung nahmen zum ersten Mal auch Kollegen aus Luxemburg teil. Das führte dazu, dass sie sich bereiterklärten 2012 die Tagung in Luxemburg auszurichten. Seither besteht der Kreis der beteiligten deutschsprachigen Länder aus Deutschland, Österreich, Luxemburg und der Schweiz.

2014 war wiederum Österreich mit der Organisation an der Reihe (http://visit.a-sit.at/index.html) und 2016 fand das Symposium wieder in Bern statt (www.visit.isb.admin.ch). Nun richtete sich der Fokus weg von der projektorientierten Darstellung der technologischen Umwälzungen hin zu Umsetzung sowie Erfahrungen der Benutzer.

Ein Ende ist nicht in Sicht. Denn dieses Jahr kommt das ViS!T-Symposium wieder einmal nach Deutschland. Es wird durch das BSI organisiert und findet findet während der it-sa vom 8. Bis 9. Oktober 2018 in Nürnberg statt. Hier wird es um die Chancen der Digitalisierung gehen, um technische Visionen und künftige Entwicklungen, um den Datenschutz und die DSGVO, sowie um Behörden in der Cloud. ■

Weitere Informationen: https://www.bsi.bund.de/visit2018

KRITIS in Europa

BSI engagiert sich in Europa für den Schutz Kritischer Infrastrukturen

Kritische Infrastrukturen (KRITIS) machen in der Regel nicht an den Staatsgrenzen halt. KRITIS-Betreiber sind häufig international aktiv und erbringen ihre kritischen Dienstleistungen grenzüberschreitend. Sicherheitsmaßnahmen und Regularien sollten daher in der EU auf ein vergleichbares Niveau gebracht werden.

von Simplice Roger Bekono, Referat Kritische Infrastrukturen - Grundsatz

Im europäischen Umfeld gilt das BSI als kompetenter und strategischer Partner in Sachen Informationssicherheit. Es bringt sich seit vielen Jahren mit seiner Expertise unter anderem in EU-Gremien und Arbeitsgruppen ein. So engagierte sich das BSI bereits seit 2006 im Rahmen des „Europäischen Programms für den Schutz Kritischer Infrastrukturen (EPSKI)". Rund zehn Jahre später wurde mit der Richtlinie 2016/1148 des Europäischen Parlaments und des Rates vom 06.07.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie) ein Meilenstein beim Schutz der Kritischen Infrastrukturen innerhalb der EU geschaffen (siehe auch BSI-Magazin 01/2018).

Bei der Ausgestaltung und Umsetzung dieses Rechtsaktes beteiligt sich das BSI aktiv auf europäischer Ebene, insbesondere durch die Mitarbeit in den beiden neu geschaffenen Gremien, der Kooperationsgruppe („Cooperation Group") und dem CSIRTs-Netzwerk (Computer Security Incident Response Teams Network).

CSIRTS-NETZWERK

Das Netzwerk besteht aus CSIRT-Vertretern der 28 Mitgliedstaaten und des CERT-EU („Computer Emergency Response Team" für die EU-Institutionen). Das BSI wird durch das CERT-Bund vertreten. Das Netzwerk hat nach Maßgabe der Richtlinie folgende Aufgaben:

- Austausch über Meldungen von KRITIS-Betreibern
- Gegenseitige Unterstützung bei der Reaktion auf grenzüberschreitende Vorfälle
- Koordinierte Reaktion auf festgestellte Vorfälle

Die Zusammenarbeit und der Austausch des Netzwerks waren bislang gut. Insbesondere während der Angriffe mit WannaCry und NonPetya war die Zusammenarbeit besonders intensiv. Täglich wurden länderspezifische Lageübersichten bereitgestellt. So konnten auch täglich Zusammenfassungen über die aktuellen Entwicklungen in Europa abgerufen werden.

Für den operativen Informationsaustausch wird von den CSIRTs neben Mailinglisten und Chat-Kanälen auch eine Kooperationsplattform genutzt. Perspektivisch bietet ein Netzwerk operativ stark aufgestellter CSIRTs dem BSI und den Kritischen Infrastrukturen einen deutlichen Mehrwert.

COOPERATION GROUP

Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der EU-Kommission und der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) zusammen. Ihre Rolle besteht darin, die Mitgliedstaaten bei deren strategischer Zusammenarbeit zu unterstützen. KRITIS-Betreiber und Anbieter digitaler Dienste können zu Beratungen der Kooperationsgruppe

eingeladen werden. Die Gruppe arbeitet auf der Grundlage von zweijährigen Programmen.

Das BSI beteiligt sich unter Federführung des Bundesinnenministeriums (BMI) mit diversen Fachexperten an verschiedenen Arbeitsgruppen (AG) der Kooperation. In der AG „Identifizierung von KRITIS-Betreibern" hat Deutschland den Vorsitz. Da bereits früh im Rahmen des IT-Sicherheitsgesetzes 2015 der Schutz Kritischer Infrastrukturen in den Fokus genommen wurde, hat Deutschland bei der Identifizierung von KRITIS-Betreibern einen Vorsprung gegenüber vielen anderen EU-Staaten. Die in Deutschland gemachten Erfahrungen bei der Umsetzung der gesetzlichen Regelungen werden daher in die Diskussion auf europäischer Ebene eingebracht.

Die qualitative und quantitative Ermittlung von KRITIS-Betreibern wurde mit der BSI-Kritisverordnung (BSI-KritisV) konkretisiert. Dabei wendete das BSI die „Methode zur Identifizierung Kritischer Infrastrukturen (MIKI)" an, die vom BSI zusammen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) entwickelt wurde. Mit MIKI werden Anlagenkategorien im Bereich der kritischen Dienstleistungen ermittelt und quantitative Kriterien für die Berechnung von Schwellenwerten definiert. Diese Methodik wurde vom BBK verallgemeinert und 2017 veröffentlicht.

Die Identifizierung von KRITIS-Betreibern durch die BSI-KritisV ist das Ergebnis eines kooperativen Ansatzes zwischen BMI, BSI, BBK, den Fachressorts, den Aufsichtsbehörden sowie Wirtschaftsvertretern aus den entsprechenden Branchenarbeitskreisen des UP KRITIS. Der kooperative Ansatz Deutschlands hat in anderen EU-Ländern für viel Aufmerksamkeit gesorgt, auch weil sich durch ihn Konflikte zwischen Staat und Wirtschaft vermeiden lassen. Eine vertrauensvolle Zusammenarbeit ist zudem eine belastbare und effektive Basis für den Schutz Kritischer Infrastrukturen.

INTERNATIONALE WIRKUNG DER NIS-RL

Gemäß Art. 13 der NIS-RL kann die EU mit Drittländern oder internationalen Organisationen internationale Übereinkünfte treffen, um deren Beteiligung an bestimmten Tätigkeiten der EU zu ermöglichen. So haben Kanada und die USA 2018 am 8. europäischen Expertentreffen zum Schutz Kritischer Infrastrukturen teilgenommen.

Die EU-Kommission und die Regierungen der USA und Kanadas werden weiter zusammenarbeiten, um die Sicherheit der Kritischen Infrastrukturen zu erhöhen. Aufgrund der Abhängigkeiten zwischen den Volkswirtschaften und nationaler Interessen sollen auch in Zukunft Erfahrungen ausgetauscht, gemeinsame Forschung betrieben und Übungen organisiert werden. In den USA werden ähnlich wie in Deutschland Regelungen in Form von Standards getroffen, die zusammen mit gesamtstaatlichen, föderalen und Standardisierungsstellen erarbeitet werden. ■

Weitere Informationen:
Methode zur Identifizierung Kritischer Infrastrukturen:
https://www.bbk.bund.de/SharedDocs/Kurzmeldungen/BBK/DE/2017/Publikation_Schutz_Kritis_Identifizierung_sieben_Schritte.html

CYBER-SICHERHEIT

Im Visier

Cyber-Angriff auf die deutschen Hidden Champions

von Joachim Gutmann

Rund 60 Prozent aller heimlichen Weltmarktführer, die sogenannten Hidden Champions, sitzen in Deutschland. Und in einem Dilemma: Einerseits schreitet auch bei ihnen die Digitalisierung der Verfahren und Prozesse ständig voran, andererseits hält die personelle und finanzielle Ausstattung der IT nicht damit Schritt. In dieses Delta stoßen Cyber-Kriminelle und Wirtschaftsspione verstärkt vor.

Am Ende konnte Valentin Stalf, Gründer und CEO der in Berlin ansässigen Direktbank N26, erleichtert sein: Sicherheitslücke geschlossen, Geschäftsmodell gerettet. Staffs 2013 als Papayer GmbH gegründetes ehemaliges Fintech-Start-up bietet ein für das Smartphone optimiertes Girokonto an, das sich komplett per App eröffnen und verwalten lässt. Alle Transaktionen lassen sich innerhalb von Sekunden in der App einsehen und werden dem Kunden per Push-Mitteilung angezeigt. Ein innovatives, aber mit erheblichem Sicherheitsrisiko verbundenes Konzept.

Was deutlich wurde, als der Sicherheitsforscher Vincent Haupert auf dem 33C3-Kongress in Hamburg 2017 erklärte, wie es ihm mithilfe von Schwachstellen in der N26-Programmierschnittstelle sowie einem zu freigiebigen Kundensupport möglich gewesen war, Kundendaten auszulesen. Auch Überweisungen ohne Authentifizierung und Wissen der Kontoinhaber hätte er anweisen können. „Die Sicherheitslücke wurde zum Glück von keinem Angreifer ausgenutzt, hätte jedoch schwerwiegende Folgen haben können, weil N26 eine eigene Banklizenz besitzt“, erklärt Stalf. N26 reagierte umgehend mit der Behebung der Schwachstellen und der Einrichtung eines Bug-Bounty-Programms.

NICHTS GEHT OHNE IT

Auch kleine und mittelständische Unternehmen (KMU) sind auf die Informationstechnologie angewiesen. Sie ist ein wichtiges Hilfsmittel für geschäftsrelevante Prozesse: Das Internet ist für die Kommunikation mit Kunden und Lieferanten unverzichtbar, die Produktionsanlagen werden von Computern gesteuert, Hersteller und Wartungsfirmen haben ungehindert Zugriff auf die interne IT-Infrastruktur. Leider häufig auch Cyber-Kriminelle. Und das ist ein zunehmendes Problem. Wenn ein Erpressungstrojaner mehrere Tage oder Wochen die gesamte Produktionslinie lahmlegt oder sämtliche Kundendaten inklusive der Back-ups zerstört, hat dies sicherlich am Ende des Jahres Auswirkungen auf die Unternehmensbilanz. Kommt es noch schlimmer, verlieren vielleicht Menschen ihren Arbeitsplatz, nur weil es versäumt wurde, ein Software-Update zeitnah einzuspielen.

Hidden Champions, also insbesondere industrielle KMU mit dem Status Weltmarktführer für die von ihnen hergestellten Produkte, sind von Cyber-Kriminalität in besonderen Maße bedroht. Zum Fundament des Erfolgs dieser deutschlandweit rund 1.600 Hidden Champions gehören Faktoren wie Innovation, Produktqualität und Wirtschaftlichkeit, aber auch höchstes technisches Know-how, störungsfreie Produktionsprozesse sowie ein effizienter Einsatz von Ressourcen.

Gleichzeitig ist die IT-Sicherheit bei ihnen häufig wenig bis gar nicht gewährleistet. Bei manchem KMU ist noch Windows XP im Einsatz. Das 17 Jahre alte Betriebssystem wird seit 2016 von Microsoft nicht mehr unterstützt; es gibt keinen

„Die hohe Zahl der betroffenen Unternehmen macht deutlich, dass Cyber-Angriffe eine der größten Bedrohungen für den Erfolg der Digitalisierung in der Wirtschaft sind."

Arne Schönbohm, Präsident des BSI

Technik-Support und keine Aktualisierungen, wenn heute noch Sicherheitslücken bekannt werden. Eine davon wurde 2017 von der Erpressungssoftware „Wannacry" genutzt und führte weltweit zu Systemausfällen.

SCHLECHT GERÜSTET

Auch wenn der Mittelstand mittlerweile mehr in IT-Sicherheitsmaßnahmen investiert, sind viele Unternehmen weiterhin schlecht geschützt vor Hackerangriffen und Wirtschaftsspionage. Allein 2016 verursachten Cyber-Angriffe in Deutschland Schäden in zweistelliger Milliardenhöhe. „Die Angreifer verfügen über leistungsfähige und flexibel einsetzbare Angriffsmittel und verbessern ihre Methoden kontinuierlich", sagt Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI). Sorge bereiten auch immer mehr groß angelegte Cyber-Angriffe mit Schadsoftware, die Produktionsstraßen, Hafenanlagen, Bahnanzeigen und Reedereien lahmlegen.

Daneben versuchen Kriminelle auch, über Advanced Persistent Threats (APT) sukzessive in die IT-Infrastruktur der Opfer einzudringen, um über einen längeren Zeitraum möglichst sensible Informationen auszuspähen und dabei so lange wie möglich unentdeckt zu bleiben. Die Bedrohungslage durch APTs ist laut der Studie IT-Sicherheit 2017 des Internetwirtschaftsverbands eco für über 40 Prozent der befragten Security-Experten ein wichtiges oder sehr wichtiges Thema. „Die mittelständischen Hidden Champions sind beliebte Opfer, denn viele haben kein ausreichendes Risikomanagement und sind sich nicht wirklich bewusst, wie wertvoll die Informationen, Konstruktionspläne oder Formeln sind, die sie in ihrem Firmennetzwerk speichern", sagt Markus Schaffrin, Geschäftsbereichsleiter Mitgliederservices im eco – Verband der Internetwirtschaft e. V..

Auch der sogenannte CEO-Fraud nimmt zu. Eine (gefälschte) E-Mail mit Absenderadresse aus dem Unternehmen und korrekter Signatur fordert zu einer finanziellen Transaktion auf. So auch den Sanitärausstatter Franke Aquarotter in Ludwigsfelde (Teltow-Fläming). Kriminelle fingierten eine E-Mail eines angeblichen Vorgesetzten mit einer Zahlungsaufforderung in beträchtlicher Höhe. Geschäftsführer Oliver D. Gessert wurde skeptisch. Seine kritische Nachfrage bei der Schweizer Mutter vereitelte einen erfolgreichen Betrug. Leider nicht beim Nürnberger Kabelspezialisten Leoni AG. Dort nutzten die Täter gefälschte Dokumente und Identitäten sowie elektronische Kommunikationswege, um Mitarbeiter dazu zu bringen, Geld auf Konten im Ausland zu überweisen. Der Betrüger hatte sich gegenüber Kollegen als Leoni-Mitarbeiter ausgegeben und behauptet, besondere Befugnisse zu haben. So konnte er die Überweisungen auslösen.

Nach den Ergebnissen der Cyber-Sicherheits-Umfrage 2017, die das BSI im Rahmen der Allianz für Cyber-Sicherheit durchgeführt hat und an der rund 900 Unternehmen und Institutionen teilnahmen, sind knapp 70 Prozent der Befragten in den Jahren 2016 und 2017 Opfer von Cyber-Angriffen geworden. In knapp der Hälfte der Fälle waren die Angreifer erfolgreich und konnten sich zum Beispiel Zugang zu IT-Systemen verschaffen, die Funktionsweise von IT-Systemen beeinflussen oder Internet-Auftritte von Firmen manipulieren. Jeder zweite erfolgreiche Angriff führte dabei zu Produktions- bzw. Betriebsausfällen. „Die hohe Zahl der betroffenen Unternehmen macht deutlich, dass Cyber-Angriffe eine der größten Bedrohungen für den Erfolg der Digitalisierung in der Wirtschaft sind", meint darum BSI-Präsident Schönbohm. „Es zeigt sich, dass die umfangreichen Sensibilisierungsmaßnahmen des BSI als nationale Cyber-Sicherheitsbehörde Früchte tragen."

RISIKOFAKTOREN UND ABHILFE

Doch leider spielt der Bereich IT-Sicherheit bei vielen KMU noch immer eine Nebenrolle. Medienwirksame Vorfälle wie die Locky-Erpressungstrojaner-Welle oder die bekanntge-

„In vielen Köpfen hat bereits ein Wandel in der Wahrnehmung von IT-Sicherheit und ihrer Wertigkeit für den Unternehmenserfolg stattgefunden."

Patrick Smolka, Abteilungsleiter Financial Lines, HDI Global SE

wordenen Fälle des CEO-Fraud tragen jedoch dazu bei, dass sich vielleicht auch ein Geschäftsführer eines mittelständischen Unternehmens zu fragen beginnt, ob beim nächsten Mal vielleicht sein eigener Betrieb Opfer eines globalen Cyberangriffs werden kann.

KMU haben im Gegensatz zu großen Unternehmen häufig neben knappen personellen Ressourcen auch nur ein schmales IT-Budget. Die IT-Abteilung muss trotzdem die Grundfunktionalitäten der technischen Infrastruktur im gleichen Ausmaß bereitstellen. Hinzu kommt der Faktor Mensch. Fehlende Sensibilisierung im Hinblick auf IT-Sicherheitsrisiken und Einfallstore ist einer der Hauptgründe für Datendiebstahl und kompromittierte Systeme. Mitarbeitersensibilisierung, die Implementierung einer IT-Strategie und ein erreichbarer Maßnahmenplan sind daher zentrale Erfolgsfaktoren einer zukunftsstabilen Strategie für IT-Sicherheit.

Um mittelständische Unternehmen besser zu schützen, haben die Sicherheitsbehörden in Deutschland verschiedene Angebote entwickelt. „Wir bieten ihnen Rat und konkrete Handlungsempfehlungen an", sagt BSI-Präsident Schönbohm. „Dazu zählen die Angebote der Allianz für Cyber-Sicherheit ebenso wie der modernisierte, praxisorientierte IT-Grundschutz, aber auch die Kooperation mit den relevanten Wirtschaftsverbänden."

Patrick Smolka, Abteilungsleiter Financial Lines in der HDI Global SE, sieht erste Erfolge: „Wir stellen in unseren Gesprächen mit den Unternehmen ein stetig steigendes Bewusstsein für IT-Sicherheit fest. In vielen Köpfen hat bereits ein Wandel in der Wahrnehmung von IT-Sicherheit und ihrer Wertigkeit für den Unternehmenserfolg stattgefunden."

Viele Angriffsvektoren lassen sich bereits durch einfache Maßnahmen abfedern, zum Beispiel durch eine ordentliche Back-up-Strategie, ein vernünftiges Update- und Patch-Management oder die regelmäßige Sensibilisierung der eigenen Mitarbeiter für IT-Sicherheit und deren Schulung dazu. Am Anfang aller Überlegungen aber sollte ein strategisches Sicherheitskonzept stehen, das die wirklich wichtigen, schützenswerten Geschäftsprozesse, Daten und Systeme identifiziert. Ein solches Sicherheitskonzept darf nicht statisch sein, vielmehr muss es sich immer wieder den wechselnden Anforderungen an die Informationssicherheit anpassen. Gleichzeitig lässt sich auch die Angriffsfläche reduzieren, indem Systeme aktualisiert, Berechtigungen reduziert und Passwörter verstärkt werden.

Damit es gar nicht erst zum Ernstfall kommt: Denn wie bei einem „herkömmlichen" Einbruch in ein Gebäude oft der Schaden durch das Einbrechen selbst oder gar Vandalismus erheblich größer ist als die gestohlenen Wertsachen, so schadet der Hacker mit seinem Angriff neben dem eigentlichen Ziel häufig auch vielen „zufälligen" Opfern. ■

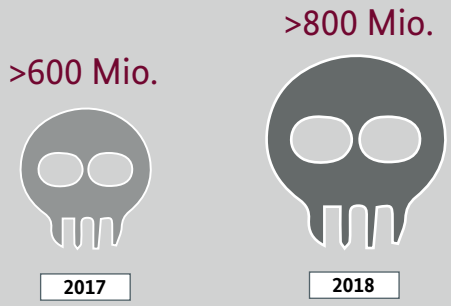
Das Jahr im Rückblick

Erkenntnisse aus dem BSI-Lagebericht 2018

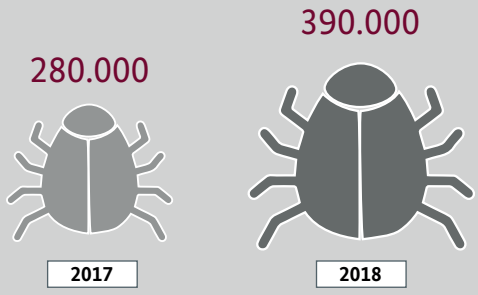
In seinem jährlichen Lagebericht gibt das BSI einen umfassenden Überblick über die IT-Sicherheit in Deutschland. Auf dieser Seite haben wir für Sie einige Ergebnisse des Lageberichts 2018 zusammengefasst. Dabei lässt sich feststellen: Die Bedrohungen durch kommerzielle Cyber-Kriminelle sind nicht nur größer geworden, sie haben auch ein neues Level erreicht.

BEDROHUNGEN IM NETZ

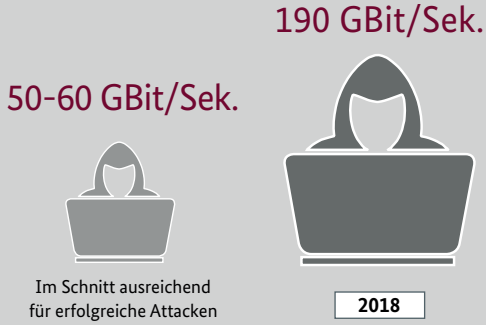
Schadprogramme im Umlauf



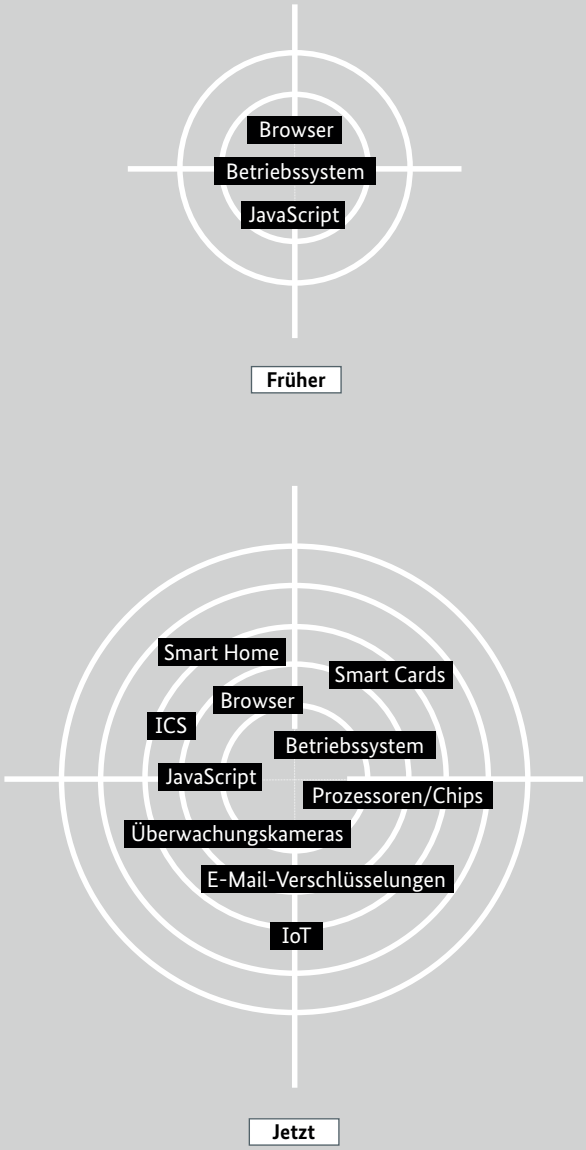
Neue Schadprogramm-Varianten pro Tag



Geschwindigkeit der Angriffe



FOKUS DER ANGRIFFE WIRD BREITER

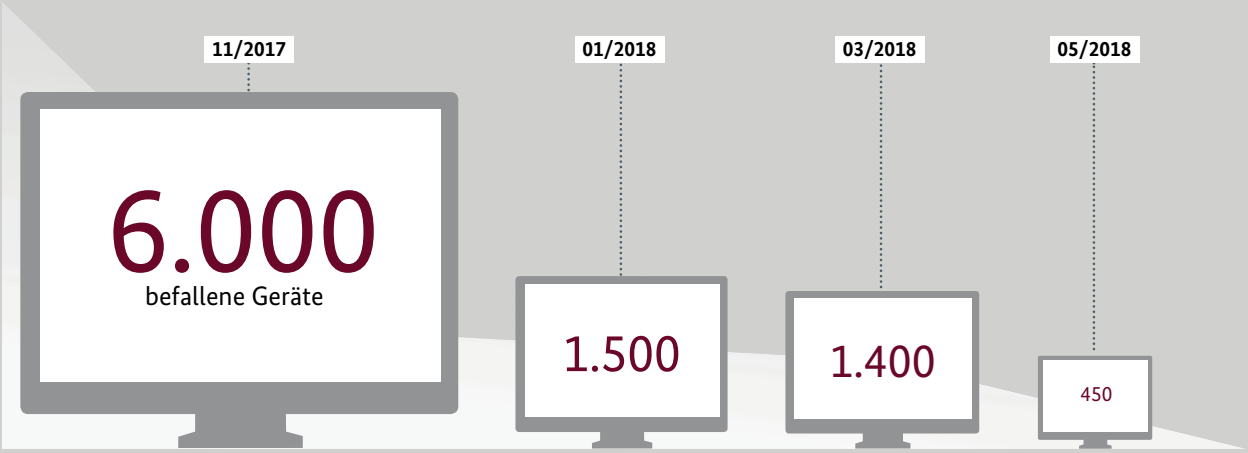


WARNUNGEN ZEIGEN WIRKUNG

Mehr als

16 Millionen Warn-Mails

hat das BSI verschickt, um auf Gefahrensituationen aufmerksam zu machen.



(Bsp: Cisco Smart Install; Die Zahl befallener Geräte sank von über 6.000 auf rund 450 nach regelmäßigen Warnungen durch das CERT-Bund des BSI an deutsche Netzbetreiber. Vgl. Lagebericht 2018, S. 85)

VERNETZTE ZUSAMMENARBEIT

Allianz für Cyber-Sicherheit

Mehr als

2.700 Institutionen

sind in der Allianz für Cyber-Sicherheit vernetzt, um das Niveau der Informationssicherheit im Unternehmen zu erhöhen und sich wirksam gegen Cyber-Bedrohungen zu schützen.

BSI FÜR BÜRGER
INS INTERNET - MIT SICHERHEIT

Mehr als

100.000 Bürger

lassen sich regelmäßig durch das BSI über Gefahren im Internet informieren.

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

Quelle: Bundesamt für Sicherheit in der Informationstechnik

Public-Key-Kryptografie zukunftssicher machen

Standardisierung quantencomputerresistenter Verfahren im NIST-Wettbewerb

von Dr. Heike Hagemeier, Dr. Stavros Kousidis, Dr. Manfred Lochter, Referat Kryptografische Vorgaben und Entwicklungen

Die Gefährdung der Public-Key-Kryptografie durch potenzielle Quantencomputer erfordert die Einführung neuer kryptografischer Verfahren (sogenannter Post-Quanten-Kryptografie). Diverse Organisationen wie beispielsweise ETSI, IETF und ISO haben bereits mit dieser Arbeit angefangen. Eine zentrale Rolle spielt der Standardisierungsprozess des US-amerikanischen National Institute for Standards and Technology (NIST).

Das NIST ist als US-amerikanische Behörde für Standardisierungsprozesse zuständig. Es hat unter anderem Wettbewerbe durchgeführt, die die weltweit anerkannten Algorithmen AES und SHA-3 hervorgebracht haben. Im November 2016 hat NIST einen Prozess gestartet, an dessen Ende eine Auswahl von quantencomputerresistenten kryptografischen Verfahren zur Verfügung stehen soll. NIST spricht dabei nicht von einem Wettbewerb, vor allem deshalb, weil nicht nur ein Sieger gewählt werden soll. Dennoch hat sich die Bezeichnung „NIST Competition“ in der Forschungsgemeinschaft verbreitet.

Bis Ende November 2017 konnten bei NIST Kandidaten eingereicht werden, von denen inzwischen noch 64 Einreichungen im Rennen sind (siehe Tabelle).

Im Rahmen eines Workshops wurden die Einreichungen im April 2018 vorgestellt. Aktuell läuft eine erste Analysephase, in der die Einreichungen sowohl von NIST als auch weltweit von Forschergruppen evaluiert werden. Ein weiterer Workshop (August 2019) und eine zweite (und ggfs. eine dritte) Analysephase sind angekündigt. NIST rechnet damit, dass erste Draft-Standards 2022–24 zur Verfügung stehen werden.

DIE AUSWAHLKRITERIEN

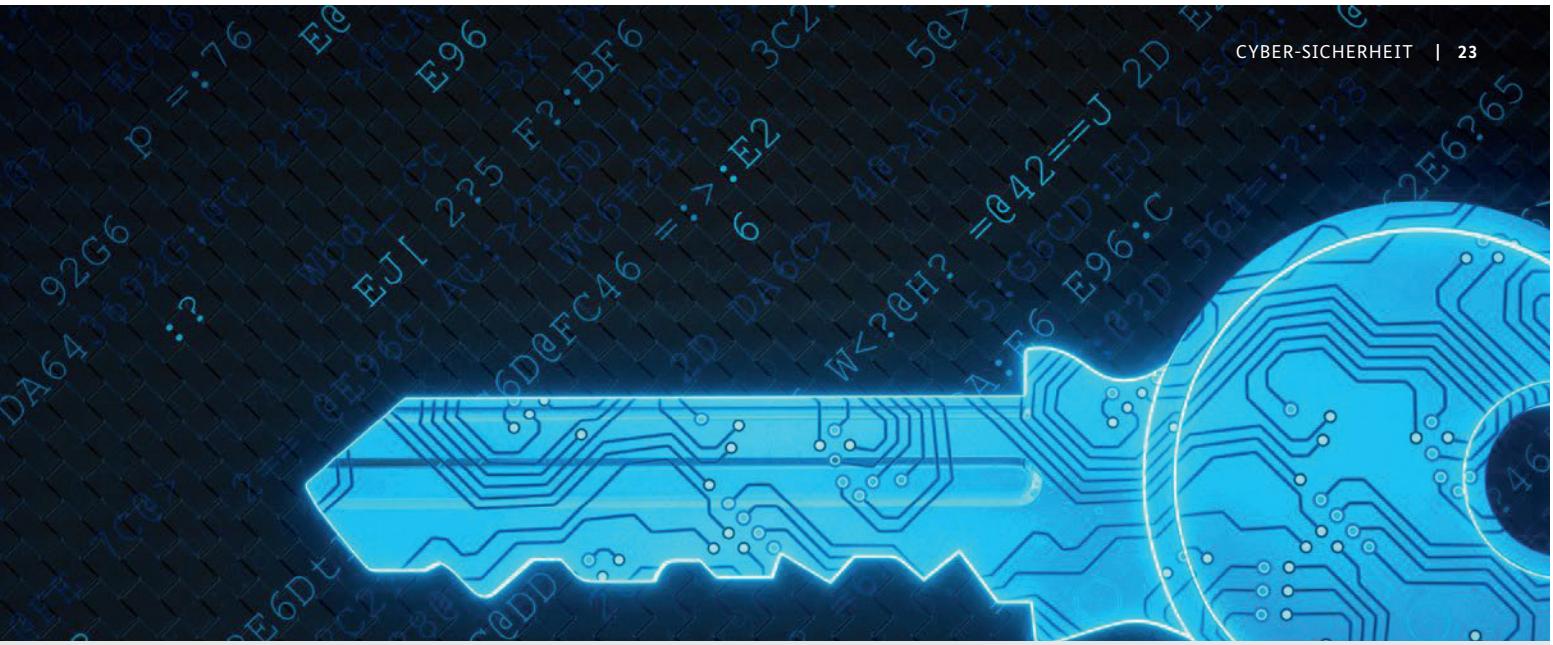
Um die eingereichten Verfahren zu beurteilen, werden zunächst die Kriterien Sicherheit und Effizienz herangezogen.

Die Sicherheit eines Verfahrens wird in der Evaluierung am höchsten gewichtet und umfasst sowohl klassische als auch quantencomputergestützte Angriffe. Neben Sicherheitsbeweisen verlangt NIST, dass die Autoren ihre Vorschläge in Sicherheitskategorien einordnen, die vergleichbar sind zu den folgenden:

I. **Schlüsselsuche bei einer 128-Bit-Blockchiffre (z. B. AES-128)**
II. **Kollisionsangriff auf eine 256-Bit-Hashfunktion (z. B. SHA-256)**
III. **Schlüsselsuche bei einer 192-Bit-Blockchiffre (z. B. AES-192)**
IV. **Kollisionsangriff auf eine 384-Bit-Hashfunktion (z. B. SHA-384)**
V. **Schlüsselsuche bei einer 256-Bit-Blockchiffre (z. B. AES-256)**

Wenn man eine Quantenoperation als Elementarschritt betrachtet, so können diese Kategorien folgendermaßen

	Signatur	KEM/Verschlüsselung	Gesamt
Gitterbasiert	5	21	26
Codebasiert	2	17	19
Multivariat	7	2	9
Symmetrisch/hashbasiert	3	–	3
Andere	2	5	7
Gesamt	**19**	**45**	**64**



grob eingeordnet werden: Der Schlüsselraum einer n-Bit Blockchiffre kann mittels Grovers Algorithmus mit einer Komplexität $2^{n/2}$ durchsucht werden, während ein weiterer Quantenalgorithmus von Brassard et al. eine Kollision einer n-Bit-Hashfunktion in $2^{n/3}$ Schritten findet. Eine genaue Komplexitätsanalyse beinhaltet Quantengatter (siehe Artikel Quantencomputer auf Seite 24/25). Der Vergleich mit der Sicherheit symmetrischer Verfahren begründet sich in der Annahme, dass sich die oben genannten Komplexitäten auch bei quantenalgorithmischen Innovationen nicht wesentlich verschieben.

Die Effizienz eines eingereichten Verfahrens wird nicht nur bestimmt durch den benötigten Rechenaufwand bei Ver- und Entschlüsselung sowie Schlüsselgenerierung, sondern wesentlich auch durch den Speicherbedarf öffentlicher Schlüssel, Chiffraten und Signaturen. Generell rechnet man bei quantencomputerresistenten Verfahren nicht mit einem für alle Szenarien einsetzbaren Kandidaten, sondern mit unterschiedlichen zu akzeptierenden Trade-offs.

Über die Sicherheit und Effizienz hinaus gibt es bei der Bewertung der Verfahren noch weitere Aspekte zu beachten: Die Möglichkeit, flexibel zu parametrisieren, um Sicherheitsniveau und Effizienz zu balancieren, die Implementierungsfreundlichkeit auf unterschiedlichen Plattformen, die Zugänglichkeit des Designs, und auch die Verwendbarkeit im Hinblick auf mögliche Patente und Lizenzbedingungen.

WARUM IST DIESER STANDARDISIERUNGSPROZESS WICHTIG FÜR DAS BSI?

Die Erfahrung zeigt, dass NIST-Standards weltweite Anerkennung finden. Es ist also sehr wahrscheinlich, dass sich die standardisierten Algorithmen in am Markt verfügbaren Produkten wiederfinden und u. a. aus Interoperabilitätsgründen auch in Deutschland genutzt werden. Auch werden andere Standardisierungsgremien wie beispielsweise die IETF die NIST-Algorithmen in ihre Standards aufnehmen. Die deutsche Kryptoindustrie hat bereits begonnen, quantencomputerresistente Algorithmen in ihre Produkte zu integrieren, und orientiert sich dabei an den Kandidaten des NIST-Prozesses.

Darüber hinaus hat sich bei den letzten NIST-Wettbewerben gezeigt, dass sie zu einer weltweiten transparenten Beteiligung mit hohem wissenschaftlichen Wert führen. So kamen die Gewinner der AES- und SHA3-Wettbewerbe aus Belgien. Auch dieses Mal gibt es Teilnehmer aus 25 Ländern und sechs Kontinenten. Aus dem europäischen Projekt PQCrypto, an dem auch das BSI beteiligt ist, sind ebenfalls Einreichungen hervorgegangen.

Das BSI misst der Standardisierung von Post-Quanten-Algorithmen große Bedeutung bei und wird den Auswahlprozess intensiv begleiten sowie durch eigene Untersuchungen ergänzen. Bereits zu nennen sind zwei aktuelle Studien des BSI zu Gitterverfahren und zum Entwicklungsstand von Quantencomputern.

In Zukunft sollte aus Sicht des BSI bereits bei der Produktentwicklung die Möglichkeit vorgesehen werden, kryptografische Algorithmen zu kombinieren („hybride Verfahren“) bzw. bei Bedarf einfach auszutauschen („Kryptoagilität“). Diese Ziele gelten unabhängig von der Existenz von Quantencomputern, sie stehen nicht im Fokus des „NIST-Wettbewerbs“. ■

Weitere Informationen:
Überblick über die beim NIST eingereichten Verfahren unter http://www.safecrypto.eu/pqclounge/

Quantencomputer

Eine BSI-Studie zum Entwicklungsstand

von Armin Cordel und Dr. Stavros Kousidis, Referat Kryptografische Vorgaben und Entwicklungen

Bisher nahmen Quantencomputer eine exotische Stellung in der Informationsverarbeitung ein. Mit den Ankündigungen von 72 bzw. 50 Qubits als angestrebte Meilensteine von Google und IBM wird jedoch deutlich, dass Forschung, Entwicklung und Kommerzialisierung deutlich vorangeschritten sind. Aufgrund der Implikationen für die gegenwärtige Public-Key-Kryptografie muss diese technologische Entwicklung sorgsam beobachtet werden.

Der Alltag in unserer Gesellschaft wird zunehmend durch Digitalisierung und Vernetzung geprägt. An die dabei zugrunde liegende Technologie der Digitalrechner wie PC und Server, die als kleinste Informationseinheit ein Bit mit den Werten 0 oder 1 speichern und bearbeiten, haben wir uns als selbstverständlich gewöhnt.

Gleichzeitig haben in den 1980er-Jahren erste Überlegungen zu Quantencomputern eingesetzt. Hier fungieren die Werte 0 und 1 als Basiswerte wie der Nord- und Südpol einer Kugel und können in Superposition zur Darstellung eines beliebigen Punktes auf der Kugel kombiniert werden. Diese Anschauung nennt man die Bloch-Kugel und die elementare Speichereinheit ein Qubit.

Im völligen Gegensatz zu digitalen Bits führen diese zusätzlichen Freiheitsgrade zu einer intrinsischen Parallelisierung. Ein Quantenalgorithmus, d. h. eine Abfolge von Manipulationen von Qubits, nutzt genau diese Parallelisierung aus. Zu den bekanntesten gehören der Suchalgorithmus von Lov Grover (1996) und die Algorithmen von Peter Shor (1994), mit denen ganze Zahlen faktorisiert und diskrete Logarithmen berechnet werden können. Insbesondere die letztgenannten brechen heutige Public-Key Kryptografie wie RSA, Diffie-Hellman, ElGamal oder ECC.

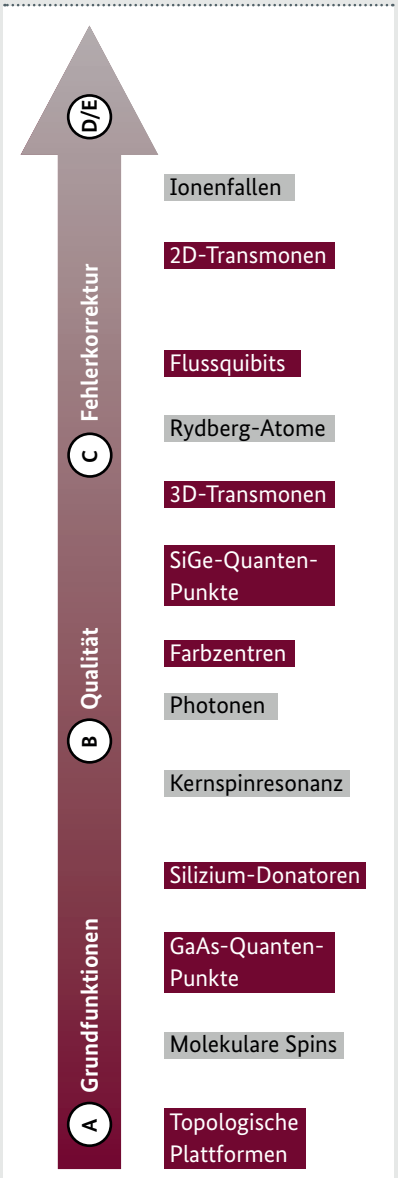


Abbildung 1: Einordnung verschiedener Plattformen im Schichtenmodell.

Daher hat das BSI nun eine Studie zu Quantencomputern veröffentlicht (www.bsi.bund.de/qcstudie). Ihr Ziel ist es, den aktuellen Entwicklungsstand eines kryptografisch relevanten Quantencomputers fundiert und unabhängig einzuschätzen, d. h. eines genügend großen Quantencomputers, um etwa einen Shor-Algorithmus zu implementieren.

QUANTENFEHLERKORREKTUR IST DAS STRUKTURIERENDE ELEMENT

Eine zentrale Herausforderung an eine skalierbare Qubit-Technologie stellt die Fehleranfälligkeit bzw. Dekohärenz quantenmechanischer Systeme dar. Neben isolierenden Maßnahmen wie elektromagnetischen Fallen und Tiefsttemperaturen muss eine Quantenberechnung aktiv fehlerkorrigiert werden.

Hieraus ergibt sich das in der Studie zusammengefasste Schichtenmodell (A-E), anhand dessen ein Qubit-Kandidat eingeordnet werden kann. Ausgehend von grundlegenden Funktionen (A) bis hin zu fehlertoleranten Elementaroperationen (D) und der daraus assemblierten Implementierung von Quantenalgorithmen (E), führt der Weg über die Operationsqualität eines einzelnen Qubits (B) und die systematische Quantenfehlerkorrektur (C).

Erst eine hohe Operationsqualität erlaubt eine effiziente Quantenfehlerkorrektur. Dieser Zusammenhang ist im Quantum-Threshold-Theorem von Ben-Or und Aharonov exakt beschrieben und führt zur Identifizierung von 2D-Transmonen (Google) und Ionenfallen (IBM) als Qubit-Technologien, die mit ihrer aktuell erreichten Operationsqualität eine funktionierende Quantenfehlerkorrektur erlauben. Für diese Technologien ist es möglich, einen daraus zusammengesetzten Quantencomputer, z. B. zur Faktorisierung eines 2048-Bit-RSA-Moduls, zu extrapolieren.

Hierfür muss der Übergang von einem einzelnen sogenannten physikalischen Qubit in eine Fehler korrigierende Architektur aufgeschlüsselt werden. Klassische Fehlerkorrekturmechanismen kodieren Information redundant, sind aber aufgrund des No-Cloning-Theorems nicht anwendbar. Stattdessen überträgt ein Quantenfehlerkorrekturcode den Zustand eines physikalischen Qubits auf ein verschränktes, d. h. auf quantenmechanische Weise verbundenes, System von Daten- und Syndrom-Qubits, das als logisches Qubit bezeichnet wird. Die Anordnung ist so gewählt, dass Messungen an den Syndrom-Qubits den Fehlerstatus des Daten-Qubits ergeben und gleichzeitig dessen Zustand stabilisieren. Außerdem erlaubt diese Struktur eine Reduktion und Vereinheitlichung des Fehlermodells. Vertreter solcher Codes sind der von Peter Shor (1995) eingeführte 9-Qubit-Code und die aktuell führende, als Surface Code bezeichnete Architektur.

Der Expansionsfaktor beim Übergang von physikalischen zu logischen Qubit und damit die gesamte Extrapolation werden entscheidend durch die Operationsqualität und die angewandte Quantenfehlerkorrektur beeinflusst.

Ausgehend vom Surface Code und einer aktuell etablierten Operationsqualität von 99 Prozent würde ein 2D-Transmonen-Quantencomputer mit einigen Milliarden physikalischen Qubits in 100 Tagen einen 2048-Bit-RSA-Modul faktorisieren können. Bei einer allgemein angestrebten Operationsqualität von 99,99 Prozent wären es einige Millionen physikalische Qubits. Der Zusatz „in 100 Tagen“ resultiert aus einem Platz-Zeit-Kompromiss, denn eine Extrapolation ergibt sich nicht allein aus einer isolierten Betrachtung der Quantenfehlerkorrektur. Zusätzlich gilt es, diese in Abhängigkeit zu Elementaroperationen und Schaltzeiten zu setzen. Tatsächlich beginnt die Studie damit, die Algorithmen von Grover und Shor in elementare Schritte zu zerlegen. Hier bedient man sich des Theorems von Solovay und Kitaev, das eine Menge von Elementaroperation beschreibt, aus der sich jede Quantenoperation zusammensetzen lässt.

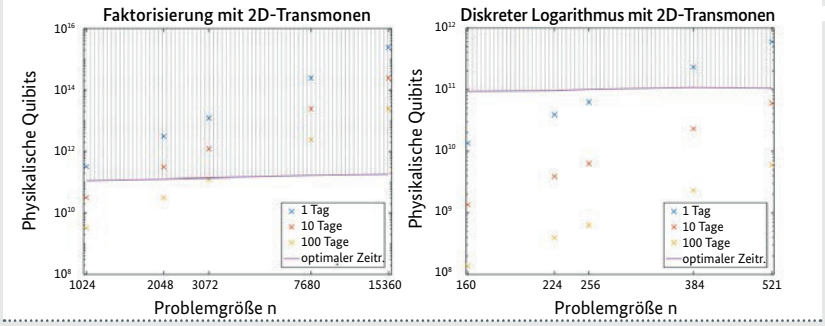


Abbildung 2: Größe eines 2D-Transmonen-Quantencomputers zur Faktorisierung und Berechnung eines diskreten Logarithmus bei heutiger Operationsqualität von 99 Prozent.

Faktorisierung		
n	Qubits	Grundlegende Operationen
1024	2050	$5{,}81 \cdot 10^{11}$
2048	4098	$5{,}20 \cdot 10^{12}$
3072	6146	$1{,}86 \cdot 10^{13}$
7680	15362	$3{,}30 \cdot 10^{14}$
15360	30722	$2{,}87 \cdot 10^{15}$

Diskreter Logarithmus auf $E(F_p)$		
n	Qubits	Grundlegende Operationen
160	1466	$2{,}97 \cdot 10^{10}$
224	2042	$8{,}43 \cdot 10^{10}$
256	2330	$1{,}26 \cdot 10^{11}$
384	3484	$4{,}52 \cdot 10^{11}$
521	4719	$1{,}14 \cdot 10^{12}$

Abbildung 3: Benötigte Elementaroperationen und (logische) Qubits für eine Faktorisierung und zur Berechnung eines diskreten Logarithmus auf einer generischen elliptischen Kurve.

GEWONNENE ERKENNTNISSE

Die Studie beschreibt und illustriert die hier skizzierten Zusammenhänge und Begriffe im Detail. Sie liefert eine Übersicht und Einordnung aktueller Technologien und Akteure. Ebenfalls wird die Peripherie zum Betrieb eines Quantencomputers betrachtet und Restrisiken, wie etwa potenzielle sprunghafte Entwicklungen, werden konkret benannt.

Insgesamt gewinnt man eine stark strukturierte Sicht auf den Entwicklungsstand von Quantencomputern. Sie zeigt, dass aktuell eine enorme Anstrengung nötig wäre, um eine kryptografisch relevante Skalierung vorzunehmen. Gleichzeitig aber wird deutlich, dass die Entwicklung durch starke Industrieakteure und große Forschungsprogramme an Fahrt gewonnen hat und weitere kommerzielle Anwendungen diese noch beschleunigen könnten. ■

Weitere Informationen: Studie zu Quantencomputern: www.bsi.bund.de/qcstudie

VS-Anforderungsprofile

Time-to-Market – Wie VS-Zulassungen beschleunigt werden.

Von Ingo Hahlen und Sandra Karger, Referat VS-Zulassungen und Grundsatz

Die Arbeit mit Verschlusssachen (VS) in Bundesbehörden und bundesunmittelbaren Einrichtungen richtet sich nach den Regelungen der „Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung – VSA)“. Immer wenn elektronische Verschlusssachen zu schützen sind, muss dafür nach §37 VSA ein zugelassenes Produkt verwendet werden. Zulassungen werden nach einer erfolgreichen Evaluierung durch das BSI ausgestellt.

Durch die Evaluierung ist die Gretchenfrage der Zulassung zu beantworten: Ist ein gegebenes Produkt geeignet, um die damit verarbeiteten elektronischen Verschlusssachen angemessen zu schützen? Was sich zunächst einfach anhört, entpuppt sich oft als schwierig. Unterschiedliche Interessen müssen möglichst gut in Übereinstimmung gebracht werden.

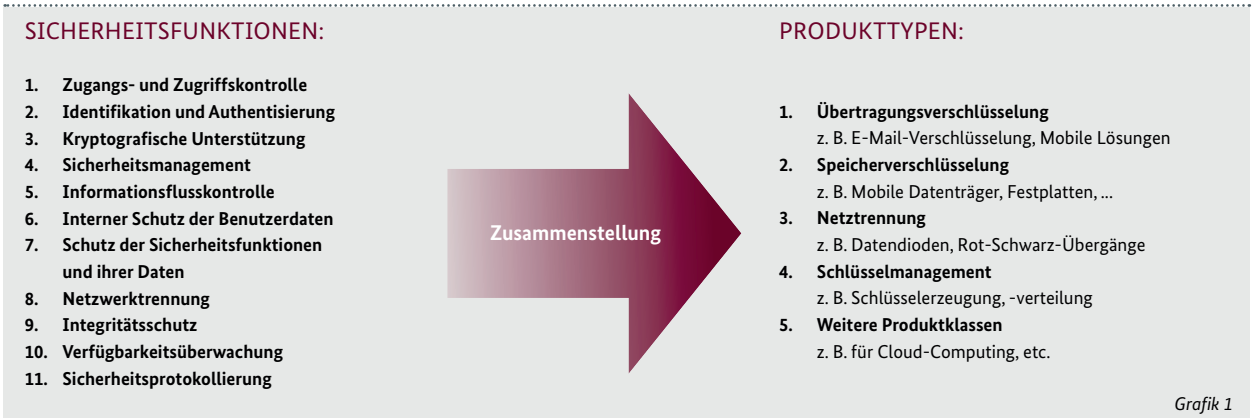
- Das BSI denkt an mögliche Bedrohungen, IT-Sicherheitsfunktionen und Annahmen, die zu beachten sind. Es hat auch regulatorischen Einfluss.
- Die Bedarfsträger, also die betroffenen Behörden, stellen bei Beschaffungen von Produkten Funktionalität, Wartbarkeit und mögliche Einschränkungen durch Anforderungen an die IT-Sicherheit in den Vordergrund.
- Hersteller denken an Vermarktbarkeit, Aufwände, planbare Produktentwicklungen, Business Case mit Return on Investment durch eine Zulassung.

Der immer schnellere Technologiewechsel und der immer größere Bedarf an IT-Unterstützung in der Bundesverwaltung erfordern eine standardisierte Vorgehensweise, um Anforderungen an IT-Sicherheitsprodukte zu entwickeln, die elektronische Verschlusssachen schützen sollen. Dazu hat das BSI das Konzept der VS-Anforderungsprofile erarbeitet. Damit

- können alle Stakeholder ihre Sichtweisen in die Anforderungen an die IT-Sicherheit frühzeitig einbringen,
- werden Produktentwicklung und -einsatz planbar,
- wird eine schnellere Entwicklung und Inbetriebnahme ermöglicht und
- werden schwierige Diskussionen zu Aspekten der IT-Sicherheit im Vorfeld einer Evaluierung geführt sowie verschiedene Sichtweisen einbezogen.

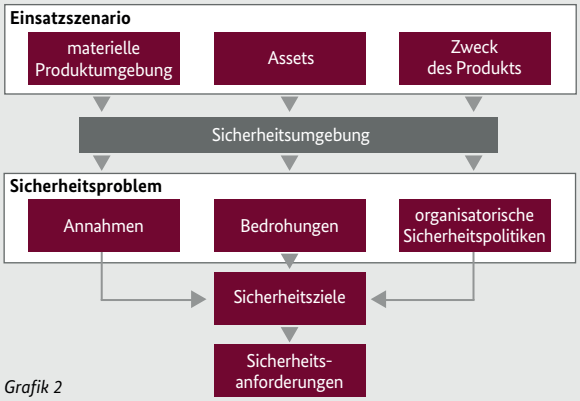
MODELL UND PROZESS

Das Modell definiert zunächst eine Menge von Sicherheitsgrundfunktionen und legt eine Liste von Produkttypen fest, für die ein Standard in Form eines VS-Anforderungsprofils entwickelt werden soll. Jedem Produkttyp werden dabei verschiedene Sicherheitsgrundfunktionen zugeordnet (siehe Grafik 1):



Grafik 1

Weiterhin legt das Modell fest, welche Inhalte für jedes VS-Anforderungsprofil in entsprechenden Kapiteln vorhanden sein müssen, um ein bestimmtes Sicherheitsproblem zu adressieren (siehe Grafik 2):



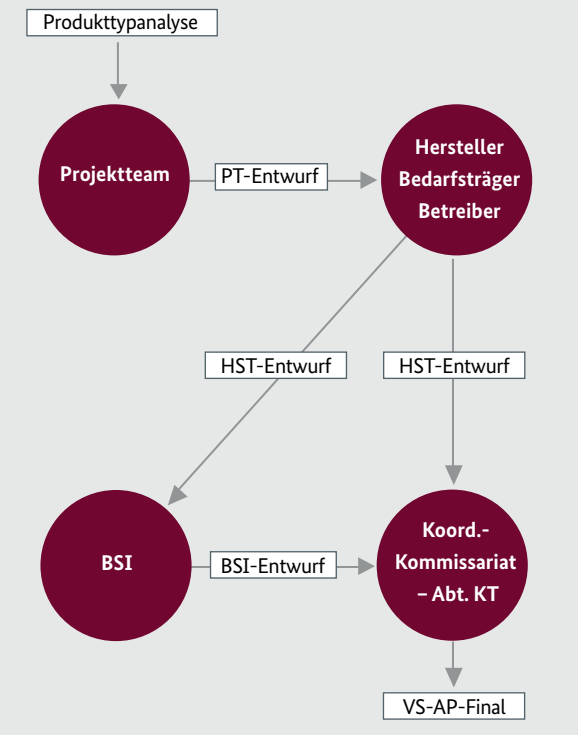
Grafik 2

Ausgehend vom Einsatzszenario, dem Geheimhaltungsgrad und dem Zweck einer Produktklasse, werden zunächst Werte festgelegt, die zu schützen sind.

Das zu lösende Sicherheitsproblem wird in Form von Annahmen, Bedrohungen und organisatorischen Sicherheitspolitiken festgelegt.

Daraus lassen sich Sicherheitsziele und entsprechende Sicherheitsanforderungen ableiten.

In einem innovativen Prozess werden dann die Inhalte eines VS-Anforderungsprofils erstellt (siehe Grafik 3):



Grafik 3

Ein BSI-Projektteam erstellt zunächst mit Unterstützung eines externen Partners auf Basis vorhandener Dokumente nach einer Analysephase den Projektteam(PT)-Entwurf. Im Anschluss wird eine Gruppe von Herstellern, Betreibern und Anwendern aufgefordert, ihren inhaltlichen Beitrag in Form eines gemeinsamen Workshops und schriftlicher Beiträge zu leisten. Das Resultat ist dann der Hersteller(HST)-Entwurf.

Dieser wird im BSI zur Kommentierung verteilt. Ein gemeinsamer Workshop zur Besprechung der Kommentare mit darauffolgender Erstellung des BSI-Entwurfs schließt diese Phase ab.

Eine Freigabe des finalisierten VS-Anforderungsprofils erfolgt durch die regelmäßig tagende Koordinierungskonferenz der Abteilung KT (Krypto-Technologie und IT-Management für erhöhten Sicherheitsbedarf) des BSI. Anschließend wird das VS-Anforderungsprofil veröffentlicht.

ERFAHRUNGEN

Die bisherigen Erfahrungen zeigen, dass alle Beteiligten von dieser transparenten Vorgehensweise überzeugt sind und sich offen in die Diskussionen einbringen. Die vorhandenen VS-Anforderungsprofile erfahren von Herstellern eine hohe Akzeptanz, werden zur Produktentwicklung verwendet sowie von Bedarfsträgern in Ausschreibungsunterlagen referenziert. Die zielführende Diskussion der wichtigsten Aspekte zu Beginn fördert ein besseres Verständnis der Problematik und sorgt für Planungssicherheit. Verkürzte Evaluierungszeiten beschleunigen das Zulassungsverfahren. Die Produkte kommen schneller auf den Markt.

Bisher wurden IT-Sicherheitsanforderungen für die folgenden Produkttypen in VS-Anforderungsprofilen definiert:

- VPN-Gateway
- VPN-Client
- Sichere Netzwerkkarte
- Kryptobeschleuniger
- Sichere Mobile Lösungen
- Sicherer Mobiler Datenträger
- Festplattenverschlüsselung
- Hardware-Sicherheitsmodul

Weitere VS-Anforderungsprofile unter anderem zu Separation Kernel-Technologien, E-Mail und Dateiverschlüsselung sind in Arbeit. ■

Weitere Informationen:
https://www.bsi.bund.de/VS-Anforderungsprofile

DAS BSI

Andreas Könen, BMI

Symposium „Deutschland.Digital.Sicher.BSI“ in der AXICA in Berlin

Podiumsdiskussion mit allen Referenten und Dr. Timo Hauschild

Begrüßung durch Arne Schönbohm, Präsident des BSI

Jürgen Schmidt, Chefredakteur heise online

Ines Schieferdecker, Leiterin Öffentlichkeitsarbeit im BSI, moderierte die Veranstaltung

Positive Resonanz auf erstes BSI-Symposium

Cyber-Sicherheitsstrategien, Industrie 4.0, Haftung und Datensicherheit, diese Themen standen im Fokus des ersten Symposiums des BSI, das am 26. Juni 2018 in Berlin stattfand. Rund 100 Teilnehmerinnen und Teilnehmer aus Politik, Wirtschaft, Wissenschaft, Verwaltung und Gesellschaft waren der Einladung von BSI-Präsident Arne Schönbohm zum Austausch ins Kongress- und Tagungszentrum AXICA gefolgt. Das Motto: **Deutschland.Digital.Sicher.BSI.**

Nach einem Grußwort des neuen Abteilungsleiters für Cyber- und IT-Sicherheit im Bundesministerium des Innern, für Bau und Heimat, Andreas Könen, beleuchteten Impulsgeber und Entscheidungsträger in ihren Vorträgen den Status quo zur Cyber-Sicherheit in der Industrie 4.0, beispielsweise in der Elektroindustrie. Dabei wurde hinterfragt, wie die Unternehmen mit geeigneten Strategien auf die aktuelle Bedrohungslage durch die fortschreitende Digitalisierung und das Internet der Dinge reagieren. Zudem diskutierten die Teilnehmer über die Problematik der Haftung im Cyber-Space und die Datensicherheit in einer weltweit vernetzten Branche wie dem Asset Management.

In einer Zeit der Digitalisierung, in der immer mehr neue und bereits bestehende Produkte und Dienstleistungen online vernetzt sind, steigt auch die Angriffsfläche für Cyber-Kriminelle. Mit dem Symposium bot das BSI als nationale Cyber-Sicherheitsbehörde Raum, sich über Probleme auszutauschen und Lösungsmöglichkeiten zu diskutieren. So waren sich die Teilnehmer während der abschließenden regen Podiumsdiskussion einig:

IT-Sicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung.

BINDEN, MOTIVIEREN, ENTWICKELN

Das BSI fördert Nachwuchs-Führungskräfte aus den eigenen Reihen

Durch den großen Zuwachs an neuen Stellen steht das BSI vor der Herausforderung, nicht nur eine große Zahl qualifizierter Mitarbeiterinnen und Mitarbeiter zu finden – auch Führungspositionen müssen neu besetzt werden. Führungskräfte bekleiden Schlüsselpositionen, da sie vielfältige Anforderungen zu erfüllen haben: Sie sollten sowohl die fachliche Tiefe als auch die führungsrelevante Breite für eine leitende Stelle besitzen. Die Lösung: das Führungskräftenachwuchsprogramm (FKNP) zur gezielten Förderung für diejenigen, die mittel- bis langfristig eine Führungsposition anstreben. Es wurde bereits zweimal durchgeführt – und findet nun zum dritten Mal statt.

WAS IST DAS ZIEL?

Mitarbeiterbindung, -motivation und -weiterentwicklung – Führungskräfte intern auszubilden hat viele Aspekte. Einmal bietet es motivierten Mitarbeiterinnen und Mitarbeitern eine langfristige Perspektive in der Behörde. Zum anderen kann das BSI bei der Besetzung von Referatsleitern auch auf aktuelle Mitarbeiterinnen und Mitarbeiter zurückgreifen, die sich bereits fachlich bewährt haben und die behördenspezifischen Handlungsfelder und Strukturen kennen.

Das eigens für das BSI erstellte Programm legt großen Wert darauf, dass die Teilnehmerinnen und Teilnehmer sich schon vor der späteren Übernahme einer Führungsposition mit dieser Rolle auseinandersetzen und gut vorbereitet an den Start gehen. Mittel- bis langfristig ist es das Ziel, den notwendigen Führungskräftebestand des BSI zu sichern und gute Mitarbeiterinnen und Mitarbeiter auszubilden sowie gezielt weiterzuentwickeln.

Ein willkommener Effekt ist auch, die Kommunikation innerhalb der Behörde zu verbessern, um den Blick über den Tellerrand des eigenen Referats zu fördern. Gleichzeitig steht auch das Netzwerken zwischen den Programmteilnehmern im Fokus. Auf diese Weise profitiert das gesamte BSI von der Kompetenzerweiterung der ausgebildeten Kolleginnen und Kollegen.

WER KANN TEILNEHMEN?

Die Teilnahme am Programm wird einmal im Jahr intern ausgeschrieben. Bewerben können sich motivierte Referentinnen und Referenten des BSI, die bereits über mehrere Jahre Berufserfahrung verfügen und mittel- bis langfristig Führungsambitionen besitzen sowie ihre persönlichen und beruflichen Kompetenzen erweitern möchten.

Die Auswahl von zwölf finalen Teilnehmenden erfolgt durch eine Auswahlkonferenz, bestehend aus Abteilungsleitern, Amtsleitung und Personalreferat. Dabei sind unter anderem die Teilnahmemotivation der Bewerber und eine überdurchschnittliche Beurteilung durch die Vorgesetzten wichtige Entscheidungskriterien.

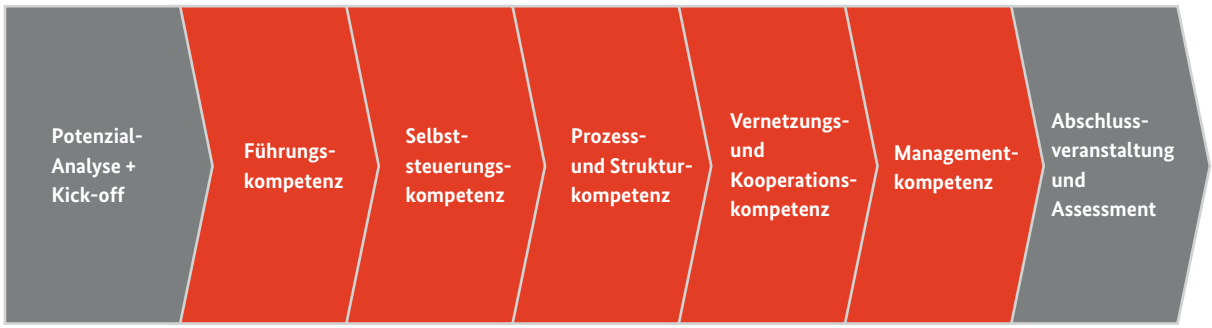
WIE LÄUFT DAS FKNP AB?

In einem Zeitraum von ca. zwölf Monaten finden fünf verschiedene Module an insgesamt zwölf Trainingstagen statt. Sie sind individuell auf die Anforderungen an Führungskräfte in der Behörde zugeschnitten, um die Teilnehmerinnen und Teilnehmer gezielt auszubilden. Ziel ist es, Kompetenzen in den Bereichen Führung, Selbststeuerung, Prozesse und Strukturen, Vernetzung und Kooperation sowie Management zu vermitteln.

Viel Wert wird auch auf die Vernetzung der Teilnehmenden gelegt: Die zwei- bis dreitägigen Module werden außerhalb der Behörde durchgeführt. Abendgespräche mit hochrangigen Führungskräften des BSI sichern den Transfer des Erlernten in die Praxis. Darüber hinaus wird der Gruppe über die gesamte Zeit eine begleitende Aufgabe gestellt, die sie gemeinsam bearbeitet.

Teilnehmerinnen und Teilnehmer des zweiten FKNP-Durchgangs im Modul Managementkompetenzen.

QUALIFIZIERUNGSPROGRAMM FÜR FÜHRUNGSNACHWUCHSKRÄFTE IM BSI



Ein bedeutsamer Teil der Ausbildung sind außerdem die Hospitationen in anderen Abteilungen. Um den Blick für den strategisch-politischen Zusammenhang von BSI-Themen zu schärfen, werden die Teilnehmenden für vier Wochen in anderen Referaten, Abteilungen oder dem Leitungsstab eingesetzt.

Über die gesamte Dauer des Programms werden die Beteiligten zusätzlich von einem Fachbereichsleiter als Mentor begleitet und beraten. Dieser hat u. a. die Aufgabe, die gesteckten Ziele mit dem Mentee zu reflektieren und fachliche sowie persönliche Fragen zu diskutieren.

Das Programm endet mit einem Assessment-Center, bei dem das Führungspotenzial eingeschätzt und eventuell notwendige weitergehende Personalentwicklungsmaßnahmen festgelegt werden. Es erfolgt ein Abgleich des Kompetenzprofils für Führungskräfte mit den tatsächlich erworbenen Kompetenzen.

WIE GEHT ES WEITER?

Nach dem erfolgreichen Abschluss des Programms können sich die Teilnehmenden im Rahmen des üblichen Bewerbungsverfahrens auf eine Führungsposition bewerben. Sie durchlaufen dabei denselben Prozess wie Externe. Der Vorteil: Die Absolventen haben ihre Führungskompetenz bereits durch das FKNP nachgewiesen.

Die Übernahme einer leitenden Position ist jedoch weder eine Garantie noch eine Pflicht. Vielmehr geht es darum, den notwendigen Führungskräftebestand langfristig zu sichern und diesen im Hinblick auf die künftigen politischen, strategischen und fachlichen Herausforderungen in der IT-Sicherheit vorzubereiten.

ARNE SCHÖNBOHM, BSI-PRÄSIDENT

Warum wurde das FKNP ins Leben gerufen?

Das Führungskräftenachwuchsprogramm aufzusetzen ist vor allem eine strategische Entscheidung gewesen, um langfristig Führungspositionen mit eigenen Mitarbeiterinnen und Mitarbeitern zu besetzen, die bereits über sehr gute fachliche Qualifikationen verfügen und darüber hinaus auch ein hohes Potenzial in führungsrelevanten Kompetenzbereichen erkennen lassen. Dieses Profil am Markt zu bekommen ist schwierig. Wir wachsen weiterhin stark. Die Entwicklung leistungsfähiger Mitarbeiterinnen und Mitarbeiter aus den eigenen Reihen ist somit neben der Personalgewinnung außerhalb des BSI logische Schlussfolgerung, um den notwendigen Führungskräftebedarf des BSI zu decken. Gleichzeitig ist es eine hervorragende Möglichkeit, Talent zu erkennen und zu fördern, und dient somit auch der Personalentwicklung und -bindung.

Durch das Programm sind Mitarbeiterinnen und Mitarbeiter bei der späteren potenziellen Übernahme einer Führungsposition besser gerüstet und haben eine realistische Einschätzung der Rolle als Führungskraft. Aber auch die Erkenntnis, dass jemand doch lieber Fachkraft bleiben und nicht in eine Führungsposition wechseln möchte, kann eine wertvolle Lehre aus dem Programm sein.

Worin sehen Sie die Vorteile, Nachwuchsführungskräfte aus den eigenen Reihen auszubilden?

Erfolgreiche Führung spiegelt sich in der Kombination aus Strategie, Struktur und Kultur wider. Die Mitarbeiterinnen und Mitarbeiter haben sich nicht nur bereits fachlich bewährt, sondern kennen auch den Kontext, in dem sich das BSI bewegt. Sie verfügen in der Regel über ein gutes Netzwerk, kennen bereits relevante Player und – nicht zu vernachlässigen – die interne Struktur und Kultur. Mit den im Programm vermittelten Kompetenzen ergänzen wir diese Eigenschaften um den strategischen Baustein und unterstützen Mitarbeiterinnen und Mitarbeiter auf der Führungsebene dabei, Veränderungen mit zu tragen.

Durch die Möglichkeit sich weiterzuentwickeln werden zusätzlich die Motivation und die Mitarbeiterbindung nachhaltig gestärkt.

HORST SAMSEL, ABTEILUNGSLEITER B

Welche Aufgaben haben Sie als Abteilungsleiter im FKNP?

Als Abteilungsleiter bin ich bereits vor Beginn des Programms bei der Auswahl der geeigneten Referentinnen und Referenten tätig. Diese Aufgabe ist entscheidend, da wir bisher immer mehr Bewerbungen bekommen haben, als wir Plätze zur Verfügung stellen konnten. Nach der Nominierung begleite ich die Teilnehmer weiter. Während der Module gibt es zum Beispiel einen Programmpunkt, der sich „Kamingespräch“ nennt. Dort stehen Personen der Leitungsebene wie ich den Teilnehmern Rede und Antwort zu unseren Einstellungen und Erfahrungen. Aber auch in den alltäglichen Austausch mit den Teilnehmern bin ich involviert, indem ich die Vereinbarkeit des Programms mit dem aktuellen Tagesgeschäft unterstütze.

Wie wirkt sich das Programm auf Ihre Abteilung aus?

Das FKNP ist eine Fortbildungsmaßnahme, die darauf abzielt, bereits vorhandene Qualifikationen auszubauen und zu erweitern. Schon nach dem ersten Durchgang hat sich dies positiv auf meine Abteilung ausgewirkt. Besonders die Hospitationen bringen Verständnis gegenüber anderen Abteilungen hervor und verbessern die Zusammenarbeit. Ich erachte es als sehr fruchtbar und sinnvoll, dass wir im BSI die Erfahrung machen können, die Abläufe anderer Abteilungen kennenzulernen.

MAXIMILIAN WINKLER, REFERENT CK 24,
TEILNEHMER AM AKTUELLEN DURCHGANG DES FKNP

Das Programm ist bald beendet – was war für Sie besonders lehrreich?

Wirklich wertvoll war und ist für mich der Austausch mit den Teilnehmern aus den anderen Abteilungen; das, was man so als Vernetzung bezeichnet. Letztendlich geht es darum, Menschen zu kennen, die man anrufen kann, um z. B. Ansprechpartner zu finden, Prozesse zu beschleunigen oder eine dritte Meinung zu bekommen. Hierdurch bekam ich hautnah mit, dass auch in den anderen Abteilungen im BSI sehr viele Themen in teilweise beeindruckender Tiefe bearbeitet werden.

Wie integrieren Sie das Programm in Ihren beruflichen Alltag?

Das Programm lässt sich gut in den Alltag integrieren. [...] Wenn wir uns für die Projektaufgabe in der Gruppe treffen müssen, ist das schon schwieriger; alleine aufgrund der Anzahl an Personen, die in ihren Referaten bereits sehr eingebunden sind und sich dann auf einen gemeinsamen Termin verständigen sollen.

Die Unterstützung durch die Führungsebenen im BSI ist auf jeden Fall gegeben. So steht jedem Teilnehmer ein Fachbereichsleiter aus dem BSI als Mentor und Ansprechpartner zur Verfügung. Bisher hat mich auch noch keiner meiner Referatsleiter, Fachbereichsleiter oder Abteilungsleiter weggeschickt, wenn ich ein Anliegen hatte - übrigens auch schon vor meiner Teilnahme am FKNP nicht.

MARTINA ROHDE, REFERATSLEITERIN KT 21,
TEILNEHMERIN AM LETZTEN FKNP

Sie sind mittlerweile Referatsleiterin. Wie hat Sie das Programm auf diese Stelle vorbereitet?

Die Module haben mir einen fundierten Überblick über die führungsrelevanten Aspekte gegeben. Während des Programms habe ich die Gelegenheit genutzt, über meine eigene Einstellung zu bestimmten Aspekten zu reflektieren; nach dem Programm stellen die Module einen Fundus dar, in dem ich hin und wieder nachschlage. Mit anderen Worten: ein guter Trainingsplan.

Würden Sie die Teilnahme weiterempfehlen?

Ein klares „Ja“. Das in den Modulen vermittelte Wissen ist durchaus auch bei der Leitung von Projekten oder beim Zusammenarbeiten im Team von Vorteil. Daher halte ich das Programm grundsätzlich auch für Kolleginnen und Kollegen ohne unmittelbare Führungsambitionen geeignet.

CYBER COMPETENCE CENTER HESSEN

Hessen3C

Die Digitalisierung bietet dem Einzelnen ebenso wie der Gesellschaft viele neue Chancen. Damit einher gehen aber auch völlig neue Herausforderungen im Bereich der Sicherheit. Hessen geht mit dem Cyber Competence Center neue Wege, um diese Herausforderungen zu meistern.

von Marcus Brambach und und Markus Wiegand, Hessisches Ministerium des Innern und für Sport

Die Digitalisierung und die Vernetzung verändern alle Lebensbereiche in einer noch nie dagewesenen Geschwindigkeit. Der Wohlstand unserer Gesellschaft hängt stark davon ab, dass Deutschland diesen Wandel nicht nur als Konsument erlebt, sondern ihn aktiv gestaltet. Die industrielle Kompetenz Deutschlands bietet beste Voraussetzungen an der Cyber-/Physical-Schnittstelle, bei der Entwicklung der Industrie 4.0 entscheidende Beiträge leisten zu können.

Wenn man an autonome Fahrzeuge oder an Medizintechnik denkt, wird sofort klar, wie wichtig die Schnittstelle zwischen der physikalischen und der digitalen Welt ist. Es wird an diesem Beispiel aber auch klar, dass diese Schnittstelle die bisherige Fehlertoleranz der digitalen Dienstleistungen nicht zulässt. Daraus ergeben sich Chancen und Herausforderungen.

Chancen insofern, als dass Sicherheit als Qualitätskriterium in der deutschen Industrie eine lange Tradition hat und „Security Made in Germany“ zu einem neuen Markenkern werden kann. Cyber-Sicherheit wird aber unter zwei Aspekten zu einer Herausforderung: Kriminelle wie auch Nationalstaaten haben längst das Potenzial erkannt, das sich aus der Kombination von weltweiter Vernetzung und immer größer werdenden Abhängigkeiten von informationstechnischen Systemen und digitalen Infrastrukturen ergibt. Eine zunehmend professionelle und hochgradig arbeitsteilige Untergrundökonomie bietet eine große Menge von Lösungen, Plattformen und Dienstleistungen für Angriffe auf digitale Systeme an. Mit dem zeitgleichen Aufkommen von Internetbasierten Zahlungsdiensten und Kryptowährungen wurde die Erpressung von Bürgern, Unternehmen bis hin zu Staaten möglich.

ÖFFENTLICHE SICHERHEIT AUCH IM CYBER-RAUM GEWÄHRLEISTEN

In diesem Umfeld muss der Staat seine Garantenrolle neu denken. Der öffentliche Raum beschränkt sich längst nicht mehr auf Plätze und Versammlungsorte, das Bedürfnis nach einer staatlich garantierten Infrastruktur, beschränkt sich längst nicht mehr auf Verkehrssysteme. Der Auftrag zur Gewährleistung der öffentlichen Sicherheit und Ordnung hat viele neue Facetten bekommen.

Die Wirtschaft braucht im digitalen Zeitalter mehr Schutz vor Konkurrenz- und staatlich initiierter Wirtschaftsspionage, die Bürger und Unternehmen werden Opfer neuer krimineller Angriffe und der Staat muss dafür Sorge tragen, dass die Kritischen Infrastrukturen resilient werden.

NEUE STRUKTUREN; DAS HESSEN3C

Diese neuen Anforderungen lassen sich nicht mit einem „Weiter so!“ in den bestehenden Strukturen bewältigen. Mit dem Hessen Cyber Competence Center, dem Hessen3C, geht das hessische Innenministerium völlig neue Wege. Hessens Innenminister Peter Beuth beschreibt den hessischen Weg in der Cyber-Sicherheit so: „Mit Hessen3C wollen wir unsere Sicherheitsbehörden bei der Cyber-Sicherheit und der Bekämpfung von Internetkriminalität durch operative Beratungsangebote und effektive Werkzeuge noch besser unterstützen. Wenn Kriminelle und Terroristen ihre Kommunikationswege zunehmend digital verschlüsseln, brauchen unsere Sicherheitsbehörden Spezialkenntnisse im Bereich Kryptografie und darüber hinaus die geeigneten Instrumente, solche Daten zu decodieren. Dafür müssen wir die Sicherheitsbehörden stärken und ihnen die richtigen rechtlichen wie tatsächlichen Werkzeuge an die Hand geben. Beides ist unser erklärtes Ziel und gelebte Praxis der Hessischen Landesregierung. Mit Hessen3C vernetzen und stärken wir die Sicherheitsbehörden im Kampf gegen Cyber-Kriminalität und -spionage.“

Im Hessen3C werden Spezialisten aus der hessischen Polizei, dem CERT-Hessen und dem Managementsystem für Informationssicherheit (ISMS) der Landesverwaltung sowie aus dem hessischen Landesamt für Verfassungsschutz zusammengezogen, um einen gemeinsamen Kompetenz- und

Der Hessische Innenminister Beuth spricht beim Cybersicherheits-Gipfel Hessen 2018

„Mit Hessen3C vernetzen und stärken wir die Sicherheitsbehörden."

Peter Beuth,
Hessischer Minister des Innern und für Sport

Expertenpool für Polizei, Landes-IT und Verfassungsschutz zu bilden und neue Technologien bereichsübergreifend bereitzustellen.

Neben einem gemeinsamen übergreifenden Cyber-Lagebild, dem Technologie-Radar (Technologietransfer) und dem Plattformbetrieb für moderne Analyse- und Auswertungsverfahren soll das Hessen3C auch den Austausch von Methodenwissen und – unter strenger Beachtung der rechtlichen Schranken – operativen Informationen zwischen allen Beteiligten optimieren.

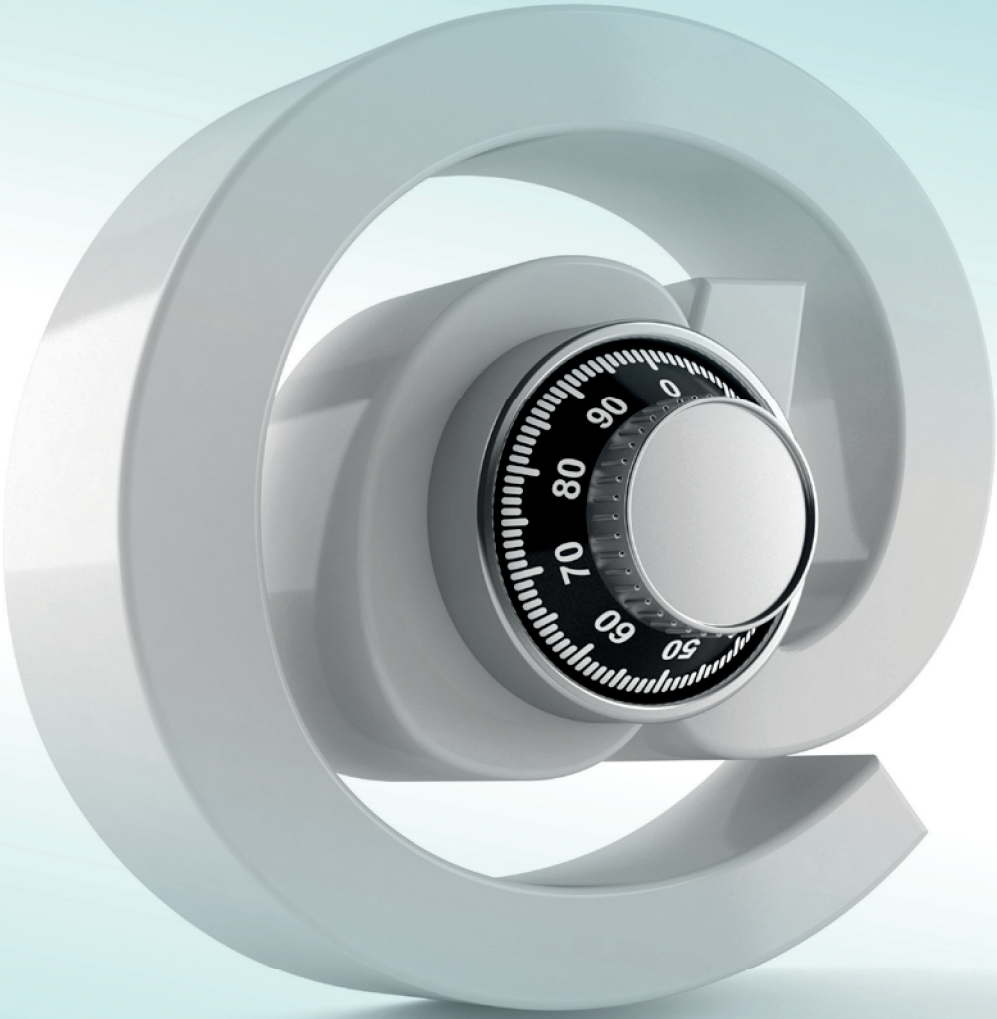
ANSPRECHPARTNER FÜR VERWALTUNG UND UNTERNEHMEN

Für die Verwaltung, für die Behörden des Bundes und die anderen Länder sowie für die hessischen Unternehmen steht mit dem Hessen3C ein rund um die Uhr verfügbarer, qualifizierter Ansprechpartner für alle Cyber-Fragen zur Verfügung. Das Hessen3C berät Unternehmen und Verwaltung kompetent, aber ergebnisoffen und absolut vertraulich. Gerade den Unternehmen soll so ein niederschwelliges Angebot für staatliche Unterstützung gemacht werden.

Das Hessen3C versteht sich als regionaler Partner bestehender Organisationen wie dem BSI oder der ZITiS (Zentralstelle für Informationstechnik im Sicherheitsbereich). Es bietet sich einerseits als Single-Point-of-Contact für Hessen an und andererseits als Multiplikator in der Fläche. Auch in Hessen sieht sich das Hessen3C nicht als Konkurrenz zu bestehenden Strukturen, beispielsweise in der Polizei, sondern als technische und methodische Unterstützung.

Zum BSI pflegt Hessen3C bereits heute enge und äußerst konstruktive Kontakte. Regelmäßig finden vertrauensvolle Abstimmungen mit der Verbindungsstelle des BSI in Wiesbaden statt. Dies insbesondere vor dem Hintergrund, Redundanzen zu vermeiden, neue Angebote des BSI zu besprechen und so den umfänglichen Service des BSI für Hessen wahrnehmen zu können. Beispielsweise nutzt Hessen3C die vom BSI erstellten Informationen für seine Beratungsarbeit, im Informationssicherheitsmanagement der Landesverwaltung und für den Warn- und Informationsdienst des CERT-Hessen. Ebenso nimmt Hessen die Möglichkeiten wahr, an Übungen des BSI für die Länder teilzunehmen, und das BSI unterstützt die Übungen des hessischen IT-Krisenmanagements (KRITEX) durch die Zuspielung von Übungseinlagen. Ein sehr guter Service und eine vorzügliche Zusammenarbeit, die in der Zukunft stetig weiter ausgebaut wird. ■

IT-SICHERHEIT IN DER PRAXIS



E-MAILS EINFACH VERSCHLÜSSELN

EasyGPG erleichtert den Schlüsselaustausch

von Dr. Christian Zier, Referat Kryptografie in Anwendungen

Die technische Möglichkeit, Ende-zu-Ende-verschlüsselte E-Mails auszutauschen, gibt es schon lange, so z. B. mit der freien Kryptografie-Software GNU Privacy Guard (GPG). Dass sie bisher wenig genutzt wird, liegt vor allem an dem aufwendigen Austausch der öffentlichen Schlüssel. Inzwischen gibt es aber viele Ansätze, um den Schlüsselaustausch zu erleichtern. Dazu zählt auch das BSI-Projekt EasyGPG.

In der analogen Welt achten wir auf den Schutz der Privatsphäre und halten ihn für eine Selbstverständlichkeit. Während eine Postkarte für jeden offen lesbar ist, werden Briefe und Pakete vor dem Verschicken zugeklebt und erst der Empfänger hat Zugang zum Inhalt. Manipulationen und unberechtigtes Öffnen würden bemerkt werden. Dieser Schutz der Privatsphäre ist bereits im Grundgesetz verankert. Art. 10 GG (1) lautet: Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich. Dies umfasst auch die Sicherheit der elektronischen Kommunikationsmittel wie Telefon oder E-Mail.

In der digitalen Welt entspricht die unverschlüsselte E-Mail der Postkarte, die potenziell für jeden lesbar ist. Viele Daten, die früher per Brief verschickt wurden, werden heute unverschlüsselt mit E-Mails versendet. Das können Passwörter sein, wichtige Arbeitsergebnisse oder private Informationen, die nicht an Dritte weitergegeben werden sollen. Durch Transportverschlüsselung wird die Kommunikation zwischen dem E-Mail-Client und seinem E-Mail-Service-Provider (ESP) abgesichert. Dieser leitet die Mail an den ESP des Empfängers weiter. Durch die Transportverschlüsselung wird das Mitlesen durch Unbefugte zwar stark erschwert, aber die beteiligten ESP haben noch immer Zugriff auf den Klartext der Mail. Daher reicht Transportverschlüsselung allein nicht aus, um drei wichtige Grundwerte der Informationssicherheit zu gewährleisten:

- **Vertraulichkeit:** Nur der berechtigte Empfänger kann den Inhalt der E-Mail lesen
- **Integrität:** Der Inhalt kann durch Dritte nicht unbemerkt verändert werden
- **Authentizität:** Die Nachricht stammt tatsächlich von dem angegebenen Absender

Diese Grundwerte können nur durch Ende-zu-Ende-Verschlüsselung (E2E) gewährleistet werden, bei der die Daten beim Absender verschlüsselt und erst beim Empfänger wieder entschlüsselt werden.

WIE FUNKTIONIERT VERSCHLÜSSELUNG?

Bei der Transportverschlüsselung wird zwischen Client und Server eine Verbindung aufgebaut und diese z. B. gemäß des weit verbreiteten Protokolls „Transport Layer Security“ (TLS) verschlüsselt. Alle Daten, die zwischen beiden Kommunikationspartnern ausgetauscht werden, sind nur während des Versands verschlüsselt. Nach Empfang werden sie automatisch entschlüsselt, sie liegen also im Klartext beim Client und Server vor.

Im Unterschied dazu wird bei E2E nicht der Kommunikationskanal verschlüsselt, sondern die einzelne E-Mail, die damit beim Sender und Empfänger verschlüsselt auf der Platte gespeichert wird. Sie ist natürlich auch beim Verschicken durch das Netz verschlüsselt, sodass auch die beteiligten ESP keinen Zugriff auf den Klartext der E-Mail haben.

Bei den Verschlüsselungsverfahren wird zwischen symmetrischen und asymmetrischen Verfahren unterschieden.

- Bei symmetrischer Verschlüsselung wird vom Sender und Empfänger derselbe Schlüssel sowohl zum Ver- als auch zum Entschlüsseln benutzt. Dieser Schlüssel muss vor der eigentlichen Kommunikation auf einem sicheren Weg zwischen Sender und Empfänger ausgetauscht und von beiden geheim gehalten werden. Für die Verschlüsselung von Nachrichten innerhalb großer und offener Nutzergruppen, so wie beim E-Mail-Verkehr, ist die symmetrische Verschlüsselung wegen der problematischen Schlüsselverteilung nicht geeignet.

- Bei der asymmetrischen Verschlüsselung wird ein Paar aus privatem und öffentlichem Schlüssel benutzt. Der private Schlüssel wird nur von dessen Eigentümer verwendet und geheim gehalten. Der zugehörige öffentliche Schlüssel wird allen potenziellen Kommunikationspartnern, z. B. allen Kunden eines E-Mail-Service-Providers, zur Verfügung gestellt. Der öffentliche Schlüssel kann mit einem herkömmlichen geöffneten Vorhängeschloss verglichen werden, das von jedem verschlossen werden kann, sich aber nur vom Besitzer des zugehörigen privaten Schlüssels wieder öffnen lässt. Um eine Nachricht sicher an einen Empfänger zu übermitteln, verschlüsselt der Absender seine Nachricht mit dem öffentlichen Schlüssel des Empfängers, der Empfänger entschlüsselt sie mit seinem privaten Schlüssel.

Die asymmetrische Verschlüsselung kann auch genutzt werden, um die Integrität einer Nachricht zu sichern. Dazu berechnet der Absender aus seiner Nachricht eine Prüfsumme, verschlüsselt diese mit seinem privaten Schlüssel und fügt die verschlüsselte Prüfsumme seiner Nachricht an. Dieser Vorgang entspricht einer digitalen Unterschrift (Signatur). Der Empfänger entschlüsselt die Prüfsumme mit dem öffentlichen Schlüssel des Absenders und vergleicht diese mit der Prüfsumme der empfangenen Nachricht. Wenn beide Prüfsummen übereinstimmen, ist er sicher, dass die Nachricht unterwegs nicht verfälscht wurde und vom Besitzer des privaten Schlüssels stammt.

Wird das erzeugte Schlüsselpaar formell und nachweislich mit einer E-Mail-Adresse assoziiert, ist sichergestellt, dass die Nachricht tatsächlich von der E-Mail-Adresse kommt, zu der das Schlüsselpaar gehört. Auf diese Weise kann auch die Authentizität des Absenders gewährleistet werden. Somit entspricht eine verschlüsselte und signierte E-Mail einem zugeklebten und versiegelten Brief.

Zur Verschlüsselung großer Datenmengen eignet sich das asymmetrische Verfahren allerdings weniger, da es sehr viel langsamer ist als das symmetrische Verfahren. Daher werden in der Praxis die Vorteile beider Verfahren als hybride Verschlüsselung kombiniert. Die zu schützenden Daten werden mit einem schnellen symmetrischen Verfahren verschlüsselt, und nur der dafür benutzte Schlüssel wird anschließend mithilfe des asymmetrischen Verfahrens verschlüsselt versandt.

Für den Austausch von E-Mails wird im Umfeld von Behörden und Firmen meistens das Protokoll S/MIME benutzt, im privaten Umfeld OpenPGP. Zwar verwenden beide die gleichen Algorithmen und Mechanismen für die Kryptografie, unterscheiden sich aber in der Schlüsselverwaltung, sodass sie nicht kompatibel miteinander sind.

WARUM WERDEN E-MAILS KAUM VERSCHLÜSSELT?

Bisher wird E2E nur sehr selten eingesetzt. Das ist unter anderem darauf zurückzuführen, dass die Hersteller weit verbreiteter Clients, wie z. B. Microsoft Outlook, E2E nicht anbieten. Anwender müssen sich selber darum bemühen, mit entsprechenden Plug-ins ihren Mail-Client um E2E zu erweitern (Gpg4win bei Outlook, Enigmail bei Thunderbird). Auch wenn bei der Installation und Konfiguration in den letzten Jahren die Nutzerfreundlichkeit durch weitgehende Automatisierung stark verbessert wurde, wird die Nutzung nach wie vor durch einen komplexen Schlüsselverteilungsprozess erschwert.

Bei OpenPGP wird der öffentliche Schlüssel üblicherweise auf einen Keyserver hochgeladen. Dabei wird nicht geprüft, ob der Schlüssel vom Besitzer der E-Mail-Adresse stammt, sodass jeder einen solchen Schlüssel für eine bestimmte Adresse auf einem Keyserver veröffentlichen kann. Bei der Suche nach einem Schlüssel anhand der Mail-Adresse werden so manchmal mehrere passende Schlüssel auf dem Keyserver gefunden, und es ist für den Nutzer nicht ohne weiteres möglich, den richtigen herauszufinden. Wird der falsche Schlüssel benutzt, so kann der berechtigte Empfänger die E-Mail nicht entschlüsseln, dafür aber derjenige, der den falschen Schlüssel hochgeladen hat.

„Eine verschlüsselte und signierte E-Mail entspricht somit einem zugeklebten und versiegelten Brief.“

Als weitere Möglichkeit kann der öffentliche Schlüssel dem Kommunikationspartner per E-Mail offen übersandt werden. Auch bei diesem Verfahren ist die Authentizität des öffentlichen Schlüssels nicht sichergestellt: Durch eine sogenannte „Man in the Middle Attacke“ könnte ein Angreifer diese Mail abfangen und den Schlüssel durch seinen eigenen öffentlichen Schlüssel ersetzen. Der Kommunikationspartner verschlüsselt seine Nachricht dann unwissentlich mit dem öffentlichen Schlüssel des Angreifers, der diese Nachricht dann mit seinem privaten Schlüssel lesen kann. Eine korrekte Assoziierung des Schlüssels mit der passenden E-Mail-Adresse ist also nicht zwingend gegeben und das Vertrauen in die Authentizität hängt auch davon ab, auf welchem Weg ein Schlüssel erhalten wurde. Versierte Nutzer können zwar untereinander über einen anderen Kommunikationskanal die eindeutige Prüfsumme eines Schlüssels (Hashwert) abgleichen und dessen Authentizität bestimmen, aber nutzerfreundlich ist das nicht.

EINE LÖSUNG DES PROBLEMS

Um auch die sichere Verteilung des öffentlichen Schlüssels nutzerfreundlich zu vereinfachen, wurde im BSI-Projekt „EasyGPG“ eine Lösung entwickelt, die die Erstellung, Anwendung und Verteilung der Schlüssel weitgehend automatisiert. Da zum ESP, der das E-Mail-Konto der Kunden betreibt, schon ein Vertrauensverhältnis besteht, soll dies auch für die Verteilung der öffentlichen Schlüssel genutzt werden. Bei der Installation der Software wird automatisch ein Schlüsselpaar erzeugt. Der öffentliche Schlüssel wird per E-Mail an den Provider geschickt. Dieser verifiziert die Veröffentlichungsanfrage durch eine verschlüsselte und signierte Antwort an den Nutzer, der diese durch einen einfachen Klick bestätigen kann. Dadurch wird der Schlüssel der richtigen Adresse eindeutig zugeordnet und die Adresse authentifiziert. Zudem werden Informationen über den Schlüssel, wie Gültigkeit oder Ersatz durch einen anderen Schlüssel, aktuell gehalten. Wenn nun ein Nutzer den so veröffentlichen Schlüssel eines Empfängers braucht, um eine E-Mail an ihn zu verschlüsseln, wird einfach wie üblich die E-Mail-Adresse des Empfängers im Adressfeld eingegeben. Ohne weiteres Zutun wird dann im Hintergrund der Schlüssel bei dessen ESP abgefragt und die E-Mail automatisch verschlüsselt. Der Schlüssel wird lokal im „Schlüsselbund“ gespeichert und kann zukünftig ohne Abfrage beim ESP benutzt werden.

Die Nutzung dieser Lösung setzt voraus, dass der ESP das in EasyGPG entwickelte Protokoll „Web Key Directory“ (WKD) unterstützt. Von dem Provider Posteo.de wird dieser Dienst bereits angeboten und mailbox.org hat die Unterstützung angekündigt. In naher Zukunft werden hoffentlich weitere Provider WKD unterstützen. Bis dahin kann sich auch ein Wechsel des Providers lohnen.

Bei allen Mail-Clients, die GnuPG ab Version 2.2 benutzen, wird der öffentliche Schlüssel automatisch abgefragt. Einschließlich des automatisierten Hochladens des öffentlichen Schlüssels an den ESP wird WKD von KMail unter Linux und Thunderbird mit dem Plug-in Enigmail sowohl unter Windows als auch unter Linux unterstützt. Mit dem Plug-in GpgOL von Gpg4win für Microsofts Outlook kann WKD ab der Version 3.1.0 ebenfalls in vollem Umfang genutzt werden. Für den textbasierten Client „mutt“ ist die Implementierung von WKD geplant.

Organisationen können über WKD authentifizierte Schlüssel zur einfachen Abfrage nach innen für Mitarbeiter bzw. nach außen für Kunden veröffentlichen. Bei kernel.org, KDAB.com und gnupg.org wird das schon gemacht. ■

Weitere Informationen: https://www.bsi-fuer-buerger.de/e-mail-verschluesselung

Praktikable Lösung

Schablonen für Informationssicherheit: Mehrere IT-Grundschutz-Profile veröffentlicht

von Birger Klein und Alexander Stanik, Referat IT-Grundschutz

Informationssicherheit, IT-Sicherheit, Datenschutz: Für viele Unternehmen und Behörden ist es immer noch herausfordernd, wichtige Aspekte der Informationssicherheit umzusetzen. Die Bandbreite der zu klärenden Fragen reicht von der Risikoanalyse über die sichere Speicherung vertraulicher Daten bis hin zur Sensibilisierung der Mitarbeiter für aktuelle Cyber-Angriffe. Der IT-Grundschutz liefert als bewährtes BSI-Angebot ein umfangreiches Portfolio von Empfehlungen und Hilfsmitteln, um die Informationssicherheit zu erhöhen. Damit können sowohl Einsteiger als auch fortgeschrittene Anwender arbeiten.

Mit der Modernisierung des IT-Grundschutzes wurde das Konzept der IT-Grundschutz-Profile in den IT-Grundschutz aufgenommen, um kleineren Unternehmen und Behörden den Weg zum Aufbau eines Managementsystems zur Informationssicherheit (ISMS) zu erleichtern. Anwendergruppen, die sich mit der Sicherheit eines bestimmten Informationsverbunds befasst haben, können ihre Ergebnisse aus diesen Überlegungen als IT-Grundschutz-Profil veröffentlichen. Dieses IT-Grundschutz-Profil kann weiteren Unternehmen und Behörden als Schablone für eigene, vergleichbare Sicherheitsbetrachtungen dienen. Ein Profil kann eine praktikable und überschaubare Lösung sein, um mit wenig personellem und finanziellem Aufwand die ersten Schritte in Richtung Informationssicherheit gehen zu können.

„Ein Profil hilft dabei, die Komplexität zu reduzieren und den ersten Schritt in die richtige Richtung zu machen.“

Heino Reinartz, Akteur beim Kommunen-Profil und IT-Sicherheitsbeauftragter der StädteRegion Aachen

SCHRITTE DES SICHERHEITSPROZESSES

In einem IT-Grundschutz-Profil werden die einzelnen Schritte eines Sicherheitsprozesses für einen definierten Anwendungsbereich dokumentiert. Dazu gehört:

- den Anwendungsbereich festzulegen,
- eine verallgemeinerte Strukturanalyse, Schutzbedarfsfeststellung und Modellierung für diesen Bereich durchzuführen,
- die umzusetzenden IT-Grundschutz-Bausteine auszuwählen und anzupassen sowie
- spezifische Sicherheitsanforderungen und -maßnahmen zu beschreiben.

Ziel ist es, dass perspektivisch ein breites Portfolio von IT-Grundschutz-Profilen als Musterszenarien für unterschiedliche Anwendungsfelder zur Verfügung gestellt wird.

IT-Grundschutz-Profile sind besonders für Branchen, Sektoren oder andere große Verbünde von Institutionen mit ähnlichen Bedingungen geeignet und können gut gemeinsam von Anwendergruppen erstellt werden. Gremien oder Anwendergruppen, die ein IT-Grundschutz-Profil für ein bestimmtes Anwendungsfeld erstellen möchten, sollten auch die zukünftigen Nutzer frühzeitig in den Prozess einbinden. Der intensive Austausch zwischen allen beteiligten Akteuren und ihren jeweiligen Anforderungen trägt in der Regel zu einem optimalen Ergebnis bei. Und zwar sowohl bei denjenigen, die das IT-Grundschutz-Profil erstellen, als auch bei den Anwendern, die im Anschluss damit arbeiten.

„Da die wichtigsten Punkte wie Strukturanalyse und Modellierung vorgegeben sind, können sich die Nutzer ganz auf die Umsetzung der Sicherheitsmaßnahmen konzentrieren. Erfahrenere Anwender können anhand eines Profils zügig überprüfen, welche Defizite noch existieren, um diese gezielt aufzuarbeiten."

Marcus Schröder, Akteur beim Kommunen-Profil und Berater Informationssicherheit und Datenschutz bei der SECURiON Rheinland-Pfalz GmbH

Zugleich kann auch eine einzelne Institution, beispielsweise ein Krankenhaus, für seine spezifischen Anforderungen ein IT-Grundschutz-Profil erstellen und dieses im Nachgang veröffentlichen. Dann können weitere Krankenhäuser ihre IT und ihr Informationsmanagement auf dieser Basis absichern. Die IT-Grundschutz-Profile können auf der BSI-Webseite veröffentlicht und so auch mit weiteren Anwendergruppen diskutiert werden. Ein einzelnes IT-Grundschutz-Profil kann dadurch mit der Zeit weiter ergänzt und verbessert werden.

PIONIERARBEIT:
ERSTES KOMMUNEN-PROFIL VERÖFFENTLICHT

Bereits im Mai 2018 wurde als erstes Profil ein IT-Grundschutz-Profil für Kommunen veröffentlicht. Es wurde in enger Abstimmung zwischen den kommunalen Spitzenverbänden Deutscher Landkreistag, Deutscher Städte- und Gemeindebund, Deutscher Städtetag und dem BSI erstellt. Das Profil soll als Schablone für IT-Verantwortliche in Kommunalverwaltungen dienen, die den IT-Grundschutz einsetzen wollen, um ihre Informationssicherheit zu erhöhen. Weitere IT-Grundschutz-Profile werden für unterschiedliche Branchen vorbereitet.

„Es entwickelte sich eine sachliche und vertrauensvolle, ebenenübergreifende Zusammenarbeit, während gleichzeitig die Vernetzung und Koordinierung der kommunalen Praktiker vorangebracht wurde."

Heino Sauerbrey, Akteur beim Kommunen-Profil ist beim Deutschen Landkreistag unter anderem für Informationssicherheit zuständig

Bei der bisherigen Erstellung von Profilen hat es sich jeweils als sehr fruchtbar erwiesen, wenn die engagierten Akteure aus den beteiligten Institutionen auch ihre Branchenverbände in den Prozess einbezogen haben.

„Zukünftig können neu entwickelte Musterszenarien einfach in IT-Grundschutz-Profile überführt und dokumentiert werden. Anwender, die an der Erstellung eines Profils mitwirken, gewinnen durch den fachlichen Austausch eine unvergleichbare Erfahrungs- und Wissensbasis für ihre weitere Arbeit."

Jens Lange, Akteur beim Kommunen-Profil und IT-Sicherheitsbeauftragter der Stadt Kassel

Neben dem veröffentlichten Profil für Kommunen sind auch zwei Masterarbeiten zu unterschiedlichen Profilaspekten durch das BSI betreut worden. Weitere IT-Grundschutz-Profile werden derzeit erarbeitet. Veröffentlichte IT-Grundschutz-Profile werden auf der BSI-Webseite veröffentlicht und kontinuierlich durch weitere ergänzt.

Das BSI unterstützt interessierte Anwender, die erstmalig ein IT-Grundschutz-Profil erstellen möchten, bei Fragen und hilft gegebenenfalls mit Kontakten zu anderen Institutionen. Zudem führt eine auf der BSI-Webseite veröffentlichte „Anleitung zur Erstellung eines IT-Grundschutz-Profils" durch den gesamten Prozess. Bei Fragen rund um das Thema IT-Grundschutz-Profile steht das Team des IT-Grundschutz-Referates zur Verfügung: **grundschutz@bsi.bund.de.** ■

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

http://info.it-sibe-forum.de
(Ansprechpartner für das Kommunen-Profil)

Signaturen bekämpfen Steuerbetrug im Einzelhandel

Schutzmaßnahmen für Registrierkassen

von Thomas Becker und Dr. Guido Frank, Referat eID-Technologien und Chipkarten

Im Zuge der Digitalisierung werden Geschäftsvorfälle heutzutage fast ausschließlich elektronisch erfasst. Hierdurch haben sich die technischen Herausforderungen für die Steuerprüfung, im Vergleich zu analogen Aufzeichnungen, stark verändert. Um Manipulationen an Kassenaufzeichnungen wirksam zu verhindern, sind daher technische Schutzmaßnahmen notwendig.

Nach den vom Bundesministerium der Finanzen veröffentlichten „Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff“ müssen elektronische Kassen Geschäftsvorfälle aufzeichnen. Diese elektronischen Aufzeichnungen müssen für die Steuerprüfung vorgehalten und bei Bedarf einem Steuerprüfer ausgehändigt werden. Die digitale Aufzeichnung von Geschäftsvorfällen erleichtert aber nicht nur die reguläre Buchführung, sie ermöglicht auch eine fast spurlose nachträgliche Manipulation.

Dies fängt bei der einfachen Nichtbuchung von Geschäftsvorfällen an und endet bei der hoch technisierten und automatischen Manipulation von Tageseinnahmen durch Spezialsoftware (s. u. Begriffserklärungen), die mit statistischen Hilfsmitteln eine Vielzahl von (kleinen) Manipulationen im Tagesgeschäft versteckt. Nicht unbeliebt ist auch die Verwendung einer sogenannten „Nirwanataste“. Mit ihr kann der zuletzt aufgezeichnete Vorgang mit nur einem Tastendruck wieder entfernt werden. Die Aufzeichnung landet im Nirwana, die Steuerlast gleich dazu.

Die gezielte Suche nach Schwachstellen im System ist hierbei ein lukratives Geschäftsmodell, das auch hohe Investitionen und zeitliche Aufwände zur Identifikation von aufwendig auszunutzenden Schwachstellen rechtfertigt.

Um solchen Manipulationen entgegenzuwirken, müssen elektronische Kassen ab dem 1. Januar 2020 mit einer zertifizierten Technischen Sicherheitseinrichtung (TSE) ausgestattet werden. Die technischen Vorgaben für die Sicherheitseinrichtung erstellt das BSI.

BEGRIFFSERKLÄRUNGEN

Zapper
Ein kurzzeitig an die Kasse angeschlossenes Gerät oder aufgebrachte Software die die aufgezeichneten Daten manipuliert.

Phantomware
Auf dem Kassensystem versteckte Software, zur automatisierten Manipulation von Daten

Nirwanataste
Taste an einer Kasse, die Aufzeichnungen verhindert, manipuliert, löscht oder ersetzt.

TECHNISCHE SICHERHEITSEINRICHTUNG

Die in den Vorgaben beschriebene Sicherheitseinrichtung wird direkt (oder über eine Netzwerkverbindung) mit einer Kasse verbunden und zeichnet alle Vorgänge kryptografisch signiert auf. Die Signatur selbst wird von einem speziellen Sicherheitsmodul in der Sicherheitseinrichtung erstellt. Die gesicherten Aufzeichnungen werden dann gespeichert und müssen vom Steuerpflichtigen, wie ungesicherte Aufzeichnungen jetzt auch schon, verfügbar gehalten werden. Finanzbehörden können die geschützten Daten einfordern und auf Vollständigkeit und Korrektheit prüfen.

Kassenhersteller oder Kassensoftware-Hersteller müssen die technische Sicherheitseinrichtung jedoch nicht unbedingt selbst entwickeln und zertifizieren, sondern können eine auf dem Markt verfügbare Sicherheitseinrichtung in ihr Kassensystem integrieren.

Das Sicherheitsmodul, als Kernelement der Sicherheitseinrichtung, signiert nicht einfach nur die Daten der Kasse, es fügt den Daten auch eine fortlaufende Transaktionsnummer sowie einen Zeitstempel hinzu. Dies sorgt für mehr Sicherheit, denn so kann erkannt werden, ob und wann es Lücken in den Aufzeichnungen gibt, ob eine Aufzeichnung gelöscht wurde oder unvollständig ist. Der Zeitstempel sorgt zudem für eine zeitgerechte Aufzeichnung der Steuerdaten. So wird ein Betrüger schnell in Erklärungsnot gegenüber dem Steuerprüfer geraten, wenn ihm – etwa zur besten Geschäftszeit – plötzlich Aufzeichnungen fehlen.

Ein weiterer wichtiger Bestandteil der Sicherheitseinrichtung ist die einheitliche Schnittstelle. Sie ermöglicht eine reibungslose Datenübertragung für Prüfzwecke und sorgt für die notwendige Interoperabilität. So ermöglicht sie einem Kassenhersteller die Sicherheitseinrichtung, unabhängig von einem konkret eingesetzten Sicherheitsmodul, an sein elektronisches Aufzeichnungssystem anzubinden.

Dies erleichtert die Integration und einen Austausch der Sicherheitseinrichtung über einen bestimmten Hersteller hinaus. Die Spezifikation der Schnittstelle basiert auf der „Secure Element API", einem allgemeinen Schnittstellenstandard nach BSI TR-03151, der auch in Zukunft leicht für weitere Anwendungsbereiche von Sicherheitselementen erweitert werden kann. Die Sicherheitseinrichtung muss nach den Vorgaben des BSI, also Technischen Richtlinien und Schutzprofilen, zertifiziert sein.

Die Zertifizierung sorgt für ein einheitliches Niveau an Sicherheit und Interoperabilität der technischen Sicherheitseinrichtung.

Die Zertifizierungspflicht beschränkt sich jedoch auf die Sicherheitseinrichtung, mit der die Aufzeichnungen des Kassensystems beim Starten des Aufzeichnungsvorgangs zu sichern sind. Eine Zertifizierung der Kasse (oder Kassensoftware) selbst ist also nicht erforderlich.

Der technologieoffene Ansatz der Vorgaben ermöglicht eine hohe Flexibilität bei der Umsetzung der Sicherheitsanforderungen. Hierdurch werden existierende Ansätze zur Sicherung von Aufzeichnungen nicht ausgeschlossen, sondern können gezielt um die notwendigen Anforderungen erweitert werden. Innovative Lösungen werden durch dieses Marktprinzip gefördert. So treiben die Sicherheitsvorgaben des BSI die Technologieentwicklung voran und sorgen für einen Sicherheitsfortschritt. ■

Weitere Informationen:
https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Grundaufzeichnungen/grundaufzeichnungen_node.html

DIGITALE GESELLSCHAFT

Digitaler Verbraucherschutz

Stärkere Unterstützung der Verbraucher in der digitalen Welt

von Florian Schumacher, Referat Cyber-Sicherheit für die Gesellschaft

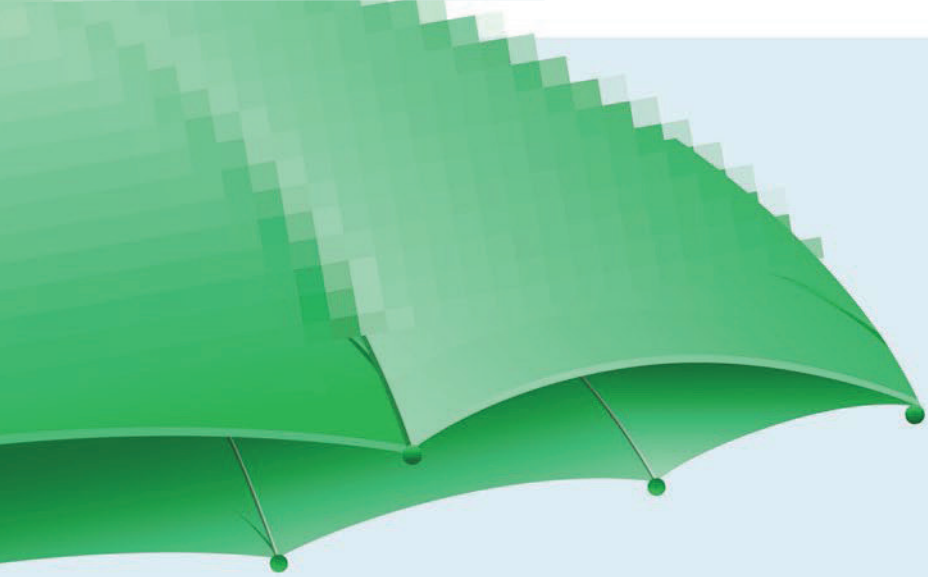
Besonders mit Blick auf die Gruppe der Verbraucher zeigt sich, dass Cyber-Sicherheit eine unverzichtbare Bedingung für das Gelingen der Digitalisierung in Deutschland ist. Das BSI baut seine Aktivitäten in diesem Bereich konsequent aus. Die Zusammenarbeit mit starken Partnern im Bereich des Verbraucherschutzes bildet dafür den Ausgangspunkt.

Die Digitalisierung sorgt zunehmend dafür, unsere Lebenswelten als Verbraucher im Alltag untrennbar zu vernetzen. Oftmals ist der Gewinn an Komfort aus unserem Leben nicht mehr wegzudenken. Smarte Technologien ermöglichen es uns, jederzeit und von jedem Ort aus auf Onlineangebote zuzugreifen und so zum Beispiel unsere Bankgeschäfte zu erledigen oder digitale Technologien in unserem Zuhause aus der Ferne zu steuern.

Doch mit diesen neuen Chancen gehen auch Risiken einher, insbesondere im Bereich der Cyber-Sicherheit. Sie betreffen besonders die individuelle Sicherheit jedes einzelnen Verbrauchers. Mit Cyber-Angriffen wird zum Beispiel versucht, in die Systeme von digitalen Diensteanbietern einzudringen, um sensible Daten der Verbraucher abzuschöpfen. Durch Entwicklungen im Bereich des Internet of Things (IoT) entstehen unsichere IT-Produkte, die Risiken für die öffentliche Sicherheit darstellen können. Der Fall des Mirai-Botnetzes belegt dieses Risiko eindrücklich. Dort wurden ungesicherte IoT-Geräte zu einem Botnetz zusammengeschlossen. Dies führte zu einem Ausfall zahlreicher Heim-Router als Folge einer versuchten Infektion mit Schadcode.

SCHUTZ DER VERBRAUCHER IN DER DIGITALEN WELT

Als die nationale Cyber-Sicherheitsbehörde gestaltet das BSI Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft. Aufgrund der genannten Risiken sind Verbraucher eine wichtige Zielgruppe, um die Cyber-Sicherheit zu stärken. Als herstellerunabhängige



und kompetente technische Stelle unterstützt das BSI die Verbraucher in der Risikobewertung von Technologien, Produkten, Dienstleistungen sowie Medienangeboten und befähigt sie damit zur Auflösung von Unsicherheiten. Damit kann die gesellschaftliche Widerstandsfähigkeit gegen Cyber-Gefahren jeglicher Art erhöht werden.

Unter dem Begriff des „Digitalen Verbraucherschutzes" möchte das BSI die Maßnahmen in diesem Bereich zukünftig bündeln und die bestehenden Aktivitäten verstärken. Auch im Koalitionsvertrag der Bundesregierung vom Februar 2018 wird der Verbraucherschutz in der digitalen Welt aufgewertet. Konkret heißt es dort, dass der „Verbraucherschutz als zusätzliche Aufgabe des BSI" etabliert werden soll.

ZIELE IM DIGITALEN VERBRAUCHERSCHUTZ

Durch seine Aktivitäten im Bereich des digitalen Verbraucherschutzes möchte das BSI die Verbraucher insbesondere in der Beurteilungsfähigkeit und der Lösungskompetenz stärken, um die Resilienz in der Gesellschaft gegen Cyber-Gefahren zu steigern. So kann bestehenden Unsicherheiten begegnet werden.

Für Verbraucher ist es zurzeit nahezu unmöglich, beim oder auch nach dem Kauf von Hard- und Softwareprodukten deren Sicherheit und Sicherheitseigenschaften qualifiziert einzuschätzen. Daher müssen sie befähigt werden, auch in der digitalen Welt informierte und mündige Entscheidungen zu treffen und Sicherheitsrisiken besser einzuschätzen. Gleichzeitig besteht bei Teilen der Verbraucher eine unzureichende Handlungskompetenz im Feld der Informations- und Cyber-Sicherheit. Daher möchte das BSI dieser Gruppe durch ein Maßnahmenbündel im digitalen Verbraucherschutz Instrumente zur Seite stellen, um die Beurteilungs- und Lösungskompetenz zu steigern.

Hierdurch wird der Aufgabe der Förderung der Sicherheit in der Informationstechnik Rechnung getragen. Daneben leistet das BSI einen wichtigen Beitrag sowohl zur individuellen Sicherheit, als auch der öffentlichen als Ganzes.

ZUSAMMENARBEIT MIT PARTNERN

Cyber-Sicherheit ist eine gesamtgesellschaftliche Aufgabe. Das BSI nimmt die Gestaltungsaufgabe im Bereich der Informationssicherheit in einem ausgeprägten kooperativen Ansatz und in Zusammenarbeit mit zahlreichen Partnern wahr. So wurde etwa im März 2017 ein Memorandum of Understanding zwischen dem BSI und der Verbraucherzentrale Nordrhein-Westfalen (VZ NRW) e.V. abgeschlossen (siehe BSI-Magazin 01/2018). Beide Seiten vereinbarten, im Rahmen einer kontinuierlichen, vertrauensvollen Kooperation gemeinsam an konkreten Themen der Informationssicherheit zu arbeiten und so von der gegenseitigen Expertise und den rechtlichen Befugnissen und Fähigkeiten zu profitieren.
Ein Beispiel für die erfolgreiche Zusammenarbeit stellt das partnerschaftliche Vorgehen bei Smartphones dar, die im Handel als neu angeboten werden, für die aber keine Sicherheitsupdates mehr durch den Hersteller angeboten werden. Hierdurch bestehen bei der Nutzung teils gravierende Gefahren. Über diesen Umstand werden Verbraucher nur unzureichend informiert. Mit der Unterstützung des BSI ging die Verbraucherzentrale NRW gegen den Verkäufer des betroffenen Geräts vor und leitete ein gerichtliches Unterlassungsverfahren ein. Die erste mündliche Verhandlung fand im August 2018 beim Landgericht Köln statt. ■

Weitere Informationen: https://www.bsi.bund.de/digitaler-Verbraucherschutz

Digitale Transformation

Den Menschen mitnehmen

von Joachim Gutmann

Ein wichtiger und oft unterschätzter Faktor der Digitalisierung ist der damit verbundene kulturelle Wandel in den Unternehmen. Dazu gehören Werte und Prozesse wie Eigenverantwortung, Fehlertoleranz, Teamarbeit und agile Prozesse. Entsprechend hinderlich sind Strukturen und Denkschemata, die hierarchisches und machtfixiertes Verhalten fördern. Das gilt auch, wenn es darum geht, Maßnahmen für mehr Cyber-Sicherheit im Unternehmen zu etablieren.

Der digitale Wandel verändert unseren Alltag, das Lernen in Schulen und Universitäten ebenso wie ökonomische Abläufe und Prozesse, die Arbeitswelt und die Arbeitskultur in den Unternehmen. Digitalisierung durchdringt unser Lebensumfeld. Fast jeder bestellt online, vom Buch bis zum Baumaterial, und was er digital bestellt, bewertet er auch digital. Wir finden Freunde und Partner, Jobs und Geld im Internet. In der Netzökonomie werden Wissen und Meinung sozial geteilt. Die Möglichkeit, Wissen und Apps mobil aufrufen zu können, gibt uns Sicherheit in jeder Umgebung und unterstützt im Alltag.

Dieser intuitive, sinngesteuerte Umgang mit den Formaten und Früchten der Digitalisierung bringt neue kulturelle und soziale Werte sowie Normen mit sich, er macht aus dem technologischen einen kulturell-gesellschaftlichen Wandel. Und der hört am Werkstor nicht auf. Für Unternehmen und Führungskräfte bedeutet Digitalisierung nicht nur eine Neuausrichtung der Prozesse und Abläufe, sondern auch der Arbeits- und Unternehmenskultur.

MEHR MITGESTALTUNG UND MEHR VERANTWORTUNG

Die Arbeitnehmer von heute wollen wesentlich aktiver und kreativer ihr Unternehmen mitgestalten. Sie erwarten künftig viel mehr Mitsprache, Transparenz und Teilhabe. Sie bringen ihre im Privatleben erworbenen digitalen Kompetenzen in das Unternehmen ein. Und sie wissen, dass auch die Cyber-Sicherheit ihres Unternehmens von ihrem selbstverantworteten und verantwortlichen Umgang mit dem digitalisierten Arbeitsumfeld abhängt. Mit einem Satz: Die Zukunftsfähigkeit von Organisationen hängt erheblich von deren Fähigkeit ab, die Führungskultur den Mitarbeitererwartungen im digitalen Zeitalter anzupassen. Gefordert ist eine offene, transparente, partizipative Unternehmens- und Führungskultur.

Viele traditionelle Geschäftsmodelle sind durch die Digitalisierung bedroht, jedes Unternehmen muss sorgfältig prüfen, welche Technologien entweder bedrohlich werden oder aber eine grundsätzliche Erneuerung von Prozessen und Produkten erlauben. Doch die Change-Projekte stoßen dort an Grenzen, wo die Menschenbilder nicht deckungsgleich mit denjenigen des antizipierten Zielbildes sind. Differenzen zeigen sich häufig in Führungs- und Steuerungssystemen. Unternehmen möchten sich in die Richtung von agilen, selbstorganisierten, lernenden Systemen bewegen. Gleichzeitig dominiert häufig die Vorstellung eines faulen und unselbstständigen Menschen. Führungskräfte trauen es ihren Mitarbeitern oft nicht zu, Entscheidungen zu treffen, oder befürchten, dass diese das Homeoffice als Freizeiteinrichtung sehen. Wollen Unternehmen ihre Systeme tatsächlich Richtung Agilität bewegen, kommen sie nicht darum herum, neue Führungsstrukturen und eine neue Unternehmenskultur aufzubauen.

CYBER-SICHERHEIT VON UNTEN AUFBAUEN

In der aktuellen Diskussion um Cyber-Sicherheit in Unternehmen gilt der Mitarbeiter als größter Risikofaktor. Unbedarft genutzte USB-Sticks, versehentlich geöffnete Spam-Mails, privates Surfen auf schadhaften Websites – viele Situationen können der Türöffner für folgenschwere Viren und Malware sein. Auch bei einer Umfrage der Allianz für Cyber-Sicherheit, einer Initiative des BSI, landeten die Mitarbeiter auf Platz eins der größten Sicherheitslücken. Über die Hälfte der befragten Unternehmen gab an, dass Kollegen, Lieferanten oder Zeitarbeiter den digitalen Übergriff durch Cyber-Kriminelle überhaupt erst möglich gemacht hätten.

Das Gegenmittel? Natürlich interne Aufklärungsarbeit, Sensibilisierung, Schulung, Regeln zum Umgang mit externen Datenträgern. Sicher notwendig, aber in einem digitalisierten Unternehmen wird das nicht reichen. Denn es funktioniert nicht mehr nach dem Prinzip Anweisung von oben, Ausführung unten. Es hat keine feste Belegschaft mehr, und erst recht sind nicht alle Beschäftigten gut kontrollierbar zu einer Zeit an einem Ort versammelt. ■

DAS DIGITALISIERTE UNTERNEHMEN IST ERFOLGREICH, WENN ES FÜR FOLGENDE FAKTOREN ANTWORTEN GEFUNDEN HAT:

1

Im digitalisierten Unternehmen werden Aufgaben stärker als bisher in Netzwerken organisiert und im Team ausgeführt. Viele Beschäftigte werden Mitglied in mehreren Teams sein. Teams werden unternehmensübergreifend mit externen Experten, mit Kunden- oder Lieferantenmitarbeitern oder mit Crowdworkern ergänzt und angereichert werden. Dafür braucht es soziale Kompetenz und genügend Prozesswissen, um mit anderen Teammitgliedern und Netzwerkpartnern Verbindungen eingehen zu können. Dafür muss die Teamfähigkeit aller Beteiligten systematisch gefördert, entwickelt, geübt und immer wieder reflektiert werden.

2

Die Arbeit in selbstorganisierten Netzwerken mit dezentraler Entscheidungsfindung und ohne feste Bindung an einen über Raum und Zeit definierten Arbeitsplatz bietet ein hohes Maß an Autonomie. Dadurch steigt die Selbstverantwortung des Einzelnen ebenso wie die Selbstbestimmung in der Zusammenarbeit. Ein Erfolgsfaktor dafür ist eine Vertrauenskultur, die das hierarchische Anweisen und die Kontrolle durch ein kollegiales Coaching ersetzt.

3

Der durch die Digitalisierung veränderte Handlungsrahmen, in dem wir agieren und kommunizieren, verlangt eine neue Führung. Führungskräfte müssen Komplexität verstehen und steuern können. Sie müssen in der Lage sein, unterschiedliche kulturelle Hintergründe, Gewohnheiten, Wertesysteme und Generationenunterschiede auszubalancieren. Sie müssen mit einer klaren, unmittelbaren und offenen Haltung Selbstverantwortung vorleben – gerade auch im Sinne einer stabilen und nachhaltigen Unternehmensentwicklung.

Elektronische Identitäten europaweit nutzen

Europäisches eID-System im September gestartet

von Dr. Jens Bender und Dr. Guido Frank, Referat eID-Technolgien und Chipkarten

Am 29. September 2018 trat der wichtigste Baustein des eID-Teils der europäischen eIDAS-Verordnung in Kraft: die gegenseitige Anerkennung. Hierdurch entsteht eine eID-Landschaft für den gesamten europäischen Wirtschaftsraum. Mit der Notifizierung der Online-Ausweisfunktion ist Deutschland hier ganz vorne mit dabei.

Mit der „Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt" – eIDAS-Verordnung – wurden 2014 erstmals einheitliche, europaweit geltende Rahmenbedingungen für die gegenseitige Anerkennung von elektronischen Identifizierungsmitteln und Vertrauensdiensten festgelegt (siehe auch BSI-Magazin 02/2016).

Im Bereich der elektronischen Identifizierung wird durch die Verordnung keine einheitliche „europäische Identität" geschaffen, sondern es werden – unter bestimmten Voraussetzungen – die elektronischen Identifizierungssysteme der Mitgliedstaaten gegenseitig anerkannt.

Grundlage für die gegenseitige Anerkennung ist die „Notifizierung" der eID-Systeme durch die jeweiligen

Mitgliedstaaten. Sie dient dazu, den anderen EU-Ländern offiziell bekannt zu machen, dass die Anforderungen der eIDAS-Verordnung eingehalten werden.

Während die Notifizierung auf freiwilliger Basis erfolgt, ist die Anerkennung notifizierter eID für öffentliche Stellen seit dem 29. September 2018 verpflichtend.

ERSTE EIDAS-NOTIFIZIERUNG DURCH DEUTSCHLAND

Im September 2017 hat Deutschland als erstes Land die Notifizierung der Online-Ausweisfunktion des Personalausweises und elektronischen Aufenthaltstitels auf dem höchsten Vertrauensniveau gemäß eIDAS-Verordnung erfolgreich abgeschlossen. Im Rahmen der Notifizierung wurde in einem Peer Review das deutsche eID-System durch die anderen Mitgliedstaaten der EU/des europäischen Wirtschaftsraums begutachtet. Im Beschluss durch das Kooperationsnetzwerk – das für die Koordination der eID-Themen zuständige EU-Gremium – wurde dem deutschen System auf Basis des Abschlussberichts des Peer Review bescheinigt, dass die Anforderungen an das eIDAS-Vertrauensniveau „hoch“ eingehalten werden.

Das BSI hat die wesentlichen Vorarbeiten für die Notifizierung der Online-Ausweisfunktion geleistet und den gesamten Notifizierungsprozess aus technischer Sicht begleitet.

Seit Ende September 2018 sind alle EU-/EWR-Mitgliedstaaten verpflichtet, die Online-Ausweisfunktion für Anwendungen des öffentlichen Sektors, d. h. insbesondere im eGovernment, anzuerkennen. Auch Unternehmen im EU-Ausland können den elektronischen Identitätsnachweis auf freiwilliger Basis anerkennen.

Natürlich setzt die gegenseitige Anerkennung von elektronischen Identitäten neben der Notifizierung auch voraus, eine technische Interoperabilitätsinfrastruktur aufzubauen. Dazu haben die Mitgliedstaaten gemeinsam technische Schnittstellen abgestimmt, über die die nationalen Systeme grenzüberschreitend kommunizieren können. Um den anderen Mitgliedstaaten eine Identifizierung mit dem deutschen Personalausweis zu ermöglichen, stellt das BSI diesen eine „eIDAS-Middleware“ – einen auf die Interoperabilitätsinfrastruktur zugeschnittenen eID-Server – zur Verfügung.

UMSETZUNG IN DEUTSCHLAND

Auch bei der Anerkennung elektronischer Identitäten anderer Mitgliedstaaten im deutschen eGovernment laufen die Vorbereitungen mit Unterstützung des BSI auf Hochtouren. Im EU-Förderprojekt TRans-European AuThentication Services (TREATS) wurde die Infrastruktur für die technische Integration in das deutsche eID-System geschaffen. Zurzeit wird diese Infrastruktur in die eGovernment-Anwendungen integriert, sodass Deutschland für die Anerkennungsverpflichtung nach eIDAS zum September 2018 vorbereitet sein wird.

AUSBLICK

Im ersten Quartal 2018 haben mit Estland, Spanien, Kroatien, Italien und Luxemburg fünf weitere Länder die Notifizierung ihrer eID-Systeme eingeleitet, gefolgt von Belgien und Portugal im zweiten Quartal. Mit weiteren Notifizierungen ist im Laufe des Jahres zu rechnen.

Auch auf nationaler Ebene hat sich einiges getan. So wurden mit einer Änderung des Personalausweisgesetzes im Juli 2017 neue Anwendungsmöglichkeiten geschaffen, etwa das „Vor-Ort-Auslesen“. Dabei handelt es sich um die elektronische Übernahme von Ausweisdaten in Formulare ohne umständliches Abtippen. Sie wird zurzeit technisch nach Vorgaben des BSI umgesetzt. Ebenfalls auf gutem Wege ist die Verwendung des Ausweises mit mobilen Geräten. Durch die kontaktlose Schnittstelle des Ausweischips kann dieser mit geeigneten NFC-fähigen Smartphones genutzt werden (https://www.ausweisapp.bund.de/mobile-geraete/). Softwarebibliotheken ermöglichen auch eine direkte Integration in eigene Apps. Da ein Großteil der Bürgerinnen und Bürger mit der Online-Ausweisfunktion ausgestattet ist, lohnt es sich für Diensteanbieter, diese sichere Art der Identifizierung in Onlineprozesse zu integrieren. Für das eGovernment ist die Integration mit dem Online-Zugangsgesetz (OZG) sogar verpflichtend, sodass künftig mit vielen weiteren eID-unterstützten Angeboten zu rechnen ist. ■

Weitere Informationen:

Notifizierung der deutschen Online-Ausweisfunktion: https://www.bsi.bund.de/eIDAS-Notifizierung

Interoperabilität im Rahmen der eIDAS-Verordnung: https://www.bsi.bund.de/eIDAS-Interoperabilitaet

Die eIDAS-Verordnung und die Online-Ausweisfunktion: https://www.personalausweisportal.de/DE/Verwaltung/eIDAS_Verordnung_EU/eIDAS_Verordnung_EU_node.html

Starke Kunden-authentifizierung nach PSD2

Herausforderung für die IT-Sicherheit

von Sabine Mull, Referat Cyber-Sicherheit für die Digitalisierung im Gesundheits- und Finanzwesen

Mit der neuen EU-Richtlinie über Zahlungsdienste im Binnenmarkt als überarbeitete und aktualisierte Payment Services Directive (PSD) soll der Wettbewerb im europäischen Zahlungsverkehr nicht nur gefördert werden: Er soll auch sicherer, bequemer und billiger werden. Daher werden nun auch onlinebasierte Zahlungsdienste betrachtet.

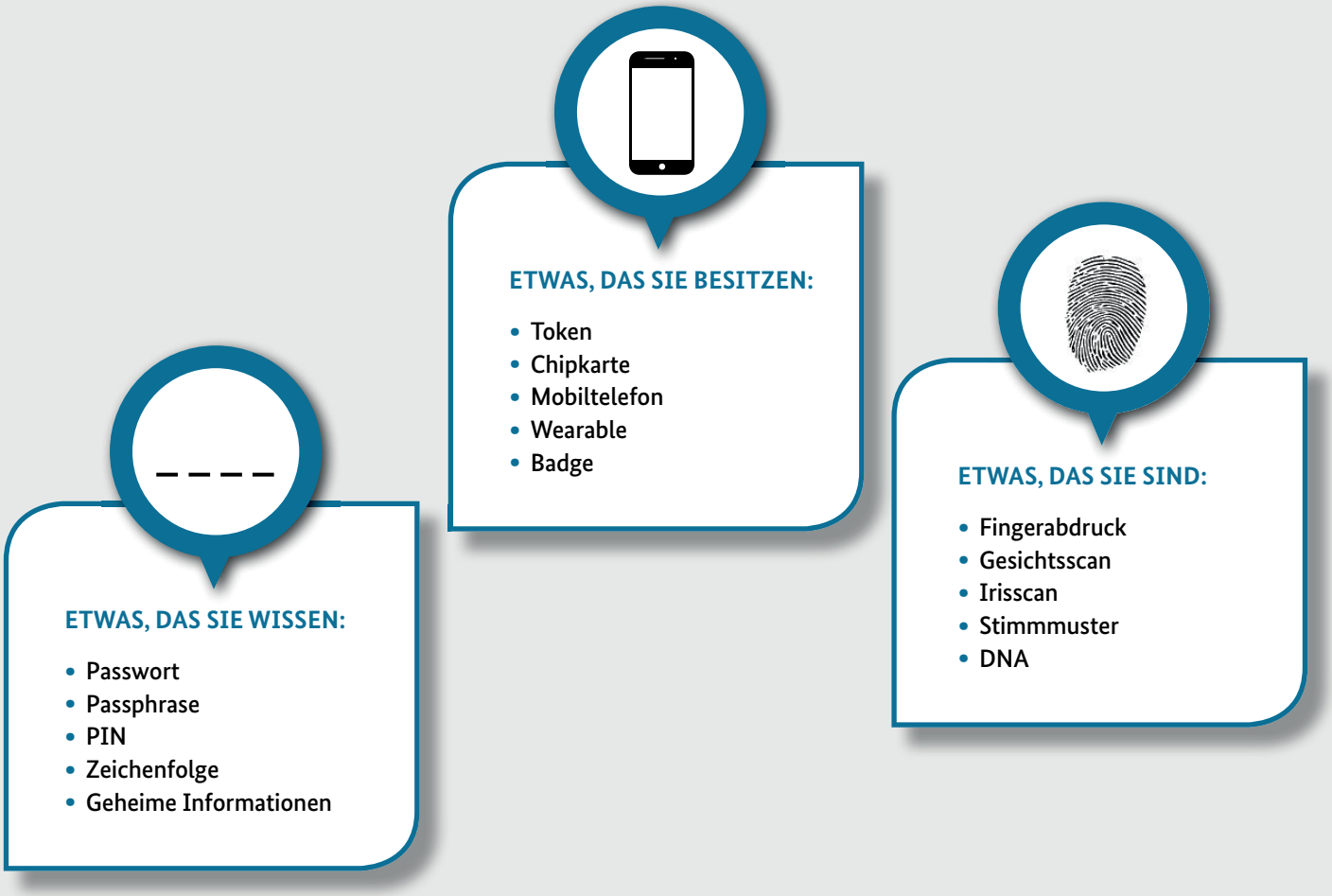
Im Januar 2016 wurde die neue Richtlinie des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt – kurz PSD2 – veröffentlicht. Nicht länger ausschließlich Banken haben nun mehr Zugang zu den Kontodaten von Privatkunden, auch Drittanbieter erhalten jetzt diese Möglichkeit. Jeder Kunde kann einen sogenannten Dritten Zahlungsdienstleister beauftragen, in seinem Namen Zahlungsaufträge gegenüber dem eigenen Kreditinstitut auszulösen. Drittanbieter erhalten so den direkten Zugriff auf Konto- und Kundeninformationen. So wird ihnen der Zugang zum Zahlungsmarkt erleichtert.

Dazu ist es erforderlich, die Schnittstelle zwischen Kunden und Kreditinstitut für den Dritten Zahlungsdienstleister zu öffnen. Die PSD2 stellt hier die Anforderung an die Banken, passende Schnittstellen für den Zugang zu Kontodaten bereitzustellen. Wie diese auszusehen hat, ist in der PSD2 allerdings nicht definiert.

SICHERHEIT VERBESSERN

Doch nicht nur der Wettbewerb soll gestärkt, auch die Sicherheit, vor allem bei der Übermittlung von Daten, soll verbessert werden. Die PSD2 sieht hier eine verstärkte Kundenauthentifizierung vor. Das führt dazu, dass Kreditinstitute ihre bisher genutzten Systemedaraufhin überprüfen müssen, ob sie den geforderten Sicherheitsstandards gerecht werden. Zusätzlich müssen die Kreditinstitute sicherstellen, dass Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale der Zahlungsdienstnutzer geschützt werden.

Die PSD2 beschreibt, in welchen Fällen die starke Kundenauthentifizierung einzusetzen ist (Artikel 97), konkretisiert die technischen Anforderungen an die Verfahren jedoch nicht. Nach PSD2, Artikel 98 obliegt es der Europäischen Bankenaufsichtsbehörde (EBA) in enger Zusammenarbeit mit der Europäischen Zentralbank (EZB), sogenannte Technische Regulierungsstandards (RTS) für die Authentifizie-



rung und die Kommunikation zu definieren. Dort werden die wesentlichen Grundlagen zur konkreten Umsetzung der Richtlinie vorgegeben. Sie werden durch die EU-Kommission als deligierte Rechtsakte erlassen und im Amtsblatt der Europäischen Union veröffentlicht. Dadurch haben sie eine unmittelbare Wirkung. Sie sind jedoch rein technischer Natur und beinhalten keine strategischen oder politischen Entscheidungen.

Der RTS für die Authentifizierung und die Kommunikation ist im März 2018 in Kraft getreten und muss ab September 2019 angewendet werden. Eine starke Kundenauthentifizierung nach PSD2 ist immer dann zwingend vorgeschrieben, wenn der Zahler beispielsweise online auf sein Zahlungskonto zugreift oder einen elektronischen Zahlungsvorgang auslöst.

Sie ist dann stark, wenn mindestens zwei Elemente aus den Kategorien Wissen (etwas, das nur der Nutzer weiß), Besitz (etwas, das nur der Nutzer besitzt) oder Inhärenz (etwas, das der Nutzer ist) herangezogen werden. Diese Elemente sollen dabei insofern voneinander unabhängig sein, als dass die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht infrage stellt. Durch die Unabhängigkeit der Elemente kann das Betrugsrisiko verringert werden, auch wenn die Sicherheit eines Kriteriums nicht mehr gegeben ist. Gleichzeitig soll die starke Kundenauthentifizierung so konzipiert sein, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist. Wird ein Element nicht korrekt eingegeben, darf nicht erkennbar sein, um welches Element es sich handelt. Artikel 4, PSD2.

ZWEI-FAKTOR-AUTHENTIFIZIERUNG

Die Forderung der PSD2 nach einer starken Kundenauthentifizierung ist erfüllt, sobald das Authentifizierungsverfahren zwei dieser drei voneinander unabhängigen Elemente kombiniert.

Allerdings wird nicht vorgegeben, in welcher Form die Elemente kombiniert werden sollen, um ein angemessenes Maß an Sicherheit bzw. das Vertrauensniveau zu erreichen, das einem Angreifer Widerstand leisten kann.

Dabei ist gerade für Nutzer des Online-Bankings in allen seinen Ausprägungen die Sicherheit der persönlichen Kontodaten und der Schutz vor Angriffen von großer Bedeutung. Hier würde sowohl Herstellern entsprechender Geräte und Verfahren zur Authentifizierung als auch Instituten eine Entscheidungsgrundlage gegeben, wenn die Anforderungen zur Unabhängigkeit der Elemente und damit die Benennung von offensichtlichen Verletzungen der Unabhängigkeit konkretisiert würden, um zukünftige Innovationen auf diesem Gebiet besser bewerten und einordnen zu können. Das aber leistet PSD2 nicht.

Das BSI kümmert sich daher im Rahmen seiner Aufgaben nicht nur in vielfältigen Aktivitäten um die Bewertung von IT-Systemen, die im Kontext des (elektronischen) Zahlungsverkehrs genutzt werden. Es untersucht auch moderne Bezahlverfahren hinsichtlich ihrer Sicherheitseigenschaften, um Empfehlungen für deren Einsatz gegenüber Herstellern und Nutzern zu geben. Das BSI bietet so in einem häufig unübersichtlichen Umfeld verschiedenster Technologien, Protokollen und Standards eine Orientierungshilfe auch für Verfahrensanbieter und deren Kunden.

Zusätzlich arbeitet das BSI daran, regulatorische Vorgaben wie die starke Kundenauthentifizierung aus technologischer Sicht zu konkretisieren. Dies geschieht in Form von Anforderungspapieren, die Marktteilnehmern Orientierung bei der Umsetzung der regulatorischen Anforderungen bieten.

Ein Papier zur Planung von Leitlinien, wie sich die in der PSD2 geforderten Kontoschnittstelle für Drittanbieter umsetzen lässt, sowie ein Statement zum Thema „Starke Kundenauthentifizierung“ wurden als Ergebnisse bereits auf

PSD2

Aufsichtliche Regelungen für mehr Sicherheit und Wettbewerb im Zahlungsverkehr

von Dr. Felix Strassmair-Reinshagen, Bundesanstalt für Finanzdienstleistungsaufsicht

Die Zweite Zahlungsdiensterichtlinie der EU – auch bekannt als PSD2 (Payment Service Directive 2) hat drei Ziele: den bestehenden europäischen Rechtsrahmen für Zahlungsdienste fortzuentwickeln, den Wettbewerb und die Sicherheit bei elektronischen Zahlungen zu verbessern und die Kundenrechte bei der Nutzung von Zahlungsdiensten zu stärken. Die Richtlinie war bis zum 13. Januar 2018 in das nationale Recht umzusetzen. In Deutschland ist dies dadurch geschehen, dass die privatrechtlichen Regelungen der Richtlinie im BGB bzw. im EGBGB umgesetzt wurden, während sich die aufsichtlichen Regelungen in einer Neufassung des Zahlungsdiensteaufsichtsgesetzes (ZAG) wiederfinden. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ist zuständige Aufsichtsbehörde für das ZAG.

Zu den wesentlichen Neuerungen des novellierten ZAG gehört, dass es eine starke Kundenauthentifizierung fordert, wenn ein Zahler eine elektronische Zahlung auslöst. Ein Zahlungsdienstleister kann nur noch im Ausnahmefall davon abweichen. Die zulässigen Ausnahmen sind in einer delegierten Verordnung der EU-Kommission geregelt. Anforderungen zur Kundenauthentifizierung finden sich zwar bereits im BaFin-Rundschreiben über „Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI)“; das ZAG und die Delegierte Verordnung wenden diese Anforderungen nun aber auch auf elektronische Zahlungen außerhalb des Internets (z.B. an der Ladenkasse) an und verschärfen sie noch in einigen Punkten.

der Webseite des BSI unter dem Schlagwort „Elektronischer Zahlungsverkehr“ veröffentlicht. Weitere Papiere in dem Bereich werden in unregelmäßiger Folge veröffentlicht. Ideen für Themen zu weiteren Einzelveröffentlichungen werden gerne entgegengenommen. ■

Weitere Informationen:
www.bsi.bund.de/payment

Kurzprofil Dr. Felix Strassmair-Reinshagen

Dr. Felix Strassmair-Reinshagen ist als Referent bei der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) in der Gruppe IT-Aufsicht tätig. Schwerpunkt seiner Tätigkeit sind die regulatorischen Anforderungen im Zahlungsverkehr. Er begann seine Berufstätigkeit als wissenschaftlicher Mitarbeiter der Monopolkommission. Nach dem Einstieg 2012 bei der BaFin war er zuerst in der Aufsicht über Investmentfonds eingesetzt, bevor er verschiedene Aufgaben in der Bankaufsicht übernahm.“

Um die dafür nötigen Umstellungen zu ermöglichen, hat der europäische Gesetzgeber dem Markt in diesem Punkt eine längere Umsetzungsfrist zugestanden. Die Starke Kundenauthentifizierung wird erst ab dem 14. September 2019 zur Pflicht. Viele Bankkunden werden die Änderungen aber schon früher bemerken, weil die Zahlungsdienstleister bereits dabei sind, ihre Systeme anzupassen.

Daneben stellt die PSD2 zwei neu normierte Zahlungsdienste unter Aufsicht, und zwar den Zahlungsauslöse- und den Kontoinformationsdienst. Zwar wurden diese Geschäftsmodelle in Deutschland bereits seit einiger Zeit ausgeübt, mit der Richtlinie wird aber der Streit über ihre Legalität beendet und gleichzeitig ein Rechtsrahmen für ihre geordnete Ausführung geschaffen. Unternehmen, die diese Dienste erbringen, müssen eine Zulassung bei der BaFin beantragen. Die meisten Kreditinstitute sind allerdings bereits gesetzlich zur Erbringung aller Zahlungsdienste zugelassen.

Um eine geordnete Ausführung dieser neuen Geschäftsmodelle zu ermöglichen, sieht die PSD2 unter anderem vor, dass Zahlungsauslöse- und Kontoinformationsdienstleister nur mit ausdrücklicher Zustimmung des Kunden auf dessen Konto zugreifen dürfen. Zudem müssen sie sich für den Zugriff auf das Konto beim kontoführenden Zahlungsdienstleister (üblicherweise die Bank des Kunden) identifizieren. Dafür müssen sie ein qualifiziertes Zertifikat nach der europäischen eIDAS-Verordnung verwenden. Auch diese Regelungen werden am 14.09.2019 anwendbar.

Bei der Umsetzung des ZAG arbeitet die BaFin auch intensiv mit dem BSI zusammen. Zum Beispiel tauschen die beiden Behörden Informationen aus Meldungen über Sicherheitsvorfälle aus, welche sie jeweils im Rahmen ihrer gesetzlichen Zuständigkeiten erhalten; dabei müssen Betreiber kritischer Infrastrukturen aus dem Finanzsektor Sicherheitsvorfälle an das BSI melden, die Zahlungsdienstleister dagegen an die BaFin. Zudem greift die BaFin auf die technische Kompetenz des BSI zurück, zum Beispiel bei der Bewertung neuartiger Authentifizierungsverfahren oder in Bezug auf die eIDAS-Verordnung. ■

HILFE BEI CYBER-ANGRIFFEN

Unterstützung von KRITIS-Unternehmen durch Fachexperten

von Julian Backhaus, Referat Penetrationstests und IS-Revisionen

Unternehmen sind einer fortlaufenden Bedrohung durch Cyber-Angriffe in den verschiedensten Formen ausgesetzt. Proaktive Schutzmaßnahmen, aber auch schnelle Reaktion bei Angriffen sind wichtig, um Unternehmen vor größeren Schäden zu bewahren. Das BSI unterstützt die Unternehmen aus dem Bereich Kritische Infrastrukturen, indem es qualifizierte Dienstleister mit hohem Spezialwissen auf dem Gebiet der Analyse und Abwehr von gezielten Cyber-Angriffen benennt.

Angriffe auf Unternehmen nehmen weiterhin zu, sowohl in der Anzahl als auch in der Intensität der Bedrohungen. Sogenannte Advanced Persistent Threats (APTs), die gezielt und mit hohem Aufwand durchgeführt werden, oder Distributed Denial-of-Service-Attacken (DDoS), die die Verfügbarkeit von Systemen und Diensten angreifen, sind dafür Beispiele. Der Schaden, der dabei entsteht, verursacht bei den betroffenen Unternehmen große wirtschaftliche Einbußen. Des Weiteren ist auch ein Reputationsverlust zu befürchten, wenn Dienste nicht zur Verfügung stehen oder ein Datenabfluss zu verzeichnen ist. Um die Abwehr zu verbessern oder um einen erfolgreichen Angriff zu bewältigen, brauchen Unternehmen oftmals die Unterstützung externer Dienstleister, die in ihrem jeweiligen Tätigkeitsgebiet ein hohes Spezialwissen erlangt haben.

Um die Betreiber Kritischer Infrastrukturen (KRITIS-Unternehmen) bei der Auswahl geeigneter Dienstleister zu unterstützen, wurden Auswahlkriterien für qualifizierte APT-Response- und DDoS-Mitigation-Dienstleister durch das BSI erarbeitet und veröffentlicht. Diese Kriterien bieten einen Überblick über Anforderungen und notwendige Kompetenzen an geeignete Dienstleister und sollten von den KRITIS-Unternehmen bereits im Rahmen der Notfallvorsorge berücksichtigt werden.

Akut betroffene KRITIS-Unternehmen benötigen allerdings häufig schnelle Unterstützung und haben keine ausreichende Zeit für eine umfangreiche Marktsichtung und Bewertung auf Basis dieser Kriterien. Das BSI hat daher zur Identifikation von qualifizierten Dienstleistern ein wettbewerbsneutrales Verfahren entwickelt, mit dem geeignete IT-Dienstleister in verschiedenen Bereichen identifiziert werden können. Angegriffene Unternehmen können dann rasch auf Basis der vom BSI vorgenommenen Bewertung Hilfestellung bei der Bewältigung von Angriffs- und Sicherheitsvorfällen anfragen.

DAS VERFAHREN

Zu Beginn jedes Verfahrens in einem Themenbereich wird initial eine Marktsichtung vom BSI durchgeführt, um potenziell geeignete Dienstleister zu identifizieren. Diese bezieht sowohl allgemein zugängliche Informationen wie Suchmaschinenergebnisse als auch Expertenmeinungen u. a. der jeweiligen Fachreferate und Fachkollegen des BSI mit ein. Anschließend werden die auf diese Weise identifizierten Dienstleister angeschrieben und zu dem Verfahren eingeladen. Weiteren Dienstleistern steht die Teilnahme an dem Verfahren bei Interesse jederzeit offen.

Das Bewertungsverfahren ist zweistufig und besteht aus einer Selbstauskunft und einem Interviewtermin. Ziel ist dabei, zu prüfen, ob die Firmen die veröffentlichten Mindestanforderungen erfüllen.

Mit der Selbstauskunft soll der Dienstleister Informationen zu seiner Qualifizierung liefern. Dazu gehören neben Unternehmensdaten (z. B. Firmenname und Anschrift), Ansprechpartnern und Kontaktdaten für KRITIS-Unternehmen auch Erläuterungen der angebotenen Produkte und Leistungen sowie eine Bestätigung, dass die vom BSI aufgestellten Kriterien eingehalten werden.

Nachdem die eingereichten Unterlagen auf Basis der veröffentlichten Kriterien für qualifizierte Dienstleister im jeweiligen Themengebiet erfolgreich geprüft und bewertet wurden, lädt das BSI die Dienstleiter zu einem ca. zweistündigen Interview ein. Hier müssen sie die technische sowie fachliche Kompetenz ihrer Beschäftigten sowie ihre Projekterfahrung anhand eines fiktiven Szenarios unter Aufsicht von Fachexperten unter Beweis stellen und erläutern, wie sie mit einem möglichen Vorfall umgehen würden.

Schließt der Dienstleister das Interview mit Erfolg ab, wird er im BSI als qualifizierter Dienstleister für sein Themengebiet geführt. Die Liste wird auf Nachfrage an betroffene KRITIS-Unternehmen ausgehändigt.

AKTUELLER STAND

Das beschriebene Verfahren wurde in den vergangenen Monaten bereits für DDoS-Mitigation-Dienstleister durchgeführt. Im ersten Schritt konnten sechs Anbieter identifiziert und durch das Verfahren bestätigt werden. Weiteren Dienstleistern steht die Qualifizierung in diesem Bereich auch in Zukunft offen.

Derzeit wird das Qualifizierungsverfahren im Bereich APT-Response-Dienstleister durchgeführt. Hierbei sollen bis zum Ende des Jahres erste Unternehmen im Rahmen des Verfahrens geprüft werden. ■

Weitere Informationen:

Übersicht zum Thema qualifzierte Dienstleister: https://www.bsi.bund.de/qualifizierte-dienstleister

Auswahlkriterien für qualifizierte DDoS-Mitigation-Dienstleister: https://www.bsi.bund.de/Dienstleister-DDoS-Mitigation

Auswahlkriterien für qualifizierte APT-Response-Dienstleister: https://www.bsi.bund.de/APT-Response_Dienstleister

Back-up: Datensicherung

BSI-Basistipp

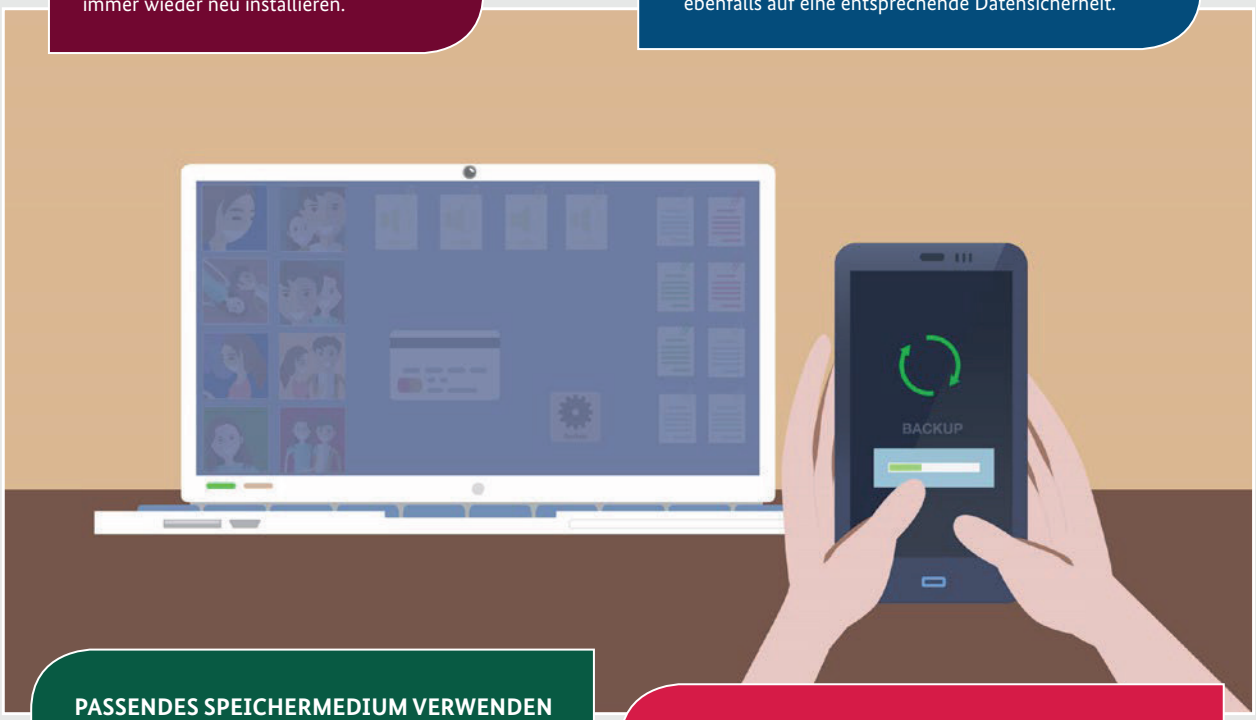
Mehr als die Hälfte aller Anwender (53 %) hat bereits elektronisch gespeicherte Daten verloren. Egal, ob durch Schadsoftware, technischen Defekt oder den Diebstahl des Geräts – verlorene Daten lassen sich in der Regel nur über ein vorhandenes Back-up retten. Eine gut durchdachte Datensicherung hilft dabei, wichtige Informationen nachhaltig zu sichern. Und so funktioniert es:

AUSGEWÄHLTE DATEN KOPIEREN

Entscheiden Sie, ob Sie das gesamte System oder nur ausgewählte Dateien wie Dokumente, Fotos und Videos sichern möchten. Betriebssysteme und Software lassen sich immer wieder neu installieren.

GEEIGNETE SOFTWARE FINDEN

Für die Erstellung von Datensicherungen bieten Gerätehersteller eigene Programme an, es existieren jedoch auch zahlreiche Lösungen von Drittanbietern. Prüfen Sie bei der Auswahl einer passenden Software die Kompatibilität mit Ihrem System und Ihren Daten. Achten Sie ebenfalls auf eine entsprechende Datensicherheit.



PASSENDES SPEICHERMEDIUM VERWENDEN

Neben externen, physikalischen Speichermedien wie Festplatten bietet sich heute auch die Auslagerung der Daten in eine sichere Cloud an. Am besten fahren Sie zweigleisig.

REGELMÄSSIGE BACK-UPS ANFERTIGEN

Um neu hinzugekommene Daten kontinuierlich zu sichern, empfiehlt sich ein regelmäßiger Turnus für die Aktualisierung der Datensicherung. Einmal eingestellt, läuft das oft ohne viel Aufwand automatisch im Hintergrund ab. Außerdem sollten Sie regelmäßig überprüfen, ob das angelegte Back-up tatsächlich alle Daten enthält.

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

ZU GUTER LETZT

V. l. BSI-Präsident Arne Schönbohm, Andreas Könen (BMI), Wolfgang Ebner (A-SIT), Peter Fischer (ISB), Gerard Caye (ANSSI Luxemburg), Guillaume Poupard (ANSSI Frankreich)

16. Deutscher IT-Sicherheitskongress

21. bis 23. Mai 2019

Stadthalle Bonn-Bad Godesberg

Mit über 600 Fachbesuchern (im Jahre 2017) ist der Deutsche IT-Sicherheitskongress, den das Bundesamt für Sicherheit in der Informationstechnik (BSI) alle zwei Jahre ausrichtet, 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.

Bild oben:
BSI-Präsident Arne Schönbohm überreicht die Siegerurkunde an den Gewinner des Best Student Awards 2017 Nils Rogmann

Bild links:
BSI-Präsident auf dem 15. Deutschen IT-Sicherheits-kongress 2017 in Bonn

Was wir wollen: Deine digitale Seite

Fotos © iStock.com/Grafissimo; © iStock.com/Krasyuk

Bundesamt
für Sicherheit in der
Informationstechnik

Informationstechnik ist die Grundlage des modernen Lebens. Umso wichtiger ist es, dass die Menschen der digitalen Welt vertrauen können. Darum kümmern wir uns. Als nationale Behörde für Cyber-Sicherheit gestalten wir IT-Sicherheit in Deutschland – aber auch in Europa und der Welt. Dazu arbeiten wir mit Wirtschaft und Wissenschaft zusammen. Wir beraten Politik und Verwaltung und stehen im Dialog mit den Bürgern sowie zahlreichen Verbänden. Im internationalen Austausch sind unsere Experten geschätzt und gefragt. Alles für ein gemeinsames Ziel: Informationssicherheit. Wir sorgen dafür, dass die Zukunft aus dem Netz erwachsen kann. Mit rund 720 Mitarbeitern sind wir ein vergleichsweise kleines Team für eine große Aufgabe. Und deshalb brauchen wir Verstärkung.

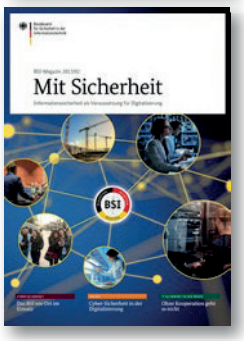
Weitere Informationen: https://www.bsi.bund.de/karriere und bewerbung@bsi.bund.de oder unter Tel.: 0228 99 9582 0

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.

Ich möchte die folgende BSI-Publikation im Abo erhalten:

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

Name, Vorname

Organisation

Straße

PLZ, Ort

E-Mail

Datenschutzrechtliche Einwilligung:
Ich stimme zu, dass meine oben angegebenen personenbezogenen Daten durch das BSI als verantwortliche Stelle für den Versand bzw. die Übermittlung der oben genannten Publikationen genutzt, elektronisch gespeichert und verarbeitet werden. Eine Weitergabe an Dritte findet nicht ohne Zustimmung statt.

Datum/Unterschrift:

Verantwortliche Stelle für die Verarbeitung Ihrer oben genannten personenbezogener Daten ist das Bundesamt für Sicherheit in der Informationstechnik, Postfach 200363, 53133 Bonn. Die von Ihnen angegebenen Daten werden ausschließlich für die Verwaltung des Versands bzw. der Übermittlung der Informationen verwendet, zu denen Sie oben zugestimmt haben. Sie können diese Einwilligung jederzeit widerrufen. Hierzu genügt eine E-Mail an bsi-magazin@bsi.bund.de. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Weitere Informationen darüber, wie wir Ihre personenbezogenen Daten bei uns verarbeiten und welche Rechte Ihnen diesbezüglich zustehen, können Sie den beigefügten „Datenschutzrechtlichen Hinweisen“ zur Bestellung von BSI-Publikationen entnehmen. 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/BSI-Magazin

Wenn Sie die BSI Publikationen nicht mehr erhalten möchten, schicken Sie uns einfach eine E-Mail an **bsi-magazin@bsi.bund.de**.

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

Datenschutzrechtliche Hinweise zur Bestellung von BSI-Publikationen

Für das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein verantwortungsbewusster Umgang mit personenbezogenen Daten hohe Priorität. Wir möchten, dass Sie wissen, wann wir welche Daten erheben und wie wir sie verwenden. Wir haben technische und organisatorische Maßnahmen getroffen, die sicherstellen, dass die Vorschriften über den Datenschutz sowohl von uns als auch von unseren externen Dienstleister beachtet werden. Im Zuge der Weiterentwicklung und Implementierung neuer Technologien können Änderungen dieser Datenschutzerklärung erforderlich werden. Daher empfehlen wir Ihnen, sich diese Datenschutzerklärung ab und zu erneut durchzulesen. Eine aktuelle Version kann jederzeit beim BSI angefordert werden oder findet sich in der nächsten Ausgabe des BSI-Magazins.

1. VERANTWORTLICHE STELLE

Verantwortliche Stelle für die Verarbeitung der personenbezogenen Daten im Sinne der Datenschutzgrundverordnung sowie anderer nationaler datenschutzrechtlicher Bestimmungen ist das Bundesamt für Sicherheit in der Informationstechnik (BSI), Godesberger Allee 185–189, 53175 Bonn, bsi@bsi.bund.de, Telefon: +49 (0)228 99 9582-0, Telefax: +49 (0)228 9910 9582-0, www.bsi.bund.de.

2. BEHÖRDLICHE DATENSCHUTZBEAUFTRAGTE IM BSI

Behördliche Datenschutzbeauftragte im BSI ist Frau Elke Gräf, Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185–189, 53175 Bonn, Telefon: 0228 99 9582-5775, +49 228 99 9582-5775, E-Mail: datenschutzbeauftragte@bsi.bund.de.

3. ALLGEMEINE HINWEISE ZUR DATENVERARBEITUNG

a) Zwecke der Verarbeitung und Rechtsgrundlage der Verarbeitung

Personenbezogene Daten werden – unter der Voraussetzung, dass hierin eingewilligt wurde – durch das BSI oder durch einen vom BSI beauftragten Dienstleister zum Zwecke des Versands von BSI-Publikationen genutzt, elektronisch gespeichert und verarbeitet. Sämtliche Verarbeitungstätigkeiten von personenbezogenen Daten erfolgen aufgrund von Einwilligungserklärungen der jeweiligen Betroffenen im Sinne von Art. 6 Abs. 1 lit. a Datenschutzgrundverordnung (DSGVO).

b) Empfänger bzw. Kategorien von Empfängern von personenbezogenen Daten

Personenbezogene Daten werden zudem an folgende Dritte weitergegeben: Versanddienstleister. Personenbezogene Daten werden an Dritte (Behörden, Unternehmen, Privatpersonen) nur übermittelt, soweit das BSI gesetzlich oder durch Gerichtsentscheidung dazu verpflichtet ist oder dies im Falle von Angriffen auf die Internetinfrastruktur zur Rechts- oder Strafverfolgung erforderlich ist. Eine darüber hinausgehende Weitergabe an Dritte findet nicht ohne Zustimmung des Betroffenen statt.

c) Dauer der Speicherung bzw. Kriterien für Festlegung der Dauer

Ihre personenbezogene Daten, die zum Versand von BSI-Publikationen genutzt werden, werden nur so lange zu diesem Zweck verarbeitet, wie eine Abbestellung der Publikation bzw. ein Widerruf Ihrer Einwilligung hierzu nicht erfolgt ist.

Ihre sonstigen Anfragen beim BSI werden in Papier oder elektronischer Form gemäß den für die Aufbewahrung von Schriftgut geltenden Fristen der Registraturrichtlinie aufbewahrt. Die Verwendung Ihrer Daten erfolgt ausschließlich für die unmittelbare Korrespondenz mit Ihnen.

d) Betroffenenrechte

Werden durch das BSI personenbezogene Daten von Ihnen verarbeitet, stehen Ihnen als Betroffener die folgenden Rechte gegenüber dem BSI zu:

i. Auskunftsrecht

Sie haben das Recht, vom BSI eine Bestätigung darüber zu verlangen, ob personenbezogene Daten, die Sie betreffen, vom BSI verarbeitet werden. Liegt eine solche Verarbeitung vor, können Sie vom BSI über folgende Informationen Auskunft verlangen:

- die Zwecke, zu denen die personenbezogenen Daten verarbeitet werden;
- die Kategorien von personenbezogenen Daten, welche verarbeitet werden;

- Empfänger bzw. die Kategorien von Empfängern, gegenüber denen die Sie betreffenden personenbezogenen Daten offengelegt wurden oder noch offengelegt werden;
- die geplante Dauer der Speicherung der Sie betreffenden personenbezogenen Daten oder, falls konkrete Angaben hierzu nicht möglich sind, Kriterien für die Festlegung der Speicherdauer;
- das Bestehen eines Rechts auf Berichtigung oder Löschung der Sie betreffenden personenbezogenen Daten, eines Rechts auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- alle verfügbaren Informationen über die Herkunft der Daten, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden;
- ob die Sie betreffenden personenbezogenen Daten in ein Drittland oder an eine internationale Organisation übermittelt werden. In diesem Zusammenhang können Sie verlangen, über die geeigneten Garantien gem. Art. 46 DSGVO im Zusammenhang mit der Übermittlung unterrichtet zu werden;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Art. 22 Abs. 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

ii. Recht auf Berichtigung

Sie haben ein Recht auf Berichtigung und/oder Vervollständigung gegenüber dem BSI, sofern die verarbeiteten personenbezogenen Daten, die Sie betreffen, unrichtig oder unvollständig sind. Das BSI wird die Berichtigung unverzüglich vorzunehmen.

iii. Recht auf Einschränkung der Verarbeitung

Unter den folgenden Voraussetzungen können Sie die Einschränkung der Verarbeitung der Sie betreffenden personenbezogenen Daten verlangen:

- wenn Sie die Richtigkeit der Sie betreffenden personenbezogenen für eine Dauer bestreiten, die es dem BSI ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen;
- die Verarbeitung unrechtmäßig ist und Sie die Löschung der personenbezogenen Daten ablehnen und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangen;
- das BSI die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, Sie diese jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen, oder
- wenn Sie Widerspruch gegen die Verarbeitung gemäß Art. 21 Abs. 1 DSGVO eingelegt haben und noch nicht feststeht, ob die berechtigten Gründe des BSI gegenüber Ihren Gründen überwiegen.

Wurde die Verarbeitung der Sie betreffenden personenbezogenen Daten eingeschränkt, dürfen diese Daten – von ihrer Speicherung abgesehen – nur mit Ihrer Einwilligung oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden. Wurde die Einschränkung der Verarbeitung nach den o. g. Voraussetzungen eingeschränkt, werden Sie durch das BSI unterrichtet, bevor die Einschränkung aufgehoben wird.

iv. Recht auf Löschung

Sie haben das Recht, vom BSI die unverzügliche Löschung der Sie betreffenden personenbezogenen Daten zu verlangen, und das BSI ist verpflichtet, diese Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

- Die Sie betreffenden personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Sie widerrufen Ihre Einwilligung, auf die sich die Verarbeitung gem. Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- Sie legen gem. Art. 21 Abs. 1 DSGVO Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder Sie legen gem. Art. 21 Abs. 2 DSGVO Widerspruch gegen die Verarbeitung ein.
- Die Sie betreffenden personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der Sie betreffenden personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem das BSI unterliegt.
- Die Sie betreffenden personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Art. 8 Abs. 1 DSGVO erhoben.

Sofern das BSI die Sie betreffenden personenbezogenen Daten öffentlich gemacht hat und es gemäß Art. 17 Abs. 1 DSGVO zu deren Löschung verpflichtet ist, so trifft das BSI unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass Sie als betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt haben.

Sie haben kein Recht auf Löschung der Sie betreffenden personenbezogenen Daten, soweit die Verarbeitung erforderlich ist

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information;
- zur Erfüllung einer rechtlichen Verpflichtung, die die Verarbeitung nach dem Recht der Union oder der Mitgliedstaaten, dem das BSI unterliegt, erfordert, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem BSI übertragen wurde;
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Art. 9 Abs. 2 lit. h und i sowie Art. 9 Abs. 3 DSGVO;
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gem. Art. 89 Abs. 1 DSGVO, soweit das unter Abschnitt a) genannte Recht voraussichtlich die Verwirklichung der Ziele dieser Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt, oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

v. Recht auf Datenübertragbarkeit

Sie haben das Recht, die Sie betreffenden personenbezogenen Daten, die Sie dem BSI bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Zudem haben Sie das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch das BSI, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern

- die Verarbeitung auf einer Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO oder Art. 9 Abs. 2 lit. a DSGVO oder auf einem Vertrag gem. Art. 6 Abs. 1 lit. b DSGVO beruht und
- die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

In Ausübung dieses Rechts haben Sie ferner das Recht, zu erwirken, dass die Sie betreffenden personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist. Freiheiten und Rechte anderer Personen dürfen hierdurch nicht beeinträchtigt werden. Das Recht auf Datenübertragbarkeit gilt nicht für eine Verarbeitung personenbezogener Daten, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem BSI übertragen wurde.

e) Recht auf Widerruf der datenschutzrechtlichen Einwilligungserklärung

Sie haben das Recht, Ihre datenschutzrechtlichen Einwilligungserklärungen jederzeit zu widerrufen. Bitte senden Sie hierfür eine E-Mail an bsi-magazin@bsi.bund.de. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

f) Beschwerderecht bei Aufsichtsbehörde

Unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs steht Ihnen das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat Ihres Aufenthaltsorts, Ihres Arbeitsplatzes oder des Ortes des mutmaßlichen Verstoßes, zu, wenn Sie der Ansicht sind, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt. Aufsichtsbehörde des Bundesamtes für die Sicherheit in der Informationstechnik ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, unterrichtet den Beschwerdeführer über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs nach Art. 78 DSGVO.

g) Erforderlichkeit der Datenerhebung

Die Bestellung von BSI-Publikationen sowie alle in diesem Zusammenhang getätigten Angaben sind grundsätzlich freiwillig. Wir weisen Sie jedoch darauf hin, dass bei nicht vollständigen Angaben bezüglich Ihres Namens sowie Ihrer Kontaktdaten ein solcher Versand nicht möglich ist.

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:	September 2018
Texte und Redaktion:	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:	Appel und Klinger Druck & Medien GmbH Bahnhofstraße 3 96277 Schneckenlohe Internet: www.ak-druck-medien.de
Artikelnummer:	BSI-Mag 18/708-1
Bildnachweise:	Titel: Dreamstime, Sashazamarasha; S. 2: Stephan Kohzer/BSI; S. 4: Bilder oben: HPI/K. Herschelmann; Bild unten: Internet Security Alliance; S. 5: Bild oben: BSI; Bild unten: trendence; S. 6: NCSC-NL; S. 9: NCSC-NL; S. 10: GettyImages©Flavio Coelho; S. 12-13: NürnbergMesse; S. 14-15: GettyImages©suedhang; S. 16: R. Winkler; S. 20-21: R. Winkler; S. 23: GettyImages©matejmo; S. 28-29: Henning Schacht ; S. 31: BSI; S. 32: BSI; S. 33: BSI; S. 35: Bild oben: Hessisches Ministerium des Innern und für Sport; Bild unten: ©HMdIS; S.36: GettyImages©Talaj; S. 40-41: R. Winkler; S. 43: links: ©Christian Müller/Fotolia; rechts: ©Monikey Business/Fotolia; S. 44-45: GettyImages©DivVector; S.46: GettyImages©TommL; S. 48: BSI; S. 51: R. Winkler; S. 53: BaFin; S. 54: GettyImages©Westend61; S. 56: junge Meister GmbH; S. 57: Foto Klein

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