Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

BSI-Magazin 2020/01

Mit Sicherheit

Im Gespräch:
Post-Quanten-Kryptografie

BSI INTERNATIONAL

EU-Ratspräsidentschaft:
Cyber-Sicherheit gestalten

DAS BSI

Kooperation:
Kommando CIR und BSI

IT-SICHERHEIT IN DER PRAXIS

Energiewirtschaft: Rollout
intelligenter Messsysteme

EDITORIAL

Cyber-Sicherheit in Krisenzeiten

Bereits jetzt im Frühjahr 2020 steht fest, welches Ereignis dieses Jahr am meisten prägen wird: das Corona-Virus. Es stellt unser aller Leben auf den Kopf und zwingt uns, viele Alltäglichkeiten neu zu denken: Statt zur Arbeit zu fahren, arbeiten wir im Home-Office. Schule heißt auf einmal Home-Schooling. Familienbesuche finden auf dem Smartphone statt. Und in den sozialen Medien sind wir Dauergast auf der Suche nach den neuesten Informationen zur Virus-Pandemie.

Cyber-Kriminelle wissen solche Gelegenheiten als Geschenk anzunehmen. Als ob uns das Virus nicht schon genug abverlangen würde, müssen sich daher viele jetzt mit alten und neuen Fragen der Cyber-Sicherheit beschäftigen: Wie schütze ich Firmengeheimnisse und vertrauliche Daten im Home-Office? Wie gestalte ich eine sichere Videokonferenz? Wie unterscheide ich vertrauenswürdige Nachrichten von Falschmeldungen? Will meine Bank wirklich mit mir chatten oder sind hier Hacker mit neuen gefälschten E-Mails am Werk?

Auch in einer solchen Krisensituation kommt das BSI seinem gesetzlichen Auftrag nach und begleitet Sie dabei, Ihre Informationstechnik sicher zu gestalten. Deutschland · Digital · Sicher · BSI – unter diesem Motto geben wir unseren Zielgruppen in Staat, Wirtschaft und Gesellschaft Empfehlungen an die Hand, wie sie in der jetzigen Krise sicher kommunizieren und dabei handlungsfähig bleiben.

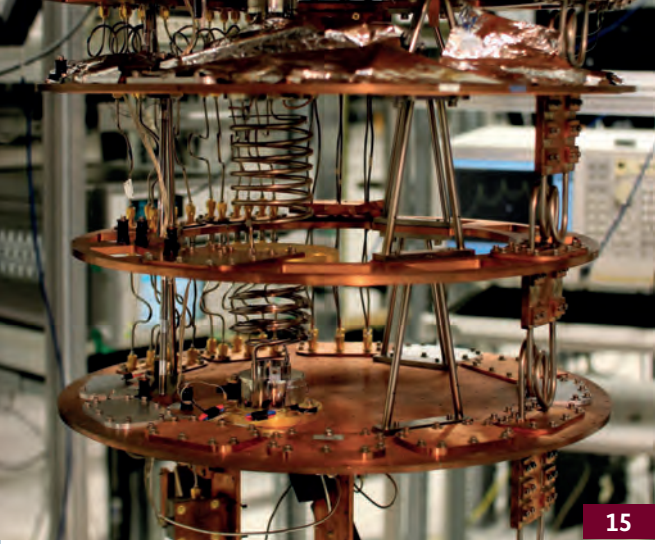
Gleichzeitig verlieren wir andere Themen nicht aus den Augen. Die vorliegende Ausgabe des BSI-Magazins widmet sich in einem Schwerpunkt der Post-Quanten-Kryptografie. Seit Google die „Quanten-Überlegenheit“ ausgerufen hat, wurde die Diskussion um die Bedeutung der Quantentechnologie aus spezialisierten Tech-Magazinen in das Bewusstsein einer breiteren, interessierten wie besorgten, Öffentlichkeit transportiert. Und tatsächlich gibt es allen Grund, sich umfassend und kritisch mit dem Thema zu befassen, das langfristig unser aller Leben entscheidend verändern könnte. Wie fast alle Entwicklungen der Digitalisierung hat auch die Quantentechnologie eine helle und eine dunkle Seite. Auch wenn kriminelle Anwendungen wie das Entschlüsseln digitaler Verschlüsselungsalgorithmen, die heute die sichere Kommunikation im Internet garantieren, noch nicht Realität sind: Seit Googles Experiment tickt die Uhr. Für das BSI ist die Post-Quanten-Kryptografie daher eines der wichtigen Zukunftsthemen, mit denen wir uns schon jetzt intensiv beschäftigen.

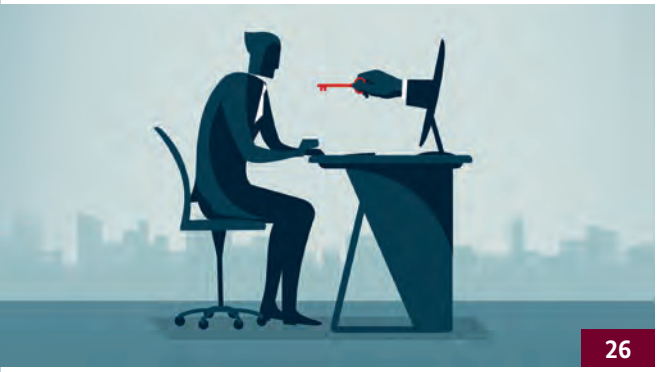
Über den Schwerpunkt Quantencomputer hinaus präsentieren wir Ihnen in dieser Ausgabe erneut ein breites Spektrum an BSI-Themen. Besonders freuen wir uns, dass sich mit dem Kommando Cyber- und Informationsraum der Bundeswehr, der Verbraucherschutzzentrale NRW und der Europäischen Agentur für Cyber-Sicherheit wichtige nationale und internationale Partner des BSI vorstellen.

Vielleicht lesen Sie diese Ausgabe als PDF im Home-Office. Vielleicht freuen Sie sich über die Print-Ausgabe, wenn Sie nach längerer Zeit wieder regelmäßig ins Büro kommen. Auf welchem Weg auch immer Sie uns finden - ich wünsche Ihnen eine interessante Lektüre.

Ihr

Arne Schönbohm,
Präsident des Bundesamts für Sicherheit in der Informationstechnik





INHALT

AKTUELLES

BSI-NEUBAU

Bonner Stadtrat beschließt Bebauungsplan

Der Stadtrat der Bundesstadt Bonn hat den Bebauungsplan für das Gebiet an der Ludwig-Erhard-Allee, in dem die neue Dienstliegenschaft des BSI errichtet werden soll, als Satzung beschlossen. Damit ist ein wichtiger städtebaurechtlicher Meilenstein erreicht, auf dessen Grundlage das Vorhaben weiter vorangebracht werden kann. In unmittelbarer Nähe der Bonner Rheinauen soll die neue Dienstliegenschaft den Charakter des BSI als fortschrittliche Cyber-Sicherheitsbehörde des Bundes widerspiegeln, dabei die Geschäftsprozesse der Behörde optimal unterstützen und sich städtebaulich in das bestehende Umfeld einfügen. Als zentraler Immobiliendienstleister des Bundes übernimmt die Bundesanstalt für Immobilienaufgaben (BImA) die Rolle der Bauherrin und die Durchführung des Verfahrens.

KONFERENZ

Erstes „Cyber Security Directors' Meeting" vor Münchner Sicherheitskonferenz

Auf Initiative und Einladung des BSI haben sich im Vorfeld der Münchner Sicherheitskonferenz (MSC) erstmals zahlreiche Leiterinnen und Leiter der Cyber-Sicherheitsbehörden Europas zu einem informellen Austausch getroffen. In Zusammenarbeit mit der MSC bot das BSI den vertretenen Behörden einen exklusiven Rahmen, um sich auf Leitungsebene über die aktuellen nationalen und europäischen Herausforderungen der Cyber-Sicherheit auszutauschen.

Damit baute das BSI seine Position als Thought Leader der Informationssicherheit aus und leistete einen wichtigen Beitrag zur besseren Vernetzung der Behörden, die jeweils in ihrem Land für das Thema federführend zuständig sind. Im europäischen Umfeld gilt das BSI bereits seit vielen Jahren als kompetenter und strategischer Partner in Fragen der Informationssicherheit.

CYBER-SICHERHEIT²

Video-Serie mit Experten für Smartphone-Sicherheit

Bei der Nutzung mobiler Endgeräte stellen sich Bürgerinnen und Bürger oftmals Fragen: Wie sicher sind Fingerabdruck- und Gesichts-Scan? Wie mache ich eine Datensicherung? Wofür brauche ich Updates? Antworten darauf gibt die neue Video-Serie des BSI, bei der sich jeweils zwei Experten mit einem digitalen Sicherheitsthema befassen.

Die ersten acht Folgen sind eine Kooperation zwischen dem BSI und der Verbraucherzentrale NRW und widmen sich vielfältiger Fragen rund um das Smartphone. Eine weitere Staffel Cyber-Sicherheit² folgt im Frühjahr und befasst sich mit Online-Zahlungen und dem Onlinebanking. Die Kompetenz des BSI wird dabei ergänzt durch einen Experten des LKA NRW.

SENSIBILISIERUNG

Gemeinsame Informations-kampagne von BMI und BSI zur IT-Sicherheit

Das Bundesministerium des Innern, für Bau und Heimat (BMI) und das BSI werden in diesem Jahr eine gemeinsame bundesweite Informations- und Sensibilisierungskampagne starten. Sie geht zurück auf den Doxing-Vorfall Ende 2018/Anfang 2019, bei dem persönliche Daten zahlreicher Personen des öffentlichen Lebens massenhaft im Internet veröffentlicht wurden.

Laut einer repräsentativen Online-Umfrage des BSI mit 20.000 Teilnehmern wünschen sich mehr als 70% der Befragten mehr Informationen über Risiken im Netz und eine größere Unterstützung im Bereich der digitalen Sicherheit. Dabei nehmen sie den unbefugten Zugriff Dritter auf sensible Daten und persönliche Informationen als größte Bedrohung im Internet wahr.

BSI INTERNATIONAL

Cyber-Sicherheit in Europa gestalten

Die deutsche EU-Ratspräsidentschaft im zweiten Halbjahr 2020

von Joshua Breuer, Referat Internationale Beziehungen

In den vergangenen Jahren hat die Europäische Union zunehmend an Bedeutung im Bereich der Cyber-Sicherheit gewonnen. Im zweiten Halbjahr 2020 wird Deutschland nach 2007 erneut den Vorsitz im Rat der Europäischen Union übernehmen. Damit gehen auch für das BSI große Chancen für die Gestaltung der europäischen Cyber-Sicherheit einher.

Im Rat der Europäischen Union (kurz Ministerrat oder Rat) sind die Regierungen der Mitgliedstaaten, repräsentiert durch ihre Minister, vertreten. Der Rat tritt in unterschiedlichen Formationen zusammen und fungiert im Institutionengefüge der EU gemeinsam mit dem Europäischen Parlament als Gesetzgeber. Wichtige inhaltliche Vorarbeiten für die Aktivitäten des Rats werden in über 300 Ratsarbeitsgruppen geleistet. Im Bereich der Cyber-Sicherheit ist dies vor allem die Horizontal Working Party on Cyber Issues, in welcher Deutschland federführend durch das Bundesministerium des Innern, für Bau und Heimat (BMI) sowie das Auswärtige Amt vertreten wird.

Der jeweiligen Ratspräsidentschaft kommt u.a. die Aufgabe zu, die Arbeit des Rats zu leiten, was sich konkret in der Übernahme des Vorsitzes der verschiedenen Ratsgremien ausdrückt. Nach Inkrafttreten des Vertrags von Lissabon wurde 2009 die rechtliche Grundlage für die sogenannte „Trio-Präsidentschaft“ geschaffen, die das Ziel verfolgt, eine gewisse Kontinuität der Arbeit des Rats zu gewährleisten. Jeweils drei Mitgliedstaaten stimmen demnach ihre Präsidentschaften miteinander ab und entwickeln ein gemeinsames Achtzehnmonatsprogramm. Deutschland gibt den Auftakt für die gemeinsame Trio-Präsidentschaft mit Portugal und Slowenien. Bereits 2007 hatten die drei Staaten als Trio in dieser Konstellation agiert und damit den Auftakt eines institutionellen Novums in der EU gegeben.

Neben dem Vorsitz in den „offiziellen“ Ratsgremien knüpfen sich an die Ratspräsidentschaft weitere Aufgaben. So ist etwa im Bereich der Cyber-Sicherheit der Vorsitz in der NIS-Kooperationsgruppe durch die Ratspräsidentschaft zu besetzen. Die Gruppe wurde durch die Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie) geschaffen. Für Deutschland wird diese Aufgabe traditionell durch das BMI in Zusammenarbeit mit dem BSI wahrgenommen. Gerade hier sowie in den daran angebundenen „Work Streams“, die sich mit Einzelthemen der Richtlinien-Umsetzung sowie neu aufkommenden Themen (z.B. zum Thema 5G) beschäftigen, bietet sich durch die bereits vorhandene breite Teilnahme von BSI-Expertinnen und -Experten die Möglichkeit, deutsche Ansätze gezielt zu bewerben und europäische Cyber-Sicherheit voranzubringen und zu gestalten.

CYBER-SICHERHEIT IM RAHMEN DER RATSPRÄSIDENTSCHAFT UND DIE ROLLE DES BSI

Die Vorbereitungen auf die deutsche Ratspräsidentschaft laufen im BSI seit Beginn des Jahres 2019 in enger Abstimmung mit dem BMI. Thematisch wird es zum einen darum gehen, bestehende Initiativen im Bereich der Cyber-Sicherheit auf europäischer Ebene voranzubringen. So ist beispielsweise eine Evaluation der NIS-Richtlinie vorgesehen. Zum anderen bietet die Präsidentschaft dem BSI die Möglichkeit, sich als führende Cyber-Sicherheitsbehörde

in der EU zu positionieren und selbst wichtige Themen anzustoßen. In diesem Sinne wird Deutschland eigene Initiativen einbringen und zudem vom 9. bis 10. November 2020 eine große Cyber-Sicherheitskonferenz in Berlin veranstalten. Als die Cyber-Sicherheitsbehörde des Bundes trägt das BSI seine Fachexpertise bei der Gestaltung des Programms bei und ist eng in die Planungen eingebunden.

Ein dritter Pfeiler der Ratspräsidentschaft ist der Austausch und die Abstimmung mit der neuen Europäischen Kommission, die in den kommenden Monaten den bisherigen Ankündigungen Taten folgen lassen will. So sieht beispielsweise der „Mission letter" von Kommissionspräsidentin Ursula von der Leyen an Thierry Breton, Kommissar für den Binnenmarkt, die Einrichtung einer „Joint Cyber Unit" vor. Aber auch das Thema „Künstliche Intelligenz" sowie konkret die Implementierung der gerade verabschiedeten 5G-Toolbox werden voraussichtlich in die deutsche Ratspräsidentschaft fallen.

Im Vergleich zu Deutschlands vorheriger Ratspräsidentschaft im Jahr 2007 muss festgehalten werden, dass man sich im Bereich der Cyber-Sicherheit europäisch in einem gänzlich gewandelten Umfeld befindet. Mit der NIS-Richtlinie ist 2016 ein erstes, zentrales Legislativvorhaben verabschiedet worden und auch der 2019 in Kraft getretene Cybersecurity Act bietet gänzlich neue Möglichkeiten für europaweite Regelungen in der IT-Sicherheitszertifizierung, vor allem auch bei der Regulierung des „Internet of Things". Konkret werden mit dem neuen Rahmenwerk für eine EU-weite IT-Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen viele neue „europäische Zertifikate" entstehen. Deutschland und vor allem das BSI haben mit einer europaweit bedeutsamen Stellung in der Zertifizierung dabei Vorbildcharakter und diese Expertise soll während der Ratspräsidentschaft genutzt werden, um das neue Rahmenwerk mit Leben zu füllen. ■

Weitere Informationen:

https://www.consilium.europa.eu/de/council-eu/presidency-council-eu/

Das neue Mandat mit Leben füllen

Ein Interview mit dem neuen ENISA Exekutivdirektor Juhan Lepassaar

Am 16. Oktober 2019 hat Juhan Lepassaar seine neue Rolle als Exekutivdirektor der Europäischen Agentur für Cyber-Sicherheit (ENISA) übernommen. Er übernimmt das Amt von Udo Helmbrecht, ehemals Präsident des BSI, der sein ENISA-Mandat nach 10 Jahren vollendet hat. Der Übergang fällt in einen besonders interessanten Zeitraum. Nur einige Monate zuvor, am 27. Juni 2019, ist der Rechtsakt für Cyber-Sicherheit (engl. „Cybersecurity Act“) in Kraft getreten. Diese EU-Verordnung leitet eine neue Ära für ENISA ein, da sie der Agentur nicht nur ein permanentes Mandat, sondern auch neue Aufgaben zuschreibt, wie zum Beispiel neue Zuständigkeiten im Europäischen Zertifizierungsrahmen für Cyber-Sicherheit. Dieses neue Mandat mit Leben zu füllen, ist nun ein wichtiger Teil in Juhan Lepassaars neuer Verantwortung.

Herr Lepassaar, in Ihrer vorherigen Position als Leiter des Kabinetts des damaligen Vizepräsidenten der Europäischen Kommission, Andrus Ansip, haben Sie bereits im Bereich der Digitalpolitik gearbeitet. Was sind die daraus gewonnenen Erkenntnisse, die Sie in Ihre neue Rolle mitgenommen haben?

Die digitale Welt ist verwoben und vernetzt. Das erhöht die Komplexität und kann von vornherein abschreckend wirken, insbesondere dann, wenn man beginnt, sich mit ihr auseinanderzusetzen, oder gar Vorschläge macht, sie zu regulieren. Es ist wichtig, die richtigen Impulse und Anreize zu finden. Das ist eine zentrale Lektion aus meiner vorhergehenden Arbeit. Sie können dabei helfen, Vertrauenswürdigkeit sowie eine verantwortungsvolle Regulierung bzw. Selbstregulierung des digitalen Ökosystems zu fördern.

ENISAs neues Mandat kommt auch mit neuen Ressourcen einher, personal- und budgettechnisch. Wie soll ENISA nach dem Ende Ihres Mandats aussehen?

Ich will, dass die Agentur sich mit unterschiedlichst talentierten Menschen auseinandersetzt, die verschiedene Bereiche und Kompetenzen umfassen. In einer Ära, in der sich alles im Wandel befindet, ist das wahrscheinlich die beste zukunftsfähige Absicherung. Aber ich möchte auch Wege erkunden, wie dieser Pool von Talenten mit anderen Cyber-Sicherheitsakteuren in Europa geteilt werden kann, um den vorhandenen Mangel an qualifiziertem Personal nicht noch zu vergrößern.

Wie sehen Sie ENISAs Rolle im größeren Kontext der neuen Prioritäten der Europäischen Kommission unter Leitung von Ursula von der Leyen?

Unsere Rolle ist es, politischen Entscheidungsträgern dabei zu helfen, die vor uns liegenden Herausforderungen in einer sich schnell entwickelnden digitalen Welt verständlich zu machen. Ebenso unterstützen wir verschiedene Communities bei der Umsetzung von Cyber-Sicherheitspolicies, sobald es zu einer Einigung gekommen ist. Eine wichtige Herausforderung für die Zukunft wird es sein, Politik auf eine innovative und flexible Art so zu entwickeln, dass sichergestellt werden kann, dass Vorgehensweisen zu Cyber-Sicherheit ein hohes Sicherheitsniveau erreichen und gleichzeitig wirtschaftlich rentabel bleiben. Die Agentur ist in der einzigartigen Position, die politischen Aspekte von zukünftigen Herausforderungen im Cyber-Bereich zu adressieren. Dabei freuen wir uns darauf, eng mit der neuen Kommission zusammenzuarbeiten. Wie immer ist es unser Ziel, proaktive Cyber-Sicherheitsnetzwerke zu bilden, die diverse Interessenträger zusammenbringen, um Fragen von gemeinsamen Interesse zu lösen.

Wo sehen Sie in den verschiedenen Handlungsbereichen der ENISA den größten Mehrwert gegenüber den Mitgliedstaaten?

Die Agentur dient als Referenzpunkt für die Mitgliedstaaten und bietet eine Plattform für paneuropäische Kollaboration. In diesem Kontext ist es wichtig, dass die Agentur ein gutes Verständnis über die spezifischen Bedürfnisse jedes Mit-

gliedstaates erhält sowie darüber, wie diesen Bedürfnissen begegnet werden kann, während zugleich EU-weite Ziele verfolgt werden. Wir streben die Entwicklung einer engeren Kooperation auf allen Ebenen innerhalb der EU an, in der wir gemeinsam mit den Mitgliedstaaten daran arbeiten, alle Interessenträger bei der Verbesserung von Cyber-Sicherheit in allen Bereichen des Lebens einzubeziehen. Über die Jahre hat ENISA Netzwerke in diesen Gemeinschaften entwickelt. Wir werden diese Netzwerke weiter im Dienst der EU und der Mitgliedstaaten nutzen.

Was sind neben bereits bestehenden EU-weiten Ansätzen andere Bereiche im Themenfeld „Digitales", wo Sie Bedarf für europäische Lösungen sehen?

Es gibt viele Bereiche, in denen europäische Ansätze für das Themenfeld „Digitales" Nutzen bringen können. In einigen Fällen wurde bereits viel Arbeit investiert, die erhebliche Vorteile hervorgebracht hat. Gute Beispiele dafür sind der Ansatz bezüglich eines Benachrichtigungssystems bei Sicherheitslücken in der EU sowie die eingeführte Rechtssetzung im Bereich elektronischer Identitäten (eIDAS). Beispiele für Bereiche, die noch Herausforderungen darstellen, sind unter anderem autonome Systeme, Künstliche Intelligenz und 5G. Die zunehmende technische Ausgereiftheit von neuen Technologien verbessert die Art und Weise, wie Gesellschaften agieren, erschafft aber auch neue Bedrohungen und Risiken. Erweiterte Cyber-Angriffe, die Verbreitung von glaubwürdigen Fake News und Angriffe auf autonome Fahrzeuge sind nur einige dieser potentiellen Sicherheitsbedrohungen. Aufgrund der vernetzten Eigenschaften moderner Technologien müssen wir EU-Koordinierung nutzen, um sicherzustellen, dass Vertraulichkeit, Integrität und Verfügbarkeit von Daten sowie die Sicherheit der Technologien unseren gesellschaftlichen Bedürfnissen entsprechen. Die europäische Digitalpolitik wird essentiell sein, um einen Datenfluss zu regulieren, den Grenzen nicht stoppen. Politische Rahmenbedingungen müssen alle Parameter integrieren, um die Werte der Europäischen Union zu bewahren, ohne Innovation zu unterdrücken.

Die deutsche EU-Ratspräsidentschaft beginnt am 1. Juli 2020. Was sind Ihre Erwartungen und Hoffnungen hierfür?

Wir erwarten, dass die Expertise und Erfahrung, die sich in Deutschland entwickelt hat, zum Wohle aller Interessenträger auf nationaler und europäischer Ebene genutzt wird.

Spannend ist, dass Deutschland sein erstes Cybersicherheitsgesetz im Jahr 2015 vor der NIS-Richtlinie verabschiedet hat.[1] Deutschland investiert viel in Forschung zum Schutz von IT-Infrastruktur und IT-Systemen und hat bereits Kompetenzzentren für IT-Sicherheit eingerichtet. Diese konzentrieren die Fähigkeiten und Kompetenzen der besten Universitäten und nicht-universitäre Forschung und fördern interdisziplinäre Kooperation in Bereichen wie „Security by Design", optisch-elektronische Technologien und Quantenkommunikation. Wir freuen uns darauf, im Rahmen der deutschen EU-Ratspräsidentschaft in einen engen Dialog zu treten, und begrüßen die deutschen Beiträge zu den Anstrengungen der EU, unser digitales Europa zu schützen. ■

Kurzprofil Juhan Lepassaar

Juhan Lepassaar war Leiter des Kabinetts des damaligen Vizepräsidenten der Europäischen Kommission, Andrus Ansip, dem das Portfolio „Digitaler Binnenmarkt" zugeschrieben war. Zuvor war er Kabinettsmitglied des damaligen Kommissionsvizepräsidenten und EU-Kommissars für Transport, Siim Kallas, und arbeitete als Direktor für EU-Angelegenheiten im Regierungsbüro Estlands.

"Die Agentur bietet eine Plattform für paneuropäische Kollaboration."

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

[1] https://www.bsi.bund.de/it-sig

CYBER-SICHERHEIT

Alice und Bob im Quantenland

BSI legt erste Empfehlungen zu Quantencomputer-resistentem Schlüsseltransport vor

von Dr. Heike Hagemeier, Referat Vorgaben an und Entwicklung von Kryptoverfahren

Die Sicherheit digitaler Infrastrukturen beruht wesentlich auf Verfahren zur Schlüsselvereinbarung und für digitale Signaturen. Mit heutigen Mitteln sind diese Verfahren nicht zu brechen. Dies gilt nicht mehr, wenn universelle Quantencomputer ausreichender Leistungsfähigkeit verfügbar sind (siehe Artikel auf Seite 15).

Zurzeit werden in einem Prozess des US-amerikanischen National Institute of Standards and Technology (NIST) kryptografische Verfahren standardisiert, die resistent gegen Angriffe mit Quantencomputern sein sollen (Post-Quanten-Kryptografie, siehe dazu auch den Artikel aus BSI Magazin 2018/2). Dieser Prozess wird frühestens 2022/23 abgeschlossen sein.

Das BSI begrüßt die Aktivitäten des NIST zur Standardisierung von Post-Quanten-Kryptografie. Diese haben dazu geführt, dass die Forschung an Quantencomputer-resistenten Verfahren deutlich intensiviert wurde. Dennoch sind diese Verfahren noch nicht so gut erforscht wie die zurzeit eingesetzten Verfahren. Dies gilt insbesondere im Hinblick auf Schwächen, die sich erst in der Anwendung zeigen, wie beispielsweise typische Implementierungsfehler. Das BSI empfiehlt daher, Post-Quanten-Kryptografie möglichst nur „hybrid“ einzusetzen, d.h. in Kombination mit klassischen Algorithmen.

Zudem spielen in dem Standardisierungsprozess des NIST neben Sicherheit auch weitere Aspekte wie Performance eine wichtige Rolle. Etliche Forschungsaktivitäten und Experimente zur Integration der Verfahren in kryptografische Protokolle (wie Transport Layer Security - TLS) konzentrieren sich hauptsächlich auf die Effizienz.

Aus Sicht des BSI steht die Sicherheit der Verfahren an erster Stelle. Als Verfahren zum Schlüsseltransport sind die Verfahren FrodoKEM (siehe Artikel auf Seite 12) und Classic McEliece die konservativste Wahl. Mit Blick auf die Dauer des NIST-Prozesses hat sich das BSI daher entschieden, nicht auf die Entscheidung von NIST zu warten und in der neuen Version der Technischen Richtlinie „BSI TR-02102-1: „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ die beiden genannten Verfahren als grundsätzlich geeignet (in hybriden Lösungen) zu empfehlen. Diese Empfehlung wird gegebenenfalls angepasst, wenn die Entwicklung im NIST-Prozess weiter fortgeschritten ist. ■

Frodo ist die „neue Hoffnung“

Gitterbasierte kryptografische Verfahren

von Dr. Heike Hagemeier, Referat Vorgaben an und Entwicklung von Kryptoverfahren

Was meint eine Mathematikerin, wenn sie über ein Gitter spricht? Was hat das mit Kryptografie zu tun? Und wie kommt „Der Herr der Ringe“ ins Spiel? Ein Ausflug in die Welt der gitterbasierten Kryptografie.

WAS IST EIN GITTER?

In der Mathematik bezeichnet ein Gitter eine diskrete Untergruppe eines n-dimensionalen reellen Vektorraums. Grob gesagt bedeutet diese Definition, dass man zwei Gitterpunkte addieren kann und wieder einen Punkt im Gitter erhält, und dass es in einer "kleinen" Umgebung um einen Gitterpunkt keinen weiteren Gitterpunkt gibt. Im zweidimensionalen Beispiel wird klar, warum dies als Gitter bezeichnet wird (siehe Abb. 1).

In einem Gitter lassen sich viele Probleme formulieren, die schwer zu lösen sind, zum Beispiel einen kürzesten Vektor in einem Gitter zu finden. Im Gitter in Abbildung 1 ist diese Aufgabe durch bloßes Hinschauen zu lösen (roter Pfeil). Der Rechenaufwand wächst aber exponentiell mit der Dimension des Gitters.

Als Grundlage für gitterbasierte Kryptografie verwendet man Probleme, die nachweislich mindestens genauso schwer zu lösen sind wie ein Gitterproblem - beispielsweise das "Learning-with-Errors"-Problem (LWE-Problem). Dieses lässt sich grob zusammenfassen als die Schwierigkeit, ein lineares Gleichungssystem, das mit einem „kleinen“ Fehler gestört wurde, zu lösen.

Ein einfaches Beispiel für ein solches System ist

$a_{11} \cdot s_1 + a_{12} \cdot s_2 + e_1 = b_1,$
$a_{21} \cdot s_1 + a_{22} \cdot s_2 + e_2 = b_2,$

wobei alle a_i und b_i bekannte ganze Zahlen sind und alle s_i und e_i unbekannte. Es lässt sich kurz schreiben als

$As + e = b.$

Dabei werden die Werte a_i in der Matrix A (eine Art Tabelle; hier mit zwei Zeilen und zwei Spalten) und die Werte s_i, e_i und b_i in den Vektoren s, e und b zusammengefasst. Das LWE-Problem besteht also darin, die unbekannten Vektoren s und e zu finden, wenn die Matrix A und der Vektor b gegeben sind. Auch hier muss die Dimension (Anzahl der Gleichungen und Anzahl der Unbekannten) ausreichend groß sein. Eine entsprechende Matrix ist leicht mehrere Kilobytes groß.

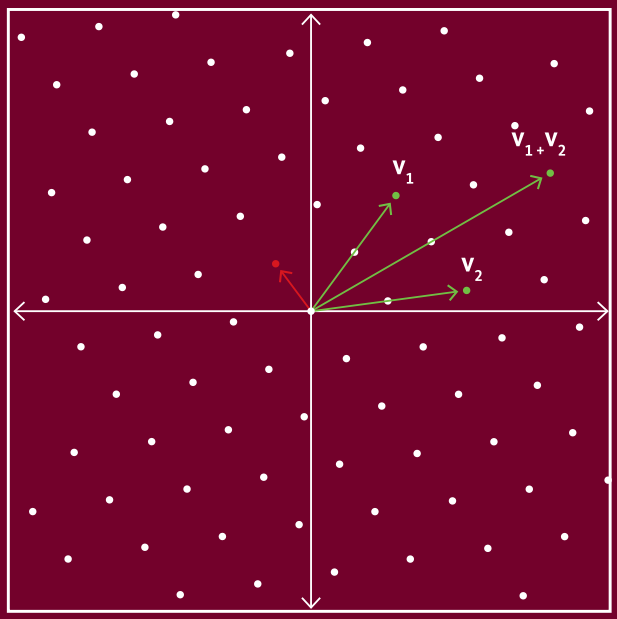


Abbildung 1

WAS HAT DAS MIT KRYPTOGRAFIE ZU TUN?

Es wird angenommen, dass die oben beschriebenen Probleme auch mit einem Quantencomputer nicht effizient zu lösen wären. Sie bieten damit einen Ansatz für Post-Quanten-Kryptografie. Die Sicherheit gitterbasierter Verfahren stützt sich auf die Schwierigkeit dieser Probleme, daher gelten diese Verfahren als Quantencomputer-resistent.

Die ersten praktikablen gitterbasierten Verfahren zur Schlüsseleinigung versuchten den bekannten Diffie-Hellman-Schlüsselaustausch in eine Post-Quanten-Welt zu retten. Abbildung 2 skizziert diesen Ansatz grob.

Ein wesentlicher Unterschied zum klassischen Diffie-Hellman-Verfahren ist, dass Alice und Bob zunächst nur ungefähr das gleiche Ergebnis erhalten. Es ist noch ein Mechanismus („Reconciliation“) nötig, um ein gemeinsames Geheimnis zu errechnen. Dafür müssen neben den öffentlichen Schüsseln b und b‘ auch noch weitere Informationen geschickt werden.

WIE IST DER STAND DER TECHNIK?

Dieser Ansatz wird inzwischen nicht mehr verfolgt, die heutigen Verfahren sind als Schlüsseltransportverfahren formuliert. Dies ist teilweise dadurch bedingt, dass im Standardisierungsprozess des National Institute of Standards and Technology (NIST) explizit Verfahren zum Schlüsseltransport gesucht waren. Andererseits wird dadurch die Reconciliation erleichtert, es müssen keine zusätzlichen Informationen mehr übermittelt werden.

In vielen gitterbasierten Verfahren wird eine zyklische Matrix verwendet. Eine solche Matrix ist komplett durch die Elemente in der ersten Zeile festgelegt. Daher reicht es, nur diese erste Zeile zu speichern bzw. zu übertragen, alle anderen Zeilen lassen sich aus dieser berechnen. Zudem werden dadurch auch einige Berechnungen vereinfacht. Das entsprechende Problem wird Ring-LWE genannt. Ein Beispiel für ein auf Ring-LWE beruhendes Verfahren ist „New Hope“, das 2017 testweise in Googles Browser Chrome implementiert wurde.

Die Sicherheit gitterbasierter Verfahren beruht entweder auf Standard LWE-Problemen oder auf LWE-Problemen (z.B. Ring-LWE), bei denen die Matrix eine spezielle Struktur (wie oben beschrieben) hat. Die zusätzliche Struktur bietet den Vorteil, dass die Verfahren effizienter sind und kleinere Schlüssel benötigen. Sie führt aber auch dazu, dass noch nicht das gleiche Vertrauen in die Sicherheit der entsprechenden Verfahren besteht. Auch wenn zurzeit keine Angriffe bekannt sind, welche zusätzliche Struktur ausnutzen, sind Verfahren, deren Sicherheit auf Standard LWE-Problemen beruht, die konservativere Wahl.

UND WIE KOMMT „DER HERR DER RINGE“ INS SPIEL?

Ein Beispiel für ein solches Verfahren ist das Schlüsseltransportverfahren FrodoKEM. Dieses Verfahren wurde für den NIST-Standardisierungsprozess eingereicht und von NIST für die zweite Runde ausgewählt. Das BSI empfiehlt FrodoKEM als eines der ersten Quantencomputerresistenten Schlüsseltransportverfahren in der Technischen Richtlinie TR-02102-1 (siehe Artikel auf Seite 27).

Und wer sich nun fragt, warum dieses Verfahren nach einer Figur aus „Der Herr der Ringe“ benannt wurde, dem sei als Hinweis verraten, dass der Titel der ersten Veröffentlichung „Frodo: Take off the ring!“ lautete. ■

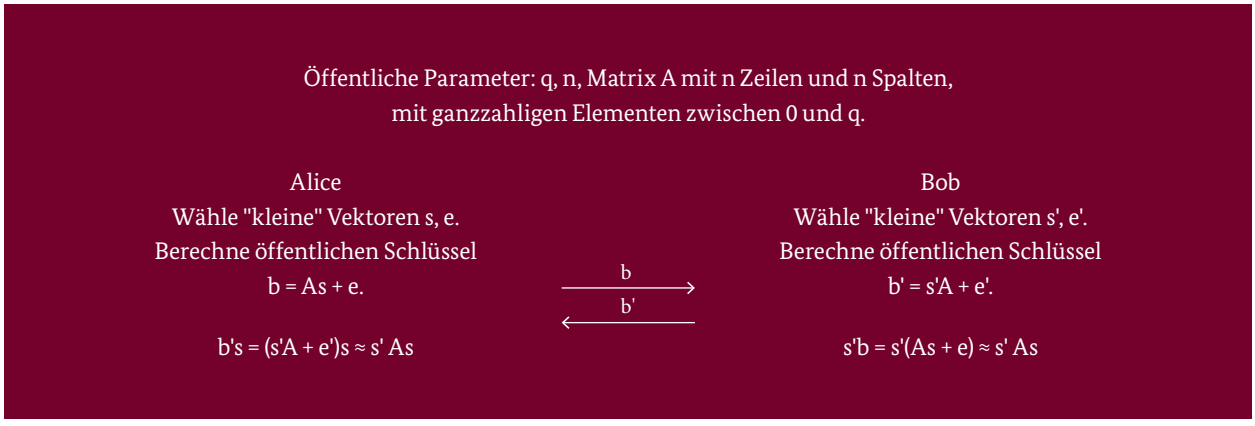


Abbildung 2

Quantencomputer und Quantenüberlegenheit

von Univ.-Prof. Dr. Frank Wilhelm-Mauch, Fachrichtung Physik, Universität des Saarlandes

Quantencomputer sind im Augenblick in aller Munde. Die Anzeichen eines Hypes sind gegeben, insbesondere seit eine Arbeitsgruppe bei Google ein Experiment veröffentlicht hat, das die Überlegenheit ihres Quantencomputers über die größten Supercomputer der Welt zeigt. Dieses anspruchsvolle Ergebnis ist schwer zu greifen und es kursiert Unsicherheit. Was verbirgt sich hinter den Schlagzeilen um Googles Quantenüberlegenheit und welche Auswirkungen hat das auf die Informationssicherheit?

Das Konzept eines Quantencomputers kann auf zweierlei Art gefasst werden – theoretisch und in konkreter Hardware.

Theoretisch besteht der Unterschied zwischen Quantencomputern und den heutigen klassischen Computern in der Art, wie klassische binäre Daten zwischen Ein- und Ausgabe verarbeitet werden. In der Quantenphysik können Systeme wie z. B. Elementarteilchen mehrere klassisch erlaubte Zustände in Überlagerung einnehmen. „In Überlagerung" bedeutet hier, dass mehrere Orte gleichzeitig möglich sind und beim Versuch der Ortsmessung verschiedene Orte mit bestimmten Wahrscheinlichkeiten erscheinen.

In einem Quantencomputer wird dieses Prinzip auf den Inhalt von binären Datenregistern übertragen: Ein Quantencomputer kann in einem Zustand sein, der im gleichen Sinn eine Überlagerung der klassischen Binärwerte darstellt. Die Auswirkung kann als massiv quantenparelleles Rechnen verstanden werden - der Quantencomputer arbeitet einen Algorithmus auf einer Überlagerung von beliebig vielen Registerwerten ab und benötigt dafür nur einen einzigen Prozessorkern. Parallelismus ist im Augenblick auch der größte Treiber von Beschleunigung bei klassischen Computern, dort wird aber für jeden parallelen Strang der Rechnung ein weiterer Prozessorkern benötigt.

Es wäre aber vorschnell, den Quantencomputer jetzt sofort zum ultimativen Parallelrechner zu küren - denn der Aspekt der Wahrscheinlichkeit muss beachtet werden: Die Benutzerin[1] möchte natürlich mit hoher Wahrscheinlichkeit das richtige Ergebnis auslesen. Die Überlagerung muss am Ende der Rechnung wieder zu einem oder wenigen Ergebnissen zusammengeführt werden („uncomputing"). Insofern (und aufgrund von Eigenschaften des Befehlssatzes) lassen sich klassische Anwendungen nicht ohne weiteres auf den Quantencomputer übertragen und einfach parallelisieren.

Kurzprofil: Prof. Dr. Frank Wilhelm-Mauch

Prof. Dr. Frank Wilhelm-Mauch studierte und promovierte in Physik an der Universität Karlsruhe, dem heutigen KIT. Nach Stationen an der TU Delft, der Ludwig-Maximilians-Universität und der University of Waterloo ist er seit 2011 Universitätsprofessor für Theoretische Physik an der Universität des Saarlandes.

Wilhelm-Mauch arbeitet seit 1999 an verschiedenen Fragestellungen zum Thema Quantencomputing rund um die Hardwareplattform der supraleitenden Schaltkreise. Er ist Mitglied der Strategic Research Agenda Working Group des EU-Quantentechnologie-Flaggschiffs für die Bereiche Quantencomputing und Strategische Ressourcen und koordiniert das Flaggschiff Projekt „An Open Superconducting Quantum Computer" (OpenSuperQ). Er ist auch federführender Autor der BSI-Studie „Entwicklungsstand Quantencomputing".

[1] weibliche Formen schließen den männlichen Fall mit ein

Praktisch ist die Hardware von Quantencomputern noch recht heterogen - durchaus vergleichbar mit der von Relais über Röhren bis zu modernen Chips reichenden Geschichte des klassischen Computers. Quantencomputer-Ingenieurinnen müssen einen weiten Spagat hinlegen: Einerseits ist die Quantenphysik die Physik kleinster, isoliert betrachteter Materieelemente - darum müssen die Bauelemente (Qubits) isoliert werden. Andererseits muss der Quantencomputer Schreib- und Leseoperationen durchführen können und flexibel benutz- und verbindbar sein - was mit isolierten Elementarteilchen eine Herausfoderung darstellt.

Unter den verschiedenen Kandidaten für Technologien werden zwei Plattformen im Augenblick als führend angesehen (andere Plattformen werden erfolgreich erforscht, sind aber im Augenblick weniger weit entwickelt):

- Im Hochvakuum gefangene atomare Ionen sind eine mit Atomuhren verwandte Technologie. Ein- und Ausgabe werden hier mit Lasern und Kameras bewerkstelligt.

- Auf der anderen Seite stehen Chips aus supraleitenden Metallen (Aluminium und Niob), die bei sehr tiefen Temperaturen betrieben werden.

Andere Plattformen werden erforscht, sind aber im Augenblick weniger weit entwickelt. Gemeinsam ist beiden Plattformen, dass es sich noch um experimentelle Technologie handelt, die den Weg vom Labor zur Anwendung findet. Dazu gehören extreme Bedingungen: Ultrahochvakuum bzw. Temperaturen nahe des absoluten Nullpunktes. Dies ist auf der Skala von Rechenzentren durchaus beherrschbar. Dort sollte man Quantencomputer auch schon aufgrund der möglichen Anwendungen verorten.

WO KÖNNEN QUANTENCOMPUTER ANGEWENDET WERDEN?

Wie oben beschrieben, besteht die Kunst bei der Entwicklung von Quantenalgorithmen darin, den Vorteil der massiven Quantenparallelität zu nutzen und dennoch am Ende ein nicht vom Zufall maskiertes Ergebnis zu haben. Die Beschleunigung entsteht daraus. Die Zahl der Schritte zum Ergebnis kann deutlich anders mit der Größe der Aufgabe wachsen als auf klassischen Rechnern.

Dies wurde für einige Aufgaben gezeigt. Dazu gehören das Durchsuchen von unstrukturierten Datenbanken und verschiedene Aufgaben im Maschinenlernen. Dazu gehört auch die Primfaktorzerlegung, die profunden Einfluss auf die Sicherheit kryptographischer Verfahren hat, ebenso wie die Simulation von Molekülen und Materialien für die chemische und andere Industrien. Letztere wird im Allgemeinen als die erste Anwendung angesehen, da sie weniger hohe Anforderungen an die Hardware stellt als die anderen.

WO STEHT DIE HARDWAREENTWICKLUNG?

In den Medien wird oft die Zahl der Qubits als Gradmesser der Entwicklung angegeben. Die zunächst bescheiden wirkenden Zahlen an Bits werden beeindruckender, wenn man sie damit vergleicht, was ein klassischer Computer benötigt, um einen Quantencomputer zu simulieren - bei N Qubits werden 2^N komplexe Fließkommazahlen benötigt.

Mindestens ebenso bedeutend ist die Fehlerrate von Quantenoperationen. Dies ist zunächst überraschend. In klassischen Computern spielen Hardwarefehler nur selten eine Rolle, da die verwendete Halbleiterlogik sich selbst stabilisiert. In Quantencomputern ist dies anders:

- Einerseits ermöglicht die reichhaltige Struktur von Quantenzuständen deutlich mehr Fehleroptionen als im klassischen Fall.

- Andererseits treten mit analogen Fehlern sowie mit der Tendenz von offenen Systemen, sich nach längerer Zeit klassisch zu verhalten, also ihre Quanteneigenschaften zu verlieren, Fehlermechanismen auf, die auf klassischen Digitalrechnern kein Analogon haben. Fehlerraten von 1:1000 sind heute der Start zu guten Qubits und 1:1000000 ist das Beste, was erreicht wurde. Doch selbst das bedeutet, dass bei einem MHz Taktfrequenz jede Sekunde ein Fehler auftritt.

Es bestehen zwei grundlegende Ansätze, mit dieser Problematik umzugehen: In der Noisy Intermediate-Scale Quantum-Technology (NISQ) wird erprobt, wie weit man mit fehlerbehafteten Rechnern gehen kann. Die durch die Fehlerrate limitierte Zahl der Rechenschritte ermöglicht nur kurze Algorithmen. Das Potenzial der Quantenbeschleunigung liegt bei Algorithmen, die klassisch eher am Speicher als an der Zeit scheitern, z.B. in der theoretischen Chemie.

Wenn man darüber hinaus gehen möchte, werden aktive Fehlerkorrektur und fehlertolerantes Rechnen benötigt. Hier werden logische Qubits - Qubits, die der Algorithmus benötigt - in einer größeren Zahl physikalischer Qubits (also realer Bauelemente) codiert und per Vergleichsmessung korrigiert. Solange die Qubits gut genug sind, lässt sich die effektive Fehlerrate weiter unterdrücken. Der so entstehende Overhead ist aber beträchtlich. Die Route zur Fehlertoleranz ist ausführlich in der BSI-Studie zum Thema (www.bsi.bund.de/qcstudie) beschrieben. Dort werden fünf Schichten an Zwischenschritten beschrieben, die es erlauben, den Fortschritt in dieser Richtung zu bewerten.

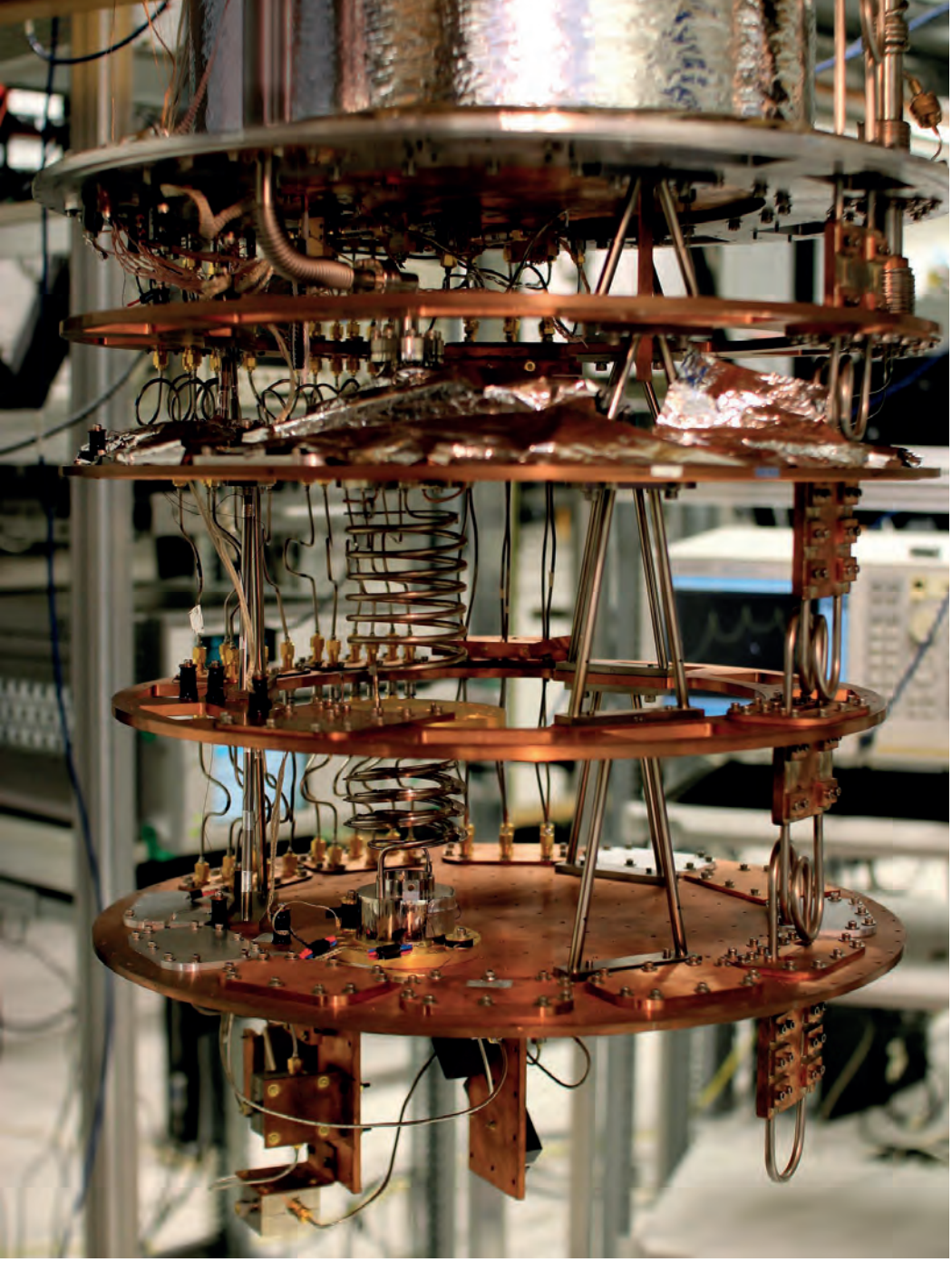


Abbildung links:
Typische Kältemaschine für den Betrieb von Qubits (Chip an der Unterseite). Die Kupferplatten dienen dem Temperaturausgleich.

QUANTENÜBERLEGENHEIT BEI GOOGLE

Im Oktober hat die Hardwaregruppe bei Google unter Leitung von John Martinis ein entscheidendes Ergebnis zur Quantenüberlegenheit veröffentlicht. Was wurde dort gezeigt? Hardwareplattform, ein Chip aus supraleitenden Qubits, die in einem Rechteck von 6 x 9 verschaltet sind. Von diesen 54 Qubits funktionierten 53. Der Prozessor wird als NISQ betrieben. Die Fehlerwahrscheinlichkeiten für die limitierenden 2-Qubit-Gatter liegen konsistent unter ein Prozent.

Als Benchmark für Quantenüberlegenheit hat das Google-Team eine Aufgabe gestellt, die es dem Quantencomputer leicht gemacht hat, seine Stärken auszuspielen. Es wird ein geeigneter Zufallsalgorithmus abgearbeitet, der das physikalische Phänomen des Quantenchaos nachbildet. Die Reproduktion dieses Ergebnisses auf einem klassischen Computer erfordert 2^{53} komplexe Zahlen im Speicher - was den größten aktuellen Supercomputer übertrifft.

Dies ist ohne Zweifel eine technologische Meisterleistung, die den weiteren Weg zu größeren und besseren Quantenprozessoren ermöglicht. Sie ist ebenso wenig „nützlich“ wie der erste Flug der Gebrüder Wright, kann aber ein ähnliches Schlüsselergebnis sein.

BEZUG ZUR KRYPTANALYSE

Kryptanalyse ist eine mögliche Anwendung von Quantencomputern. Die aktuelle RSA-Kryptografie beruht auf der Schwierigkeit und dem explodierenden Aufwand, große Ganzzahlen auf klassischen Computern in ihre Primfaktoren zu zerlegen. Quantencomputer haben diese Einschränkung nicht, sie können dies in einer Zeit erreichen, die nur langsam mit der Größe der Ganzzahl wächst. Sobald also Quantencomputer einmal RSA entschlüsselt haben, wird diese Verschlüsselung nicht mehr zu retten sein. Dies bezieht sich allerdings zunächst einmal nur auf die Public-Key-Kryptografie. Symmetrische Verfahren können bei ausreichender Schlüssellänge weiterhin quantensicher sein.

Die kompilierten Algorithmen sind aber lang und komplex - etwa 10^{12} Zeitschritte. Dies wird nach menschlichem Ermessen eine aktive Fehlerkorrektur erfordern. Der Durchbruch von Google war zwar ein wichtiger Schritt in diese Richtung, die tatsächliche Relevanz für Kryptanalyse ist aber noch weit entfernt. Dennoch ist es wichtig, für langfristige Informationssicherheit, jetzt in einen Prozess einzusteigen, kryptographische Infrastrukturen quantensicher zu machen. Panik ist aber unangebracht. ■

Auf neuen Wegen

29. Cyber-Sicherheits-Tag der Allianz für Cyber-Sicherheit

Von Till Kleinert, Referat Cyber-Sicherheit für die Wirtschaft und Allianz für Cyber-Sicherheit

Mit einem neuen Veranstaltungskonzept lockten die Allianz für Cyber-Sicherheit (ACS) und der Deutsche Industrie- und Handelskammertag (DIHK) am 26. September 2019 zahlreiche Interessierte zum 29. Cyber-Sicherheits-Tag nach Berlin. Denn im Bereich der Cyber-Sicherheit lässt sich zwar vieles individuell lösen. Einfacher und besser funktioniert es aber, wenn man von Erfahrungen und Erkenntnissen anderer lernen kann.

Ausstellung, interaktive Formate und Fachvorträge zu aktuellen Herausforderungen der Cyber-Sicherheit - der 29. Cyber-Sicherheits-Tag im Haus der Deutschen Wirtschaft in Berlin hatte den teilnehmenden Unternehmen, Cyber-Sicherheitsinitiativen, Verbänden und Behörden einiges zu bieten. Dabei verfolgte die Allianz für Cyber-Sicherheit ein neues Veranstaltungskonzept, das sich merkbar von den vorherigen Cyber-Sicherheitstagen unterschied. Im Mittelpunkt standen nicht nur Vorträge, sondern auch zahlreiche Gelegenheiten zur Zusammenarbeit bei verschiedenen Themen der Cyber-Sicherheit. Die Moderatoren nutzten nun Barcamps, um die Kreativität der Beteiligten zu lenken und handfeste Arbeitsergebnisse zu realisieren. In Workshops wurden kurzfristig Ideen für Projekte zum wenige Tage später stattfindenden European Cyber Security Month (ECSM) generiert. Bereits fertiggestellte Vorhaben zum Aktionsmonat – wie die IT-Notfallkarte, die das BSI unter dem Dach der ACS gemeinsam mit vielen Cyber-Sicherheitsinitiativen und Partnern realisiert hatte – wurden in einer Ausstellung im Foyer des Hauses der Deutschen Wirtschaft vorgestellt. Zeitgleich berichtete die Allianz für Cyber-Sicherheit über die Sozialen Medien live vom Geschehen und hielt die Veranstaltung erstmalig auch auf Video fest (https://www.allianz-fuer-cybersicherheit.de/ACS/CSTVideo). Ein Event dieser Größenordnung verlangte den Organisatoren nicht nur am Tag selbst, sondern auch im Vorfeld, viel ab. Bereits mehrere Monate zuvor hatten DIHK und ACS mit den Abstimmungen begonnen. Die Mühe sollte sich lohnen: Mit mehr als 300 Vertretern deutscher Organisationen erfuhr der 29. Cyber-Sicherheits-Tag einen

Cyber-Sicherheits-Tage

Unter der Schirmherrschaft des BSI, in Kooperation mit Multiplikatoren wie Verbänden, Kammern, Initiativen oder Netzwerken, organisiert die Allianz für Cyber-Sicherheit sechs Cyber-Sicherheits-Tage pro Jahr an wechselnden Standorten im gesamten Bundesgebiet. Die Veranstaltungen sind für einen Teilnehmerkreis von bis zu 200 Personen ausgelegt und befassen sich mit einem aktuellen Thema der Cyber-Sicherheit, welches in Fachvorträgen aus unterschiedlichen Blickwinkeln beleuchtet und in begleitenden Kurzworkshops oder Diskussionsrunden vertieft wird.

Die nächsten Veranstaltungen werden rechtzeitig auf der Webseite der Allianz für Cyber-Sicherheit angekündigt.

bis dato unerreichten Zuspruch. Auch die Rückmeldungen der Gäste spiegelten wider, dass das neue Konzept gut ankam. Das Team der Allianz für Cyber-Sicherheit wird daher auch bei den kommenden Cyber-Sicherheitstagen wieder verschiedene interaktive Elemente in die Veranstaltungsplanung einfließen lassen. ■

Hier erfahren Sie, warum Sie bei einem Cyber-Sicherheits-Tag dabei sein sollten:

https://www.allianz-fuer-cybersicherheit.de/cybersicherheitstag

Professionelle Begleiter

Zertifizierung zum IT-Grundschutz-Berater

von Johannes Oppelt, Referat BSI-Standards und IT-Grundschutz

Der BSI-Lagebericht 2019 hat es jüngst wieder eindrucksvoll belegt: Die Gefahr für Unternehmen und Behörden, Opfer eines Cyber-Angriffs zu werden, ist weiterhin hoch. Zugleich werden die Angriffe immer professioneller durchgeführt. Hinzu kommen die elementar wichtigen internen Herausforderungen: klar definierte Prozesse und Verantwortlichkeiten zu Fragen der Informationssicherheit sowie gut geschulte Mitarbeiter – am besten ein Managementsystem zur Informationssicherheit nach IT-Grundschutz. Hier setzt die Personenzertifizierung zum IT-Grundschutz-Berater an.

Viele Unternehmen und Behörden benötigen einen kompetenten Berater an ihrer Seite, um IT-Sicherheitsmaßnahmen und -Prozesse zu planen und umzusetzen. Besonders kleinere Institutionen können häufig mangels personeller oder finanzieller Ressourcen die damit verbundenen, umfangreichen Aufgaben nicht alleine bewältigen. Auch um ein umfassendes Managementsystem zur Informationssicherheit (ISMS) zu implementieren, im Anschluss zu etablieren und aufrecht zu erhalten, ist meist externe Expertise erforderlich.

INFORMATIONSSICHERHEIT NACH IT-GRUNDSCHUTZ

Das BSI bietet interessierten Anwendern daher die Personenzertifizierung zum IT-Grundschutz-Berater an. Das Zertifizierungsangebot basiert auf einem zweistufigen Schulungskonzept. Im ersten Schritt kann ein Nachweis als IT-Grundschutz-Praktiker abgelegt werden, bevor die Personenzertifizierung zum IT-Grundschutz-Berater möglich ist (siehe Abbildung 1).

Ziel der noch recht neuen Zertifizierungsmöglichkeit ist es, ein einheitliches und hohes Ausbildungsniveau im Bereich IT-Grundschutz zu erreichen. Die ausgebildeten IT-Grundschutz-Berater können mit ihrer nachgewiesenen Expertise Institutionen zu allen IT-Grundschutz-Themen beraten. So können sie Behörden und Unternehmen, zum Beispiel bei der Entwicklung von Sicherheitskonzepten oder der ISMS, unterstützen. Im operativen Tagesgeschäft können sie mit den zuständigen Mitarbeitern der Institution auf Basis des IT-Grundschutzes Maßnahmen definieren und im Betrieb umsetzen. Zertifizierte IT-Grundschutz-Berater können zudem dabei helfen, ein ISO 27001 Audit auf Basis von IT-Grundschutz vorzubereiten.

„Das BSI als Cyber-Sicherheitsbehörde des Bundes setzt mit dem Zertifizierungsangebot den Standard für ein einheitlich hohes Niveau in der Ausbildung der Experten“, erläutert BSI-Präsident Arne Schönbohm. „Diese können die Empfehlungen und Maßnahmen aus dem IT-Grundschutz fundiert und kompetent in der Praxis weitergeben. Jeder einzelne IT-Grundschutz-Berater kann damit künftig einen wichtigen Beitrag für die Widerstandsfähigkeit der deutschen Wirtschaft sowie der öffentlichen Verwaltung im Bereich der Informationssicherheit leisten.“

„Das BSI als Cyber-Sicherheitsbehörde des Bundes setzt mit dem Zertifizierungsangebot den Standard für ein einheitlich hohes Niveau in der Ausbildung der Experten“

IT-GRUNDSCHUTZ-EXPERTISE IST GEFRAGT

Inzwischen bieten über 20 Schulungsanbieter Schulungen nach den Vorgaben des BSI an. Im Jahr 2019 wurden bereits über 300 Personen zum IT-Grundschutz-Praktiker ausgebildet und über 50 Personen zum IT-Grundschutz-Berater zertifiziert. Die hohe Nachfrage nach der neuen Personenzertifizierung spiegelt den Bedarf nach kompetenter Unterstützung und Beratung bei der Einführung, dem Betrieb und der Weiterentwicklung von Informationssicherheit in Institutionen.

- Interessierte Anwender können zunächst die Basisschulung zum IT-Grundschutz-Praktiker absolvieren und mit einer Prüfung abschließen. Diese Ausbildung eignet sich für Interessierte im Bereich Informationssicherheit und vermittelt grundlegende Kenntnisse über den IT-Grundschutz.

- Nach einer Aufbauschulung erfolgt die Personenzertifizierung zum IT-Grundschutz-Berater. Dieser Weg empfiehlt sich für Anwender, die bereits über ausgeprägte Praxiserfahrung im Bereich IT-Grundschutz verfügen.

- Das BSI arbeitet mit Schulungsanbietern zusammen, die interessierten Anwendern die Basisschulung zum IT-Grundschutz-Praktiker und die Aufbauschulung IT-Grundschutz-Berater anbieten. Es stellt dafür ein Curriculum zur Verfügung. Auch die Prüfungen zum IT-Grundschutz-Berater werden vom BSI abgenommen.

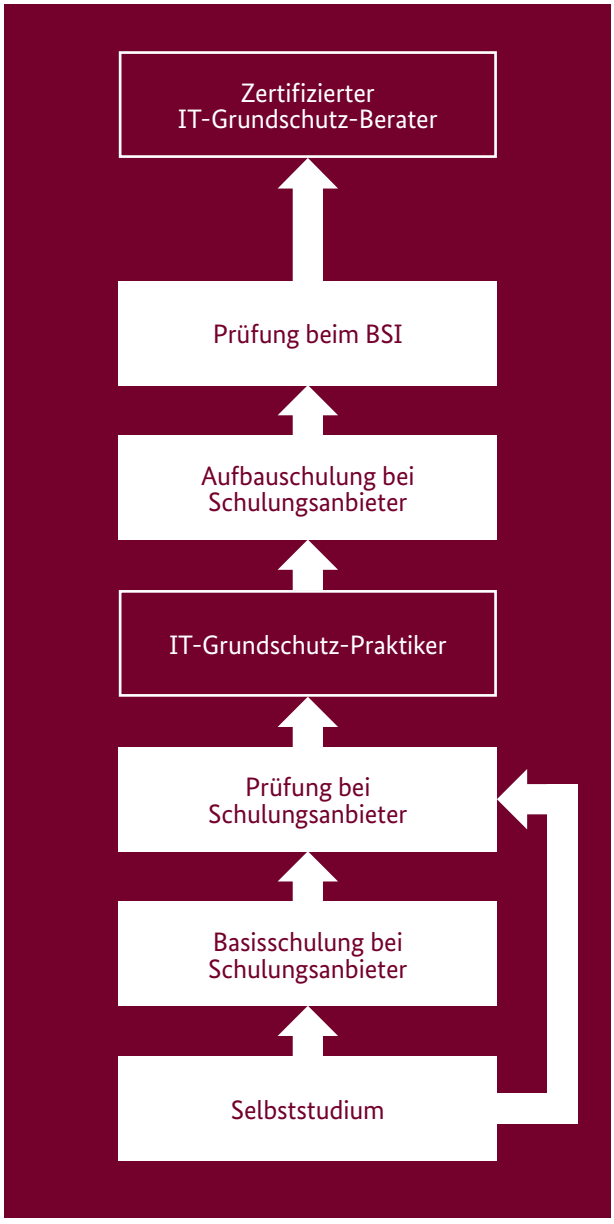


Abbildung 1

Weitere Informationen:

https://www.bsi.bund.de/gsberater

Qualifiziertes Zulassungsverfahren

IT-Sicherheitsprodukte für den Geheimschutz

von Frank Sonnenberg, Thomas Borsch, Referat Zulassung von VS-Produkten

Das BSI hat im Rahmen seines gesetzlichen Auftrags die Verpflichtung, die IT-Sicherheit zu stärken und aufrecht zu erhalten. Dazu gehört, Bund, Länder und geheimschutzbetreute Wirtschaft mit IT-Sicherheitslösungen zu versorgen, die für die Bearbeitung von Verschlusssachen (VS) zugelassen sind. Die zunehmende Digitalisierung, immer kürzer werdende Innovationszyklen und sich stets verändernde Bedrohungslagen stellen für die Sicherheit von VS-Systemen eine große Herausforderung dar. Daher müssen frühzeitig innovative Methoden entwickelt werden, um den Bedarf IT-sicherheitsrelevanter Technologien zu erkennen, entsprechende Anforderungen zu definieren, diese in umsetzbare Produktentwicklungen zu überführen und dem VS-Markt zeitnah als zugelassene VS-Lösung bereitzustellen.

Zulassungsverfahren sind aufgrund ihrer Komplexität grundsätzlich sehr aufwändig und zeitintensiv. Dies begründet sich insbesondere dadurch, dass sich die in ihnen definierte Evaluierungsmethodik eng an den Common Criteria und ihrem formalen Ansatz orientiert. D.h., IT-Sicherheitsprodukte mit kurzen Innovationszyklen scheinen daher auf den ersten Blick für derartige Prüfverfahren nicht geeignet. Insbesondere Softwareprodukte und mobile Kommunikationsgeräte sind in hohem Maße sich ständig verändernden Angriffsvektoren ausgesetzt. Darum müssen, um sie als VS-Produkte einsetzen zu können, möglichst kurzfristig wirksame Gegenmaßnahmen neu entwickelt und diese als zugelassene Produkte in die Anwendung überführt werden. Die dadurch erschwerten zeitlichen Rahmenbedingungen stellen die Zulassung von VS-Produkten vor eine große Herausforderung, da die fachlich geforderten kurzen Reaktionszeiträume zum etablierten Prüfprozess konträr sind. Deshalb gilt es, die Zulassungsverfahren bei möglichst gleichbleibender Wirksamkeit zukünftig effizienter zu gestalten. Um dieser Aufgabe gerecht zu werden, hat das BSI für VS-Lösungen für den Geheimhaltungsgrad „VS-NUR FÜR DEN DIENSTGEBRAUCH“, die einen großen Teil der Zulassungsverfahren ausmachen, einen neuen Prozess definiert, das „Qualifizierte Zulassungsverfahren“.

QUALIFIZIERTE HERSTELLER

Der grundsätzliche Ansatz des Qualifizierten Zulassungsverfahrens besteht darin, neben technischen Prüfkriterien erstmals auch die Sicherheit der Entwicklungsumgebung und die Prozesse der Produkthersteller systematisch mit zu betrachten. Die Eignungsfeststellung in diesem Bereich wird mit dem Prädikat „Qualifizierter Hersteller“ zum Ausdruck gebracht. Dies ist ein im Gegensatz zu reinen Produktprüfungen zeitgemäßer Ansatz, der die IT-Sicherheit ganzheitlich und über den gesamten Lebenszyklus der Produkte betrachtet. Mit dem Qualifizierten Zulassungsverfahren sollen VS-NfD-Produkte qualifizierter Hersteller effizient und dennoch effektiv einen wohldefinierten Prüfprozess durchlaufen. In diesem Zusammenhang wird unter „effizient“ und „effektiv“ die Realisierung zeitnaher Prüfergebnisse, bei optimiertem und ressourcensparendem Vorgehen bzw. die Wahrung der prinzipiellen Anforderungen an die Vertrauenswürdigkeit von IT-Sicherheitsprodukten verstanden. Das Standard-Zulassungsverfahren behält jedoch weiterhin Gültigkeit und kommt für Zulassungen

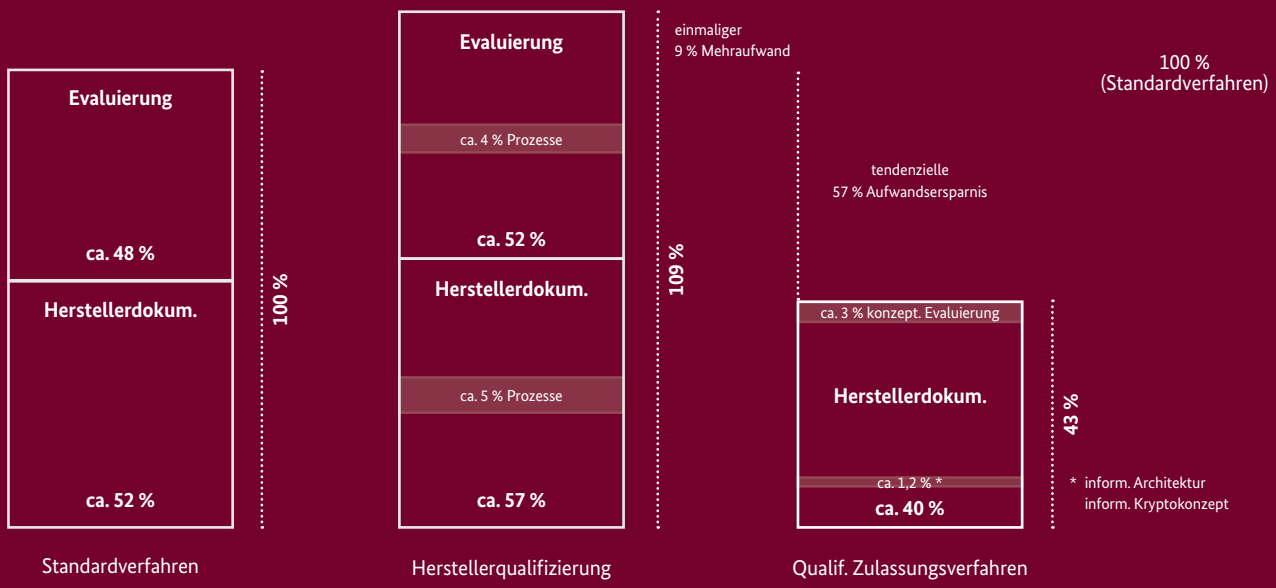


Abbildung 1: Aufwände Standardverfahren vs. Qualifiziertes Verfahren

auf dem Niveau oberhalb VS-NfD, sowie für Hersteller, die sich noch nicht qualifiziert haben, zur Anwendung. Um dieses Ziel zu erreichen, musste ein alternatives Vorgehen bei der Zulassung von IT-Sicherheitsprodukten definiert werden. Bis dahin beruhte die Vertrauenswürdigkeit einer Zulassungsaussage ausschließlich auf einer rein technikbasierten Evaluierung des untersuchten IT-Produktes. Um nun die zeit- und aufwandsintensiven individuellen Produktprüfungen zu reduzieren, mussten andersgeartete, aber fachlich gleichwertige Vertrauenswürdigkeitskriterien gefunden werden. Dieser Ausgleich wird realisiert, indem unternehmensweite prozessorientierte Sicherheitsanforderungen integriert und bewertet werden. Sie umfassen in Anlehnung an die Common Criteria sämtliche Vorgaben an den gesamten Lebenszyklus eines IT-Sicherheitsproduktes von der frühen Planungsphase (Requirement), über die Entwicklung, Markteinführung, Pflege und Support (Maintenance) bis hin zur geregelten Abkündigung und zur Aussonderung.

Somit stützt sich das Qualifizierte Zulassungsverfahren auf folgende Vertrauenswürdigkeitsaspekte: Vertrauenswürdige Entwicklungsprozesse und -umgebung: Ein für dieses Verfahren „Qualifizierter Hersteller“ erfüllt spezielle Anforderungen des BSI an die Entwicklung und Bewertung seiner IT-Sicherheitsprodukte. Die Anerkennung als „Qualifizierter Hersteller“ erfolgt durch das BSI auf Basis spezifischer wohldefinierter Kriterien. Konzeptionelle Produktprüfung: Die bisher verwendete klassische, rein technische Produktevaluierung reduziert sich nun im qualifizierten Verfahren auf eine konzeptionelle Produktprüfung. Dabei werden informell, aber systematisch die grundsätzliche Struktur und die Sicherheitseigenschaften des zu bewertenden IT-Sicherheitsprodukts festgestellt. Verbindliche Herstellererklärung: Der Hersteller versichert dem BSI in einer Herstellererklärung schriftlich, dass er ein Produkt gemäß der vom BSI überprüften Herstellerprozesse entwickelt und alle im Rahmen einer herkömmlichen Evaluierung erforderlichen Produktnachweise erzeugt hat sowie diese im Bedarfsfall dem BSI zur Prüfung übergeben könnte. Die nachstehende Grafik veranschaulicht den Gewinn, der sich mit der Anwendung des Qualifizierten Zulassungsverfahrens ergibt und sich tatsächlich durch die bereits durchlaufenden Verfahren bestätigt (siehe Abbildung 1).

PRÜFUNGSAUFWAND WIRD SIGNIFIKANT REDUZIERT

Der Aufwand im Qualifizierten Zulassungsverfahren wird nach einer vom Hersteller erfolgreich durchlaufenen Hersteller-Qualifizierung auf unter 50 Prozent reduziert. Dem steht nur ein einmaliger Mehraufwand von ca. 9 Prozent entgegen. Dieser zusätzliche Aufwand ist durch die zusätzlich zu erbringende initiale Prozessevaluierung des Unternehmens während seiner Herstellerqualifizierung bedingt. Wurde diese erfolgreich durchlaufen, können alle folgenden VS-NfD-Zulassungsverfahren, die sich dieser Entwicklungsprozesse bedienen, im Qualifizierten Zulassungsverfahren durchgeführt werden. Neben der Aufwandsreduzierung ist auch die Verfahrensdauer eines Qualifizierten Zulassungsverfahrens signifikant reduziert, da bei vorliegender Hersteller-Qualifizierung lediglich eine konzeptionelle Produktprüfung bestimmter Prüfaspekte erforderlich ist. Die im Standardverfahren angewandte detaillierte, tiefergehende und iterative Prüfung, die wesentlich zu einer Verlängerung des Verfahrens führt, ist im Qualifizierten Zulassungsverfahren nicht mehr erforderlich. Zusammenfassend betrachtet, führt das Qualifizierte Zulassungsverfahren damit zu einer effizienteren Bedarfsdeckung zugelassener Produkte. Für die beteiligten Unternehmen stehen unter dem Aspekt „Time to Market“ neben einem finanziellen Gewinn durch das Verfahren, die bessere Steuerbarkeit und zeitnahe Marktzuführung verbesserter und sicherer IT-Sicherheitsprodukte im Vordergrund. ■

Elektronische Identitäten auf dem Smartphone

Wie mobile Identitäten sicher verwendet werden können

von Rainer Schönen, Referat Cyber-Sicherheit im Gesundheits- und Finanzwesen

Um einzukaufen, nutzt man Webshops, Medien werden online gestreamt, soziale Interaktion findet über die Sozialen Medien statt und (Bank-)Geschäfte erledigt man unterwegs auf dem Tablet oder Mobiltelefon. Ein Großteil des heutigen Lebens findet digital statt. Daher arbeitet das BSI im Rahmen des Förderprojekts OPTIMOS 2.0 mit daran, dass elektronische Identitäten sicher auf dem Smartphone gespeichert werden können, damit selbst datensensible Dienste auf mobilen Endgeräten nutzbar sind.

Um eine Vielzahl von Online-Services nutzen zu können, benötigt man eine elektronische Identität (eID). Der Begriff eID ist dabei sehr generisch und kann für ganz verschiedene Online-Zugänge stehen, wie zum Beispiel:

- das Pseudonym, mit dem man in einem Online-Forum aktiv ist,
- einen Account in einem sozialen Netzwerk, den Inhaber eines digitalen KFZ-Schlüssels, der auf dem Smartphone gespeichert ist,
- als Käufer in einem Online-Shop aufzutreten oder
- Bankkunde beim Online-Banking zu sein.

Jede dieser eIDs muss gegen Missbrauch geschützt werden, der ja nach Art der elektronischen Identität unterschiedlich stark sein muss. Manchmal genügt zwar die Eingabe einfacher Zugangsdaten (z. B. Nutzername und Passwort), jedoch ist diese Art von Schutz bei sensiblen Daten oder dem Zugriff auf hochpreisige Güter nicht ausreichend.
Will man beispielweise mit dem Smartphone den Zutritt zu einem Gebäude oder den Besitz eines ÖPNV-Jahrestickets nachweisen, sollten diese Funktionalitäten besser geschützt sein, als durch die Eingabe von Nutzername und Passwort. Andernfalls können diese Formen von eIDs zu leicht in unberechtigte Hände gelangen.
Natürlich ist es nicht notwendig, dass für alle Anwendungsfälle höchste Sicherheitsanforderungen einzuhalten sind. Der Nutzer erwartet dennoch zurecht, dass man seine Identität nicht einfach stehlen oder manipulieren kann.

SCHUTZ DER EIDS

Smartphones sind, wie jedes vernetzte Gerät, ständig der Gefahr eines Cyber-Angriffes ausgesetzt. Darum müssen besondere Voraussetzungen erfüllt sein, damit man davon ausgehen kann, dass eIDs auf dem Smartphone sicher gespeichert sind. Hier bietet sich ein Blick auf die „Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG", kurz eIDAS-Verordnung, und ihre definierten Vertrauensniveaus an. Die eIDAS-Verordnung unterscheidet drei Vertrauensniveaus: gering, substanziell und hoch. An jedes dieser Vertrauensniveaus ist eine Widerstandsfähigkeit gegen ein definiertes Angriffspotenzial geknüpft. Die Technische Richtlinie TR-03107 des BSI ist die nationale Ausprägung der eIDAS-Regulierung. Sie bietet viele Anhaltspunkte, welche Voraussetzungen einzuhalten sind, um die genannten Vertrauensniveaus und damit eine bestimmte Widerstandsfähigkeit gegen Cyber-Angriffe zu erreichen. In der Richtlinie werden u.a. Vorgaben zur Ausgabe und Verwaltung einer eID gemacht, aber auch dazu, welche Authentifizierungsmechanismen zum Einsatz kommen müssen. Daraus lässt sich ableiten, dass mindestens ein substantielles Vertrauensniveau notwendig ist, um in einem Smartphone eIDs ausreichend sicher zu speichern und zu verwalten.

Um einem substantiellen Vertrauensniveau zu genügen, muss das System einen Angriff mit dem Angriffspotenzial „moderate" im Sinne der Common Criteria Evaluation Methodology bzw. der ISO 18045 verhindern. Um diese Anforderungen sicher umzusetzen, empfiehlt das BSI, einen Hardware-Anker zu verwenden, da ansonsten ein erfolgreicher Angriff auf lediglich mit Softwaremitteln geschütztes kryptografisches Material nicht ausgeschlossen werden kann.

Moderne Smartphones verfügen über einen solchen Hardware-Anker in Form eines Secure Elements. Diese gibt es in Form von eingebetteten Sicherheitselementen oder als eingebettete SIM-Karte. Beide Varianten eines Secure Elements sind funktional eng mit den bekannten Plastik-Chipkarten verwandt und erreichen durch Verwendung hochentwickelter Sicherheitsfunktionen ein sehr gutes Sicherheitsniveau.

OPTIMOS 2.0

In dem vom Bundesministerium für Wirtschaft und Energie geförderten Forschungsprojekt OPTIMOS 2.0 entwickelt ein Konsortium aus Universitäten, Behörden und Unternehmen Lösungen, wie eIDs nach den oben genannten Kriterien sicher und praktikabel auf Smartphones gelangen können. Mit OPTIMOS 2.0 soll eine Infrastruktur geschaffen werden, die für alle Serviceanbieter diskriminierungsfrei zugänglich ist und höchste Sicherheits- und Datenschutzstandards erfüllt. Das zentrale Element ist hier der Trusted Service Provider, es als Schnittstelle zwischen Diensteanbietern und Endkunden übernimmt, die eIDs auf den Hardware-Anker einzubringen. Der Nutzer muss ledglich, wie gewohnt, seine Apps aus dem jeweiligen Appstore installieren. Um dies zu ermöglichen, engagiert sich das BSI in der Standardisierung der notwendigen Komponenten, Interfaces und Abläufe, damit die entwickelte Technologie für möglichst viele Endnutzer zur Verfügung steht. ■

Weitere Informationen:

https://www.bundesdruckerei.de/de/Unternehmen/Innovation/Optimos

Sicherer Online-Zugang zu Verwaltungsleistungen

Das Onlinezugangsgesetz als Werkzeug der Digitalisierung

von Michael Klabe und Dr. Ulf Löckmann, Referat eID-Lösungen für die digitale Verwaltung

Das Onlinezugangsgesetz verpflichtet Behörden von Bund, Ländern und Kommunen, ihre Verwaltungsleistungen auch elektronisch über einen Verbund von Verwaltungsportalen anzubieten. Um Bürger und Unternehmen sicher zu identifizieren und zu authentifizieren, stellen Bund und Länder dazu Nutzerkonten bereit. Das BSI macht in seinen Technischen Richtlinien (TR) Vorgaben, wie diese Nutzerkonten interoperabel genutzt werden können, und definiert die erforderlichen Vertrauensniveaus auf Basis der eIDAS-Verordnung der EU, denen Behörden ihre Verwaltungsleistungen zuordnen müssen.

Die Digitalisierung der Verwaltung ist von Bund, Ländern und Kommunen als wichtiges politisches Ziel identifiziert worden, nicht zuletzt, da Deutschland bei internationalen Vergleichen zum Umsetzungsgrad der Modernisierung und Digitalisierung der Verwaltung zumeist einen hinteren Rang einnimmt. Die Politik hat 2017 mit dem Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) reagiert, das „die bislang heterogenen IT-Strukturen bei Verwaltungsleistungen von Bund, Ländern und Kommunen sukzessive interoperabel gestalten“ soll.

TR-SERVICEKONTEN ALS RAHMENBEDINGUNG DER INTEROPERABILITÄT

Nutzerkonten als Basisfunktionalität von Servicekonten sind im Bereich vieler Länder schon seit längerem und nun auch beim Bund verfügbar. Deshalb war es wichtig, den Schutz der bereits getätigten Investitionen sicherzustellen. Um die Interoperabilität und das Vertrauen zwischen den Teilnehmern einer Föderation interoperabler Servicekonten gewährleisten zu können, müssen gemeinsame Standards und verbindliche IT-Sicherheitsmaßnahmen definiert werden. Jedes teilnehmende Servicekonto soll so sicher sein,

dass Anfragen zu personenbezogenen Nutzerdaten nur von berechtigten, an der Föderation teilnehmenden anderen Servicekonten kommen.

Der konkrete Auftrag an das BSI, diese Definition vorzunehmen, ergibt sich aus der Begründung zu § 8 Absatz 3 OZG. Danach legt das BSI die technischen Anforderungen an die Nutzerkonten und deren Verknüpfung, insbesondere an Datenschutz und Datensicherheit, in Form einer Technischen Richtlinie fest.

Dem in Realisierungsphasen gegliederten Projektplan der Bund-Länder-Projektgruppe „Interoperabler Servicekonten“ unter Federführung Bayerns folgend ist eine Aufteilung der „TR-03160 Servicekonten“ auf vier Teile vorgesehen. Parallel zur ersten Pilotierungsphase der „Interoperabilität von Bürgerkonten“ hat das BSI die ersten beiden Teile „Identifizierung und Authentisierung“ und „Interoperables Identitätsmanagement für Bürgerkonten“ erstellt. Für die späteren Pilotierungsphasen „Interoperables Identitätsmanagement für Postfächer“ und „Interoperables Identitätsmanagement für Organisationskonten“ sind entsprechende Teile vorgesehen. Außerdem können zukünftig weitere Teile hinzukommen, sofern für zusätzliche Funktionalitäten, wie etwa einen Dokumentensafe, Regelungsbedarf besteht (siehe Abbildung 1).

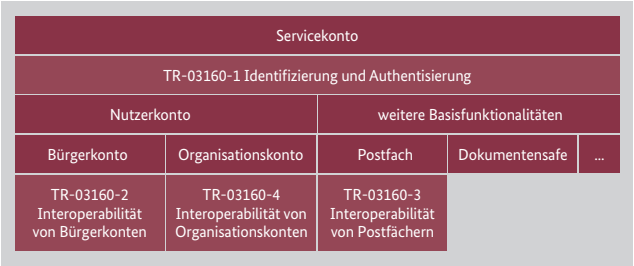


Abbildung 1: Gliederung der Technischen Richtlinie TR-03160 Servicekonten

EIDAS-VERTRAUENSNIVEAUS UND SERVICEKONTEN

Über die Nutzerkonten als Identifizierungs- und Authentisierungskomponente der Servicekonten können Bürger und Organisationen auf verschiedenen Vertrauensniveaus auf Online-Dienstleistungen aller Verwaltungsebenen zugreifen. Die erforderlichen Vertrauensniveaus nach der eIDAS-Verordnung werden im Einzelfall seitens der für die Dienstleistung zuständigen Verwaltung bestimmt und mit unterschiedlichen Anmeldeverfahren, die durch das BSI im Auftrag des IT-Planungsrates bewertet werden, erreicht. So können Online-Dienstleistungen mit sehr sensiblen personenbezogenen Daten auf eIDAS-Vertrauensniveau „hoch“ mittels der Online-Ausweis-Funktion des Personalausweises genutzt werden. Risikoarme Leistungen auf Vertrauensniveau „normal“ können hingegen über eine Kombination aus Benutzerkennung und Passwort genutzt werden (siehe Abbildung 2).

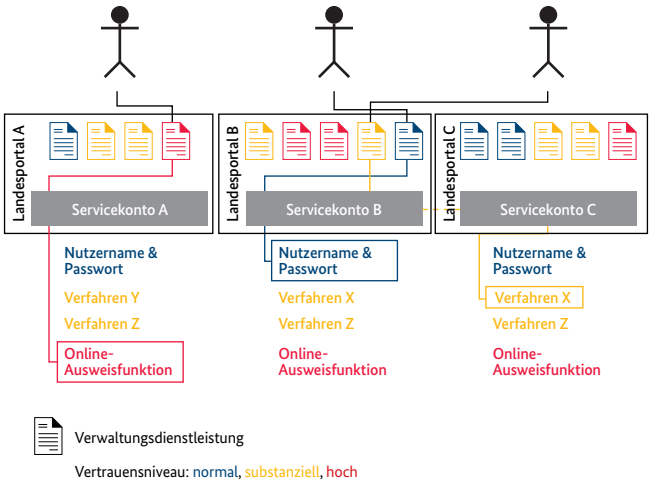


Abbildung 2: Landesportale mit Servicekonten und Verwaltungsleistungen auf verschiedenen Vertrauensniveaus

MEHRWERT FÜR NUTZER DURCH INTEROPERABILITÄT

Für Bürger sowie Organisationen ergibt sich aus der Identitätsföderation der Interoperablen Servicekonten ein großer Vorteil. Sie benötigen keine 17 Servicekonten für den Zugriff auf Verwaltungsleistungen von Bund und Ländern – ihnen genügt ein Servicekonto, mit dem sie auf die Services der anderen Föderationsteilnehmer zugreifen können. Damit nutzen sie künftig ein Single-SignOn im weiteren Sinne: Möchte beispielsweise der Inhaber eines Nutzerkontos beim Servicekonto NRW heiraten und muss dazu eine Geburtsurkunde aus seiner Geburtsstadt München beantragen, so benötigt er hierfür nicht auch noch ein Nutzerkonto beim Servicekonto Bayern-ID, sondern nutzt für diese Leistung sein NRW-Servicekonto. Entsprechendes gilt in viel größerem Umfang auch für Organisationskonten, die durch Unternehmen, Vereine oder Behörden genutzt werden können.

Das BSI unterstützt Behörden, die ihre Fachverfahren oder digitalisierten Prozesse in das Servicekonto einbinden möchten. Hilfestellung gibt das Referat DI 15 „eID-Lösungen für die digitale Verwaltung“ unter referat-DI15@bsi.bund.de. ■

Weiterführende Links:

BSI TR-03107
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03107/index_htm.html

eIDAS Verordnung (EU)Nr. 910/2014
https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910&from=DE

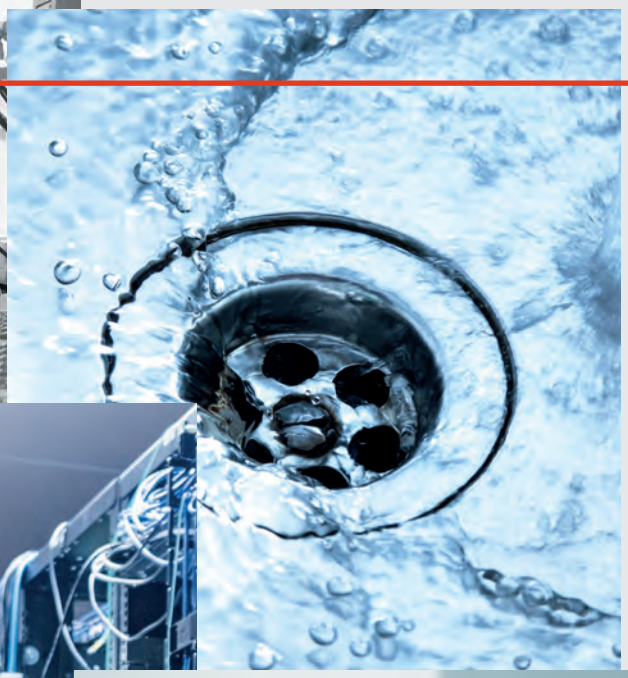
DAS BSI

Cyber-Sicherheit für Kritische Infrastrukturen

Das BSI als vertrauenswürdiger Partner für KRITIS-Betreiber

von Isabel Münch, Leiterin des Fachbereichs Kritische Infrastrukturen, und Dr. Henning-Timm Langwald, Referat Kritische Infrastrukturen - Grundsatz

Damit in unserer hochgradig IT-abhängigen Welt Strom und Wasser fließen, in Krankenhäusern Operationen durchgeführt oder die in der Cloud abgelegten Daten genutzt werden können, muss die dabei eingesetzte IT sicher und zuverlässig funktionieren. Insofern ist es konsequent, dass der Gesetzgeber Betreiber Kritischer Infrastrukturen (KRITIS) verpflichtet hat, für eine angemessene IT-Sicherheit zu sorgen. Das BSI hat die Aufgabe, die Betreiber dabei zu unterstützen.



Mit dem 2015 in Kraft getretenen IT-Sicherheitsgesetz (IT-SiG) wurden die Betreiber Kritischer Infrastrukturen verpflichtet, dem BSI schwerwiegende IT-Störungen zu melden, Maßnahmen zum Schutz ihrer IT-Systeme/-Prozesse zu treffen und die wirksame Umsetzung gegenüber dem BSI nachzuweisen. Dem BSI wurden somit im Umfeld Kritischer Infrastrukturen aufsichtsrechtliche Funktionen übertragen.

Die Rolle des BSI geht aber weit über diese Aufsichtsfunktion hinaus. Seit Jahren arbeitet es als Partner der KRITIS-Betreiber mit ihnen gemeinsam daran, die IT-Sicherheit zu verbessern, und verfolgt diesen kooperativen Ansatz auch nach Inkrafttreten des IT-SiG konsequent weiter. Daher unterstützt es die Betreiber Kritischer Infrastrukturen dabei, die gesetzlichen Regelungen konsequent umzusetzen. Diese langjährige, vertrauensvolle Zusammenarbeit erlaubt es dem BSI, das richtige Maß von Kooperation und Aufsicht zu wählen, um ein hohes Niveau der Informationssicherheit bei KRITIS-Betreibern effektiv und effizient zu erreichen.

ANGEMESSENES SICHERHEITSNIVEAU BEI KRITIS IN DER BREITE UND IN DER TIEFE

Durch das IT-SiG und die damit verbundenen Vorgaben an KRITIS-Betreiber und an das BSI wird ein Mindestsicherheitsniveau bei den durch das Gesetz regulierten KRITIS-Betreibern erreicht – mittels Sicherheitsmaßnahmen, die dem Stand der Technik entsprechen und dem Schutzbedarf angemessen sind. Durch das Gesetz bzw. die zugehörige BSI-Kritisverordnung werden diejenigen KRITIS-Betreiber adressiert, deren Anlagen in der Verordnung festgelegte Schwellenwerte übersteigen. Doch auch den KRITIS-Betreibern, die unterhalb dieser Schwellenwerte liegen, stehen die Unterstützungsangebote des BSI offen.

Zu den zahlreichen Produkten und Dienstleistungen für Betreiber Kritischer Infrastrukturen, die das BSI anbietet, gehören u. a.:

- Cyber-Sicherheitswarnungen und Lageinformationen: Erkenntnisse zu Vorfällen und Gefährdungen bereitet das BSI mit eigenem Expertenwissen auf. Ergibt sich daraus ein potenzielles Interesse für KRITIS-Betreiber, finden die Erkenntnisse Eingang in die Lageinformationen oder Cyber-Sicherheitswarnungen. Diese dienen der Information von KRITIS-Betreibern über aktuelle Schwachstellen, Sicherheitslücken sowie Vorfälle und Bedrohungen für IT-Systeme und enthalten Bewertungen des BSI, Empfehlungen für umzusetzende Sicherheitsmaßnahmen und z.B. konkrete Signaturen.

- Mobile Incident Response Team (MIRT): In herausgehobenen Fällen bietet das BSI Unterstützung durch eines seiner MIRTs an. Diese können schnelle Hilfe bei akuten Notfällen leisten und wurden beispielsweise bei Sicheheitsvorfällen in den KRITIS-Sektoren Ernährung und Gesundheit schon erfolgreich eingesetzt.

- IT-Sicherheitsberatung: Das BSI bietet KRITIS-Betreibern nach IT-SiG die Möglichkeit, sich bei der Einführung oder Umsetzung neuer Prozesse zu Sicherheitsfragen beraten zu lassen.

- Betreuung: Im Rahmen der partnerschaftlichen Kooperation unterstützt das BSI Betreiber dabei, gesetzliche Anforderungen umzusetzen und die geforderten Nachweise zu erbringen, u. a. durch Informationsmaterialien und auf einzelne KRITIS-Sektoren spezialisierte Ansprechpersonen.

- UP KRITIS: Der UP KRITIS dient als eine zentrale Drehscheibe, um Informationen sowohl zwischen BSI und Betreibern Kritischer Infrastrukturen als auch untereinander effektiv und partnerschaftlich auszutauschen. Er erlaubt es allen Betreibern, passiv als Teilnehmer vom Informationsfluss zu profitieren oder auch aktiv durch Mitarbeit in Branchen- und Themenarbeitskreisen die IT-Sicherheit mitzugestalten.

In diesen Angeboten zeigt sich, dass das BSI der Kommunikation mit den KRITIS-Betreibern aller Größenordnungen eine besondere Bedeutung zumisst, um die Probleme und Sorgen der Betreiber frühzeitig erkennen zu können und um hierauf aufbauend Angebote zu erstellen oder Hilfestellungen zu leisten.

KOOPERATION ALS GEMEINSAMER VORTEIL

Die intensive Kooperation mit den KRITIS-Betreibern ist für das BSI ein zentrales Anliegen. Durch Kooperation über die verschiedenen Branchen hinweg entsteht insgesamt eine höhere Transparenz über die Prozesse und Vorgehensweisen, die eingesetzte Technik und die umgesetzten Sicherheitsmaßnahmen bei den KRITIS-Betreibern.

Ein offener Erfahrungsaustausch ermöglicht es außerdem, von anderen Betreibern in derselben Branche oder mit vergleichbaren Prozessen oder IT-Systemen zu lernen. Das BSI schließlich nutzt den Überblick, den es so gewinnen kann, zum Vorteil aller Beteiligten. ■

Weiterführende Links:

„Kritische Infrastrukturen“ der BSI-Website: https://www.bsi.bund.de/kritis

Wichtige Downloads zum IT-SiG, inklusive Orientierungshilfen und Formulare: https://www.bsi.bund.de/kritis-downloads

Was wir wollen: Deine digitale Seite

Foto ©Markus Feger; Composing ©Jens Ripperger

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital·Sicher·BSI·

Als Cyber-Sicherheitsbehörde des Bundes kümmern wir uns darum, dass die Menschen in Deutschland der digitalen Welt vertrauen können. Mit derzeit rund 1000 Beschäftigten gestalten wir IT-Sicherheit in Deutschland – aber auch in Europa und der Welt.

Eine große Aufgabe für engagierte Fachleute, deren Herz auf der digitalen Seite schlägt.

Erfahren Sie mehr: **www.bsi.bund.de/karriere**

Weitere Informationen: **bewerbung@bsi.bund.de** oder unter Tel.: 0228 99 9582 6388.

Vom Gesetz in die Praxis

Fünf Jahre Mindeststandards: ein Rückblick

von Philipp Deuster, Referat Mindeststandards Bund

In der IT sind fünf Jahre eine lange Zeit. Das zeigt auch die Entwicklung der Mindeststandards des BSI für die Sicherheit der Informationstechnik des Bundes. Seit der ersten Veröffentlichung im Jahre 2014 ist vieles passiert. Zeit für einen Rückblick!

DIE ANFÄNGE

„Das Bundesamt erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes." So steht es seit 2015 in § 8 Abs. 1 des BSI-Gesetzes. Der erste Mindeststandard (zum Einsatz des SSL/TLS-Protokolls) wurde aber schon ein Jahr früher veröffentlicht, denn die Idee der Mindeststandards des BSI ist zu diesem Zeitpunkt schon einige Jahre alt. Bereits in der Gesetzesfassung von 2009 wurde die Möglichkeit erwähnt: „Das Bundesamt kann Mindeststandards für die Sicherung der Informationstechnik des Bundes festlegen." Bevor davon zum ersten Mal Gebrauch gemacht wurde, mussten allerdings zunächst Rahmenbedingungen geschaffen, Zuständigkeiten vergeben und Themen identifiziert werden.

ETABLIERUNGSPHASE

Nachdem der Mindeststandard „Transport Layer Security (TLS)" erfolgreich veröffentlicht war und die Gesetzesformulierung sich von einer Möglichkeit zu einer konkreten Aufgabe geändert hatte, wurde die Erstellung der Standards schließlich auch fest in der BSI-Organisation verankert: 2016 wurde das Referat „Mindeststandards Bund" gegründet. Zunächst wurde der Entwicklungsprozess standardisiert, um sicherzustellen, dass Mindeststandards effizient und transparent erstellt werden können. Dies setzte das Referat sogleich in die Praxis um und innerhalb eines Jahres folgten Veröffentlichungen zu den Themen Schnittstellen, Web-Browser, Cloud-Dienste, Mobile Device Management und HV-Benchmark.

Mindeststandard Zeitstrahl

2009
Erste Erwähnung im BSI-Gesetz

2011
Die Aufgabe, Realisierungsoptionen zu prüfen, wird formal vergeben

2014
Veröffentlichung des ersten Mindeststandards: Einsatz von TLS

2015
Änderung des BSI-Gesetzes

2016
- Gründung des Referats „Mindeststandards Bund"
- Standardisierter Entwicklungsprozess
- Einrichtung der zentralen Support-Kanäle (Mail und Hotline)
- Schnittstellenkontrolle v1.0 - erste Ressortkonsultation

2017
- Sichere Web-Browser v1.0
- Nutzung externer Cloud-Dienste v1.0
- Mobile Device Management v1.0
- Anwendung des HV-Benchmark v1.0
- Schnittstellenkontrolle v1.1 - erste Aktualisierung

AKTUELL BLEIBEN

Doch im IT-Bereich reicht es nicht, einen Sachverhalt einmal zu betrachten und Regelungen dazu zu veröffentlichen, denn die Technologie ist kurzlebig und entwickelt sich ständig weiter. Hinzu kommt, dass auch Prozesse stets optimiert werden können. Durch die gesammelte Erfahrung wurde bald deutlich, dass die veröffentlichten Mindeststandards früher oder später aktualisiert werden müssen - sei es wegen technischer Veränderungen oder auch wegen redaktioneller Verbesserungen. Ende 2017 wurde der Mindeststandard für Schnittstellenkontrolle daher bereits in der aktualisierten Version 1.1 veröffentlicht. Neben weiteren neuen Themen wurden im Laufe der Zeit auch die übrigen Mindeststandards überprüft und wenn nötig überarbeitet. So wurde der dienstälteste Mindeststandard (TLS) schließlich auch als erster „Major Release“ in die Version 2.0 überführt. Im Gegensatz zu den kleineren „Minor Releases“ erhalten hierbei die Anwender erneut die Möglichkeit, einen Entwurf zu kommentieren. Denn der Austausch mit dem Fachpublikum ist ein weiterer Punkt, der immer mehr an Bedeutung gewonnen hat.

KOMMUNIKATION IST ALLES

Mindeststandards werden aufgrund gesetzlicher Vorgaben erstellt und dürfen aus Sicht des BSI in der Bundesverwaltung nicht unterschritten werden. Trotzdem - oder viel eher deswegen - werden sie nicht im Vakuum erstellt. Das BSI versteht sich als Dienstleister und als solcher ist ihm daran gelegen, mit seinen Kunden im Dialog zu bleiben. Denn starre Verbote und Vorschriften tragen nicht zum Ziel der Informationssicherheit bei, wenn sie praxisfern sind und daher nicht umgesetzt werden. Schon im Gesetz steht, dass das BSI auf Ersuchen bei der Umsetzung der Mindeststandards berät. Doch die Anwender werden schon weit vorher in den Prozess eingebunden. Dieser Dialog wird auch weiterhin aktiv ausgebaut. Zu den zentralen Kontakten für Support-Anfragen und der möglichen Kommentierung von Beta-Entwürfen kommen immer neue Kommunikationskanäle hinzu. Seit September 2019 werden auch Vertreter der Länder über die AG Informationssicherheit (AG InfoSic) eingebunden und sind eingeladen, die Mindeststandards zu kommentieren und ggf. für ihre eigene Verwaltung zu adaptieren. Außerdem kann inzwischen der Mindeststandard-Newsletter abonniert werden, um regelmäßig über die Arbeit des Referats Mindeststandards Bund informiert zu bleiben.

AUSBLICK

Allein in 2019 wurden Mindeststandard-Dokumente über 40.000 Mal heruntergeladen. Das Interesse ist also hoch, daher soll das Angebot auch in Zukunft weiterentwickelt werden. Geplant sind unter anderem Vorträge, Workshops und weitere Hilfs- und Informationsmaterialien. Natürlich bleibt die Kernaufgabe - das Erstellen von Mindeststandards - ebenfalls nicht auf der Strecke. Es wird neue Mindeststandard-Themen geben und bereits veröffentlichte Dokumente werden weiterhin aktualisiert werden. Das stellt das Ende 2019 gestartete jährliche Monitoring sicher. ■

Weitere Informationen:

https://www.bsi.bund.de/mindeststandards

2018
- Mitnutzung externer Cloud-Dienste v1.1
- erster Community Draft
- HV-Benchmark v1.1
- Protokollierung und Detektion v1.0

2019
- TLS 2.0 - erste Aktualisierung als Major Release
- Nutzerpflichten NdB v2.0
- Sichere Web-Browser v2.0 - erste Beteiligung der Länder (AG InfoSic)
- Veröffentlichung des ersten Mindeststandard-Newsletter
- Druck der Mindeststandard-Broschüre

2020
Schnittstellenkontrolle v1.2

2020 - Ausblick:
- BAköV-Schulungen
- Weitere Aktualisierungen
- Neue MST-Themen
- Mindeststandard-Broschüre

Welcome on Board!

Neue Fachkräfte schnell einarbeiten und gut vernetzen

von Alessandra Krüger, Referat Personalgewinnung und -entwicklung

Nicht zuletzt wegen des engen IT-Arbeitsmarktes macht der Fachkräftemangel auch vor dem BSI keinen Halt. Darum spielt neben der Personalgewinnung auch die gute Einarbeitung und schnelle Bindung der neuen Kolleginnen und Kollegen im Wettbewerb um die besten Köpfe eine entscheidende Rolle. Ein erfolgreicher Start im BSI ist für die Motivation und Leistungsbereitschaft aller Mitarbeitenden von großer Bedeutung.

Durch den hohen Stellenzuwachs in den vergangenen fünf Jahren (plus 149 Prozent), sind die Herausforderungen des Onboardings im BSI vielfältig. Neue Mitarbeiter zu finden und zu gewinnen bindet viele Ressourcen im Personalbereich. Beim Onboarding arbeiten dann der Personalbereich und die Fachabteilungen Hand in Hand. Umso wichtiger ist ein gut abgestimmtes Zusammenspiel, damit die Erwartungen und Bedürfnisse aller Kolleginnen und Kollegen erkannt werden, die Zufriedenheit steigt und die Fluktuation so gering bleibt wie sie ist.

Während des Preboardings, also vor dem eigentlichen Dienstantritt, wird zwischen dem neuen Mitarbeitenden, dem Personalbereich und der zukünftigen Führungskraft besonders eng kommuniziert, sei es telefonisch, per Mail oder mit eigens entwickelten Postkarten. Dadurch können viele Fragen geklärt, Unsicherheiten beseitigt und Orientierung gegeben werden. Um die neuen Mitarbeitenden während dieser Zeit auch bereits sozial einzubinden, laden viele Fachabteilungen vorab zu Veranstaltungen im Haus ein. Bei Bedarf werden bereits erste Qualifizierungsmaßnahmen geplant. Das schnelle Personalwachstum des BSI und die hohe Spezialisierung der Mitarbeitenden erfordern von den Fachabteilungen beim Start, der neuen Fach- und Führungskräfte in erster Linie strukturierte Wissenstransfers zwischen alten und neuen Kolleginnen und Kollegen zu organisieren. Aus diesem Grund wurde ein flächendeckendes Patenmodell etabliert. Jede neue Mitarbeiterin bzw. jeder neue Mitarbeiter bekommt einen Paten zur Seite gestellt, der fachliche und persönliche Fragen beantwortet.

Daneben prägen selbstverständlich weiterhin die Führungskräfte das Ankommen der Mitarbeitenden. Das Feedback beider Seiten ist durchgehend positiv, obwohl die Anzahl der Einarbeitungsprozesse enorm ist.

DAS ONBOARDING-MODELL IM BSI

PREBOARDING

- Rekrutierung
  Erfassung Qualifizierungsbedarf,
  Klärung Erwartungen
- Kommunikation zu Personalbereich,
  Vorgesetztem und Paten

ORIENTIERUNGSPHASE

- Einführungsveranstaltung durch Personalberatung
- Begrüßungsmappe und Checkliste
- Abholung und Betreuung durch den Paten/die Patin
- Material, Schlüssel, IT bei jeweiligen Ansprechpartnern einsammeln
- Kennenlerngespräch Abteilungsleiter, Zentrale Aufgaben

INTEGRATIONSPHASE

- Einführungsmodule - Vorstellung aller Abteilungen und Ihrer Aufgaben
- Einarbeitung durch die Paten:
  Basis für kritische Fragen und gegenseitiges Lernen
  Einbindung in bestehende Projekte
- Teilnahme an Events (Sommerfest, Firmenlauf, Aktionsmonate, Projektvorstellungen)

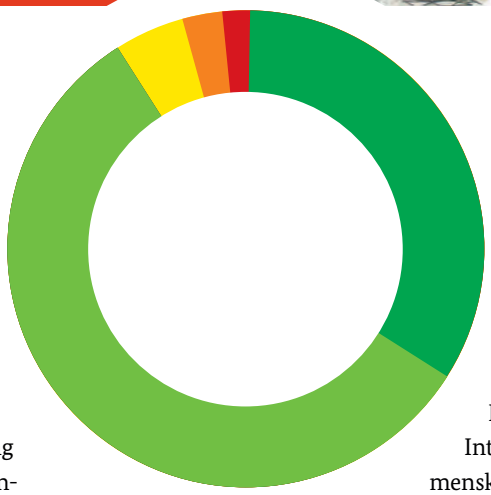
AUS EINEM INTERVIEW MIT EINEM PATENPAAR
(Patrick Klee (Pate) und
Hans Wetzel (neuer Mitarbeiter):

Was hat euch im Onboarding-Prozess bzw. in der Zusammenarbeit als Paten besonders gut gefallen?
Wetzel: Besonders gut gefallen hat mir, dass ich einen direkten Ansprechpartner für all die kleinen Fragen des Alltags habe, zum Beispiel: „Ich hab hier eine Frage zu den Passwörtern“ oder „Wie verbinde ich mich mit dem Drucker?“ und so weiter. Man wird hier sehr, sehr gut aufgenommen und das wird durch den ganzen Prozess des Onboardings noch mal unterstützt.

Klee: Strukturiert, aber dennoch offen genug. Das Arbeitsumfeld wirkt nicht so eingestaubt, wie man das von einer Behörde vielleicht vermutet. Das ist das BSI einfach nicht. Und die direkte Nähe, ohne formellen Prozess mit Terminvereinbarung etc., das ist das, was mir an unserem Patensystem besonders gut gefällt.

Wie läuft der Onboarding-Prozess im Vergleich zu anderen Unternehmen/Behörden ab?
Wetzel: Ich glaube, dass die Onboarding-Maßnahmen hier sehr gut durchstrukturiert sind und sehr geordnet ablaufen. Und vor allem ist es gut, dass es direkt vom ersten Tag an läuft, mit einer großen Informationsveranstaltung, auf der man direkt auch den Paten übergeben wird, das ist schon besonders.

ZUFRIEDENHEIT IM ONBOARDING



- sehr zufrieden 34%
- zufrieden 58%
- teils/teils 4%
- unzufrieden 3%
- sehr unzufrieden 1%

DER START IM BSI

Der erste Arbeitstag im BSI startet mit einem Rundum-sorglos-Paket. Alles ist gut vorbereitet: Empfang durch den Personalbereich, Begleitung durch den Paten oder die Patin und anschließend die sofortige Ausstattung mit allen Arbeitsmitteln, angefangen beim Post-it bis hin zu Hard- und Softwarekomponenten.

Der Personalbereich unterstützt mit einer zentralen Begrüßungsveranstaltung, um wichtige Informationen mitzuteilen und den bereichsübergreifenden Austausch unter den „Neuen“ zu fördern. Dies setzt sich in den folgenden Monaten durch die sogenannten Einführungsmodule fort. Alle neuen Mitarbeiternden besuchen sieben Module, in denen sich die verschiedenen Abteilungen des BSI vorstellen. Auch hier spielen das Kennenlernen und die Vernetzung eine wichtige Rolle. Zudem unterstützen saisonale Events, wie z. B. der Firmenlauf, das Sommerfest oder – typisch Rheinland – die Karnevalsparty, die Integration ins BSI, tragen zur Willkommenskultur bei und fördern ein positives Wir-Gefühl.

Im Ergebnis geben derzeit 92 Prozent der neuen Mitarbeitenden an, mit ihrem Onboarding im BSI sehr bzw. zufrieden zu sein. Neben dem Ziel, diesen Wert zu steigern, kommen zukünftig neue Herausforderungen auf das BSI zu. Durch die beiden neuen Standorte Freital und Saarbrücken wird Onboarding zukünftig an mehreren Standorten und dezentralisiert stattfinden. Es bleibt so spannend wie dynamisch.

Ein Tag im BSI

IT-Sicherheit ist vielfältig – und so sind es auch die Aufgaben in den rund 100 Referaten im BSI. Wie die Gestaltung von Informationssicherheit konkret aussehen kann, zeigen unsere Kollegen Petra Hofmann, Referat DI 22 „Cyber-Sicherheit für die Digitalisierung von IoT mit Smart Devices“ und Martin Zobel aus dem Referat BL 35 „Mindeststandards Bund“.

Martin Zobel
BL 35: Mindeststandards Bund

Martin Zobel startete 2016 als IT-Referent im BSI in der damaligen Abteilung B im Referat B12 (heute BL 35). Neben der Arbeit interessiert er sich für Laufsport und Reisen.

Petra Hofmann
DI 22: Cyber-Sicherheit für die Digitalisierung von IoT mit Smart Services

Petra Hofmann arbeitet seit Mitte 2017 im BSI. Direkt nach dem Abschluss im Studienfach Verwaltungsinformatik an der Hochschule des Bundes begann sie in der damaligen Abteilung D im Referat D32 (heute DI22). In ihrer Freizeit geht sie leidenschaftlich gern schwimmen, trifft Freunde oder probiert neue Kochrezepte aus.

08:12 Uhr

Meistens fahre ich mit der Straßenbahn zur Arbeit. Auf dem Weg in mein Büro spricht mich ein Kollege an. Wir haben eine Nachfrage aus einem Bundesministerium erhalten. Da diese einen von mir erstellten Mindeststandard betrifft, übernehme ich die Beantwortung. Dazu wähle ich die entsprechende Mail in unserem zentralen Postfach aus und erarbeite einen individuellen Lösungsvorschlag zur korrekten Umsetzung.

08:14 Uhr

Im ICE auf dem Weg von Bonn nach Mainz gehe ich noch einmal die Agenda und meine Notizen für den Tag durch. Derzeit beschäftige ich mich mit der IT-Sicherheit von Wearables. Heute findet eine Arbeitsgruppensitzung des Verbraucherdialoges zu genau diesem Thema statt. Ziel ist es, ein Papier mit Handlungsempfehlungen zu entwickeln, das vorwiegend die Hersteller adressiert und wertvolle Empfehlungen dazu geben soll, wie sichere Wearables entwickelt werden können.

10:00 Uhr

Das zuständige Fachreferat für Cloud-Computing führt einen Workshop für Cloud-Anbieter durch. Da ich mich für die praktischen Anwendungsbereiche von sicheren Cloud-Diensten sehr interessiere, habe ich einen 30-Minuten-Slot, um mein Fachthema vorzustellen. Die Teilnehmer sind sehr interessiert, welche Sicherheitsanforderungen Bundesbehörden bei der Nutzung von externen Cloud-Diensten einfordern müssen.

10:15 Uhr

Zunächst werden alle Teilnehmer der Arbeitsgruppe begrüßt und der Arbeitsgruppenleiter bedankt sich für die zahlreichen schriftlichen Beiträge aus der Arbeitsgruppe. Spannende und intensive Diskussionen zu unterschiedlichen Themen wie Daten- und Verbraucherschutz entstehen.

13:00 Uhr

Eigentlich stand nun ein referatsinternes Meeting an. Wegen eines häuslichen Notfalls konnte meine Kollegin aber heute nicht ins Büro kommen. Sie arbeitet daher von zu Hause, da sie auch dort Zugriff auf ihre Dateien und E-Mails hat. In einem Telefonat werten wir die aktuellen Ergebnisse aus dem Monitoring der bereits veröffentlichten Mindeststandards aus. Unsere Arbeitsergebnisse halten wir zusammen in unserem Wiki fest und konkretisieren unsere weitere Zeitplanung.

MINDESTSTANDARDS BUND

Das Referat BL35 beschäftigt sich schwerpunktmäßig mit der Konzeption, Weiterentwicklung und Pflege einer standardisierten Vorgehensweise, um Mindeststandards nach § 8 Abs. 1 BSIG zu erstellen, zu verwalten, zu überwachen und das entsprechende Änderungsmanagement zu organisieren. Hierbei ist es federführend zuständig, die damit verbundenen Abstimmungen, Konsultationen und Veröffentlichungen zu erstellen, durchzuführen und zu steuern.

CYBER-SICHERHEIT FÜR DIE DIGITALISIERUNG VON IOT MIT SMART SERVICES

Das Referat DI 22 gestaltet präventive IT-Sicherheit vom Smart Home bis zur Smart City für Staat, Wirtschaft und Gesellschaft. Ziel ist dabei, die eingesetzten Systeme resilient zu machen. Dafür werden Marktstudien, Bedrohungsanalysen und Technologiebewertungen geplant und durchgeführt. Darauf basierend werden in Zusammenarbeit mit Herstellern und Betreibern Sicherheitsstandards im Bereich Smart Home und Smart Cities (insbesondere Technische Richtlinien und Schutzprofile) für Produkte und Services erstellt.

13:51 Uhr

Der Mindeststandard über Mitnutzung von externen Cloud-Diensten hat die Beta-Phase erreicht. Damit steht das Konsultationsverfahren mit den verschiedenen Bundesministerien an. Die Bundesministerien haben dann die Gelegenheit, den Arbeitsentwurf aus ihrer fachlichen Sicht zu kommentieren. Gleichzeitig veröffentlichen wir auch einen Community Draft auf der BSI-Webseite. Hier bieten wir allen interessierten Fachleuten die Möglichkeit an, uns Rückmeldung zu geben.

14:35 Uhr

Eine hitzige Diskussion zum Thema Softwaresupport ist entbrannt. Manche Arbeitsgruppenmitglieder sind der Meinung, dass ein Mindestzeitraum, in dem sich der Anbieter verpflichtet, Softwaresupport für ein Produkt bereitzustellen, nicht tragbar ist, da es von unterschiedlichen Faktoren wie z.B. den Verkaufszahlen abhängt. Ich versuche unseren Standpunkt zu vertreten und halte dagegen, dass sich so ein Anbieter überlegen kann, wie er die Lauffähigkeit und Sicherheit seines Produktes auch in Zukunft sicherstellt. Und genau das trifft den Gedanken von, Security by Design', der eines der wichtigsten Prinzipien für unsere Arbeit im BSI ist. Mithilfe von technischen Richtlinien und Standards wollen wir erreichen, dass Sicherheit schon im Entwicklungsprozess eines Produkts berücksichtigt wird und nicht erst dann, wenn es eigentlich schon zu spät ist.

15:18 Uhr

Ich arbeite an einem Artikel über unsere Mindeststandards. Er soll in der nächsten Ausgabe einer IT-Fachzeitschrift erscheinen und den Prozess vorstellen, mit dem wir Mindeststandards nach § 8 Abs.1 BSIG erarbeiten. Diesen Prozess haben wir im Referat entwickelt und optimieren ihn ständig weiter. Die Publikation von Fachartikeln ist eine wichtige Aufgabe für mich. Sie bietet uns die Möglichkeit, ein breites Publikum auf unser Thema aufmerksam zu machen.

16:10 Uhr

Eine spannende Arbeitsgruppensitzung liegt hinter uns. Bevor wir uns auf den Heimweg machen, verabschiede ich mich noch persönlich bei den anderen Arbeitsgruppenmitgliedern und danke für die gute Zusammenarbeit. Ich freue mich, dass unsere Arbeit später in den Handlungsempfehlungen verankert wird. Und sicher sehe ich irgendwann auch entsprechend gestaltete Wearables in den Kaufhausregalen und Onlineshops.

16:52 Uhr

Für heute mache ich Feierabend, denn es ist Donnerstag. Da trifft sich um 17 Uhr immer die Laufgruppe des BSI für einen gemeinsamen Dauerlauf durch die nahe gelegene Rheinaue.

Weitere Informationen:

https://www.bsi.bund.de/eintagimbsi

Wir gestalten

Das BSI zertifiziert in der dritten Runde die Smart Meter Gateways und schafft die notwendige Basis für das Gelingen der Energiewende.

Das Jahr 2019 für das BSI

Rückblick

Das BSI gestaltet bei der Digitalisierung mit und leistet mit seinem Sicherheitskatalog und der internen 5G-Task Force wichtige Arbeit beim Ausbau des 5G-Netzes.

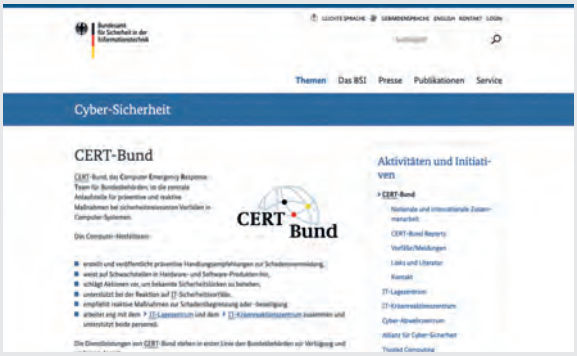
Das BSI brachte auf dem 16. IT-Sicherheitskongress rund 700 IT-Sicherheits-experten zusammen.

25 Jahre IT-Grundschutz

Das BSI feierte 25 Jahre IT-Grundschutz.

Wir vernetzen

Wir schützen



Das BSI baut seine CERT-Aktivitäten weiter aus und erweitertet seine Angebote für Wirtschaft, Bürger und Gesellschaft.

Das BSI erfüllt Ansprüche und schützte erfolgreich sowohl Regierungsnetze als auch Kritische Infrastrukturen.

Das BSI Mobile Incident Response Team hat erfolgreich und tatkräftig einen Krankenhausbetreiber bei der Entfernung einer Schadsoftware aus dem Netzwerk unterstützt.

Wir wachsen

Mit der Eröffnung des zweiten Dienstsitzes in Freital schafft das BSI zukünftig 200 neue Arbeitsplätze.

Das BSI hat 2019 insgesamt 350 neue Stellen geschaffen und bereits 143 Mitarbeiterinnen und Mitarbeiter im letzten Jahr willkommen geheißen.

Erfolgreiche Umstellung der IT-Systeme an 1200 Büroarbeitsplätzen.

IT-Sicherheit gemeinsam gestalten

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ)

von Manuel Bach, Leiter des Referats Nationales Cyber-Abwehrzentrum

Die komplexen Gefahren für die IT-Sicherheit gehen über feste Zuständigkeitsgrenzen der Sicherheitsbehörden hinaus. Für sich allein kann keine Einrichtung optimal auf die dynamische Bedrohungslage reagieren. Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) schafft durch permanenten Informationsaustausch zwischen allen sicherheitsverantwortlichen Bundesbehörden die Voraussetzungen für eine effektive Gefahrenabwehr und wirksame Prävention.

Mit dem 1. September 2019 wurden, mit der Verabschiedung einer neuen Geschäftsordnung des Cyber-AZ, wesentliche Änderungen wirksam. Erstmals haben sich alle beteiligten Behörden dazu verpflichtet, Verbindungspersonen vor Ort ins Cyber-AZ zu entsenden. Die neue Vor-Ort-Präsenz ermöglicht es nun, insbesondere die Menge der durch das Cyber-AZ herausgegebenen Lageprodukte zu erhöhen. Darüber hinaus erleichtert sie auch den Informationsaustausch und die Abstimmung operativer Maßnahmen bei akut zu bewältigenden Sachverhalten.

Gleichzeitig wurde die Struktur des Cyber-AZ an die ähnlicher Kooperationsplattformen angepasst. Nunmehr orientiert sich das Cyber-AZ am Modell des Gemeinsamen Terrorismusabwehrzentrums (GTAZ). Dort kooperieren die Beteiligten ohne Federführung einer einzelnen Behörde allein im Rahmen ihrer gesetzlichen Zuständigkeiten. Die Funktion des Leiters des Cyber-AZ wurde durch die eines Koordinators ersetzt. Diese Aufgabe wird seit dem 16. Dezember 2019 für die nächsten zwei Jahre durch das BKA wahrgenommen. Unterstützt wird das BKA dabei durch stellvertretende Koordinatoren des Bundesamtes für Verfassungsschutz (BfV) und der Bundeswehr/Kommando Cyber- und Informationsraum (KdoCIR).

Räumlich bleibt das Cyber-AZ weiterhin im BSI und damit auch in unmittelbarer Nähe des Nationalen IT-Lagezentrums/IT-Krisenreaktionszentrums und des CERT-Bund. Das BSI stellt darüber hinaus wie bisher die IT-Infrastruktur und Mitarbeiter für das Cyber-AZ und dessen Geschäftsstelle zur Verfügung.

Das Cyber-AZ ist ein Kernelement der 2011 ausformulierten Cyber-Sicherheitsstrategie (CSS), die den vorangegangenen „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ aus dem Jahr 2005 fortschrieb und gleichzeitig an die gewachsenen Herausforderungen des neuen Jahrzehnts anpasste. Offiziell eröffnet wurde es am 16. Juni 2011 durch den damaligen Bundesinnenminister Hans-Peter Friedrich.

Von nun an arbeiteten das BSI, das Bundesamt für Verfassungsschutz (BfV), das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), das Bundeskriminalamt (BKA), die Bundespolizei (BPOL), das Zollkriminalamt (ZKA), der Bundesnachrichtendienst (BND) und die Bundeswehr unter Federführung des BSI zusammen für mehr Sicherheit in der Informationstechnik.

BEHÖRDENÜBERGREIFENDE ZUSAMMENARBEIT

Nach einer intensiven Aufbauphase und ersten Erfolgen wurde 2014 die heutige „Operative Fallbearbeitung“ im Cyber-AZ eingeführt: Wird einer der im Cyber-AZ vertretenen Behörden ein akuter Cyber-Sicherheitsvorfall bekannt, der auch für mindestens eine weitere Behörde von Relevanz ist, wird eine Arbeitsgruppe dazu eingerichtet. Darin werden alle Informationen zum Vorfall ausgetauscht und auch die jeweiligen operativen Maßnahmen der einzelnen Behörden abgestimmt. Die Arbeitsgruppen tagen zwischen einmal wöchentlich und mehrmals täglich. Oftmals finden auch gemeinsame Termine bei Betroffenen eines Angriffs statt. Daran sind zwar häufig Verbindungspersonen aus dem Cyber-AZ beteiligt, die tatsächliche Facharbeit erfolgt aber durch die Kollegen in den Fachreferaten der jeweiligen Behörden.

Die Experten, die den Kern des Cyber-AZ bilden, werden also bei ihrer Arbeit durch die Kompetenzen und Ressourcen der jeweiligen Behörde unterstützt. Im BSI sind dies insbesondere die Mitarbeiter der Abteilung OC sowie die Kollegen der Fachbereiche TK 1 und WG 1. Virtuell verfügt das Cyber-AZ somit über eine vierstellige Anzahl von Mitarbeitern und durch die beteiligten Behörden über alle nötigen Befugnisse, um Cyber-Angriffe aufklären zu können. Das reicht von der Analyse von Netzwerkverkehr und gesicherten Daten über die Beschlagnahme von Servern bis zur Überwachung von Schadcode-Kommunikation. Vieles davon ist VS-VERTRAULICH oder GEHEIM eingestuft, weshalb die Arbeit im Cyber-AZ eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen („Ü3“) nach Sicherheitsüberprüfungsgesetz erfordert. Zudem wird das Cyber-AZ im BSI auch als eigener Sicherheitsbereich mit eingeschränkten Zutrittsrechten geführt.

INFORMATIONSAUSTAUSCH UND LAGEBERICHTE

Wochentags erstellt die Geschäftsstelle des Cyber-AZ eine interne Lageübersicht. Dabei stammt der Großteil der Meldungen von den Kollegen des Nationalen IT-Lagezentrums – ergänzt um Meldungen der übrigen Behörden. Diese interne Lageübersicht ist dann Grundlage für die tägliche Lagebesprechung der Verbindungspersonen im Cyber-AZ, in der die Lagebeiträge aus Sicht der einzelnen Behörden bewertet werden. Wird dabei ein Sachverhalt identifiziert, der eine hohe technische, politische und/oder mediale Relevanz aufweist, erstellt das Cyber-AZ dazu einen Beitrag für die „Cyber-Sicherheitslage Deutschland (CSLD)“.

Darin wird auf VS-NfD-Niveau kurz und auch für Nicht-Techniker verständlich der Sachverhalt erklärt und bewertet. Außerdem werden die Maßnahmen der zuständigen Cyber-AZ-Behörden dargestellt. Ursprünglich für die Unterrichtung der Staatssekretäre der Bundesressorts gedacht, wird die CSLD mittlerweile auch an alle Landeskriminalämter, Landesämter für Verfassungsschutz, den Verwaltungs-CERT-Verbund sowie die Koordinierungsstellen KRITIS verteilt. Zur CSLD kommen anlassbezogen noch – meist GEHEIM eingestufte – Hintergrundberichte in Form der „Informationen des Cyber-AZ“ hinzu, die jedoch nur einem sehr eingeschränkten Personenkreis zugänglich gemacht werden. ■

Gesamtstaatliche Sicherheit im Verbund

Ressortübergreifende Kooperation zwischen Kommando CIR und BSI

von Generalleutnant Ludwig Leinhos, Inspekteur Cyber- und Informationsraum der Bundeswehr

Der Cyber- und Informationsraum als Dimension kennt weder nationale noch institutionelle Grenzen. Erfolgreiches Handeln und Wirken innerhalb dieser Dimension ist nur gesamtstaatlich und ressortübergreifend denkbar. Dies führt in der logischen Konsequenz zu einer Zusammenarbeit zwischen dem BSI und uns, dem Kommando Cyber- und Informationsraum.

Die aktuelle Cybersicherheitsstrategie für Deutschland aus dem Jahr 2016 beschreibt den Bereich Cyber als Dimension ohne exakt greifbare politische oder institutionelle Grenzen. Zuständigkeiten sind nicht immer eindeutig. Folglich kann die nationale Sicherheitsvorsorge Deutschlands nur ressortübergreifend und gesamtstaatlich gedacht und umgesetzt werden. Die explizite Zusammenarbeit zwischen den Bundesministerien des Innern und der Verteidigung ist notwendig. Diesen politischen Auftrag setzt unser Kommando Cyber- und Informationsraum (Kommando CIR), das sowohl für die Sicherheit des Betriebs als auch für die Überwachung und den Schutz der IT-Systeme der Bundeswehr im In- und Ausland verantwortlich ist, in einer engen Zusammenarbeit mit dem BSI um.

Mitarbeiter des BSI verstärken das Blue-Team bei der Cyber-Abwehr-Übung Locked Shields

KONKRETE ZUSAMMENARBEIT SEIT 2019

Unser Referat Nationale und Internationale Zusammenarbeit des Kommandos CIR hat bereits früh Verbindung zu seinem Counterpart im BSI aufgenommen. Auf dieser Ebene entwickelt sich die Zusammenarbeit nach dem „Bottom-up-Prinzip“. In Gesprächen auf Arbeitsebene erörtern wir seit Anfang 2019 verschiedene Felder der Zusammenarbeit und arbeiten Vorschläge zu einer konkreten Umsetzung aus. So werden jetzt die bereits seit Jahren bestehenden guten Arbeitsbeziehungen zwischen dem BSI und der Informationssicherheitsorganisation der Bundeswehr gezielt weiter ausgebaut, gestärkt und neu ausgerichtet.

PERSONELLER AUSTAUSCH UND DAS SPEZIALFELD CYBER-RESERVE

Spitzenpersonal im IT-Bereich gewinnen und binden zu können, ist auch für uns eine große Herausforderung. Wir sehen uns aber nicht nur als Konkurrent zu anderen Akteuren, sondern wollen mit diesen gemeinsam Lösungswege erarbeiten, wie wir die Ressource „Mensch“ optimal nutzen können. Deshalb haben wir gemeinsam mit dem Bundesministerium der Verteidigung das Konzept der Cyber-Reserve entwickelt, um die Expertise aus Behörden, Wissenschaft und Industrie integrieren und einsetzen zu können. Schon jetzt bringen Fachleute aus dem IT-Lagezentrum des BSI als Reservedienstleistende ihr Wissen in unseren Organisationsbereich CIR ein. Zudem hat das Fachpersonal beider Häuser die Möglichkeit, durch Hospitationen Einblicke in die jeweiligen Arbeitsbereiche, etwa Kryptologie, IT-Grundschutz und Abstrahlprüfung, zu gewinnen, um dadurch die Zusammenarbeit und das gegenseitige Verständnis zu verstärken. Hier sind wir also auf einem guten Weg, denn erste bereits absolvierte Hospitationen haben unseren beiden Institutionen bereits wertvolle Erkenntnisse ermöglicht.

Wenn die Analysten des GLZ zu dem Ergebnis kommen, dass ein IT-Sicherheitsvorfall nicht nur die Bundeswehr betrifft, benachrichtigen sie über das Nationale Cyber-AZ die deutschen Sicherheitsbehörden

Generalleutnant Ludwig Leinhos, Inspekteur Cyber- und Informationsraum

AUSTAUSCH ZU SAP-SOFTWARE

Die Bundeswehr betreibt eine der größten SAP-Installationen in Europa. Auch hier können wir dem BSI, insbesondere im Sinne eines Erfahrungsaustausches, wertvolle Hinweise zum Betrieb und dem Schutz von Daten und IT-Infrastrukturen von SAP-Softwarelösungen bieten. Im Gegenzug dürfen wir auf die reichhaltige Erfahrung des BSI bei der Ausgestaltung von Netzsicherheit und modernen IT-Sicherheitsarchitekturen zurückgreifen. Der Austausch auf diesem Themenfeld, da sind wir uns sicher, ist fruchtbar und dient in erster Linie der Sicherung von SAP-Lösungen, die in öffentlichen Institutionen betrieben werden.

AUSTAUSCH VON IT-LAGEINFORMATIONEN

Die zentrale Rolle beim Austausch von Lageinformationen spielt für uns das Nationale Cyber-Abwehrzentrum (Cyber-AZ). Die verschiedenen Fähigkeiten und Möglichkeiten der Behörden im Cyber-AZ sollen auf unterschiedlichste Cyber-Bedrohungen reagieren können und der Bundesregierung ein gesamtstaatliches Cyber-Lagebild für Deutschland zur Verfügung stellen. Seit Anfang 2019 unterstützt ein ständiger Verbindungoffizier unseres Kommandos CIR vor Ort das Cyber-AZ. Darüber hinaus stellen wir seit Januar 2020 einen der stellvertretenden Koordinatoren im Cyber-AZ. Täglich tauscht unser Gemeinsames Lagezentrum Cyber- und Informationsraum (GLZ CIR) aktuelle Informationen mit dem Cyber-AZ aus.

Unsere Kooperation mit dem BSI im Bereich der Informationssicherheit beinhaltet auch den Austausch von Lageinformationen. Unser Cyber Security Operation Center (CSOCBw) tauscht im Auftrag unseres Chief Information Security Officer der Bundeswehr (CISOBw), meinem Stellvertreter, Generalmajor Jürgen Setzer, ständig und unmittelbar Informationen zur Informationssicherheitslage mit dem nationalen IT-Lagezentrum im BSI aus. Hier geht es vorrangig um aktuelle, konkrete Vorkommnisse, um schnell und mit zusätzlichen Informationen und Erfahrungen auf die Gefährdungen reagieren zu können. Darüber hinaus werden im nationalen CERT-Verbund meist technische Parameter zu Malware datenbankgestützt ausgetauscht. Als Betreiber und Nutzer einer der umfangreichsten und vielseitigsten IT-Infrastrukturen auf Bundesebene stellt die Bundeswehr somit eine wichtige Informationsquelle für die übergreifende nationale IT-Lage des BSI dar. Der unmittelbare Informationsaustausch erhöht damit die Sicherheit der IT der Bundeswehr und die Lagetransparenz im BSI.

ERFOLGREICHES NETZWERKEN IM SINNE GESAMTSTAATLICHER SICHERHEIT

Ich bin froh, dass wir mit dem BSI einen so hochwertigen Partner an unserer Seite haben, mit dem wir gemeinsam einen wesentlichen Beitrag zur gesamtstaatlichen Sicherheitsvorsorge Deutschlands leisten können. Diese Zusammen arbeit wollen wir weiter voranbringen – und zwar auf allen Ebenen. Das BSI ist der nationale Key Player. Doch allen, die auf dem Feld der Sicherheit des Cyber- und Informationsraums agieren, ist bewusst, nur gemeinsam und mit starken Partnern können wir in Deutschland die Chancen der Digitalisierung nutzen und dabei auch deren Risiken wirksam begegnen. Schlüssel hierzu ist die aktive Kooperation mit allen wichtigen Playern in der gesamtstaatlichen Cyber-Sicherheitsarchitektur.

So runden unsere Kooperationen mit weiteren nationalen Partnern, wie zum Beispiel der Telekom-Security, dem Fraunhofer-Institut FKIE innerhalb des Cyber Security Clusters Bonn, aber auch mit befreundeten Nationen aus der Europäischen Union, der NATO und darüber hinaus, das Bild eines erfolgreich vernetzten und gesamtstaatlichen Handelns ab. Gemeinsam machen wir mit dieser vernetzen Zusammenarbeit aller staatlichen und nicht staatlichen Stellen Deutschland ein großes Stück sicherer. ■

IT-SICHERHEIT IN DER PRAXIS

Scannen ersetzt Papier

Sichere und vertrauensvolle Digitalisierung mit den technischen Richtlinien des BSI

von Jawad Ahmad und Sascha Neinert, Referat eID-Lösungen für die digitale Verwaltung

Die Digitalisierung erfasst immer mehr Prozesse in der Verwaltung. Daneben muss jedoch auch der Umgang mit papiergebundenen Dokumenten geregelt werden. Wenn die betreffenden Dokumente eingescannt werden, können sie auch im Rahmen digitalisierter Verwaltungsabläufe verwertet werden. Derzeit steht das BSI als Cyber-Sicherheitsbehörde des Bundes selbst vor der Aufgabe, das ersetzende Scannen einzuführen.

Der Übergang zum „papierlosen Büro“, in dem Arbeitsprozesse vollständig elektronisch bzw. digital abgewickelt werden, wird sich früher oder später in den meisten Organisationen vollziehen. Oft stellt ein papiergebundenes Dokument den Beginn eines digitalen Prozesses dar (siehe Abbildung 1) und wird eingescannt, um es ohne Medienbruch weiter bearbeiten zu können. Die Langzeitspeicherung steht am Ende des Bearbeitungsprozesses, sofern das Dokument nicht unterdessen gelöscht wird. Für diese beiden wesentlichen Bereiche hat das BSI technische Richtlinien formuliert.

- Die BSI TR 03138 „Ersetzendes Scannen“ (TR-RESISCAN) widmet sich dabei der rechtssicheren Überführung papierbasierter Aufzeichnungen in eine digitale Form.
- Die BSI TR-03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“ (TR-ESOR) adressiert die ordnungsgemäße Aufbewahrung elektronischer Aufzeichnungen einschließlich der vollständigen Erhaltung von deren Beweiswert.

Abbildung 1: Generischer digitaler Prozess mit den technischen Richtlinien des BSI

Nach E-Government Gesetz und Vertrauensdienstegesetz wird der Stand der Technik eingehalten, wenn diese Richtlinien umgesetzt worden sind.

DAS ERSETZENDE SCANNEN

Die TR-RESISCAN regelt, wie Papierdokumente ordnungsgemäß und risikominimierend in elektronische Abbilder übertragen werden. Sie wird branchenübergreifend überall dort angewendet, wo ein hohes Maß an Rechtssicherheit und Nachweisfähigkeit digitaler Aufzeichnungen erforderlich ist. Erst das rechtssichere Einscannen von papiergebundenen Dokumenten ermöglicht eine vollständige digitale Vorgangsbearbeitung. Auch andere durch Papierdokumente hervorgerufene Medienbrüche können dadurch behoben werden.

Zahlreiche Institutionen und Dienstleister haben mit einer Zertifizierung nachgewiesen, dass sie die Vorgaben der TR- RESISCAN erfüllen. Doch nicht nur die Nachweisfähigkeit elektronischer Prozesse wird auf diese Weise gewährleistet. Ein weiterer wesentlicher Vorteil liegt darin, dass Lagerkosten für Akten signifikant gesenkt werden können, wenn Papier auch tatsächlich im Anschluss an den Scanprozess vernichtet wird. Je nach Aufwand liegen alleine die Lagerkosten für einen laufenden Aktenmeter (entspricht 12 Aktenordern) zwischen 25 und 60 Euro pro Monat.

BEWEISSICHERE LANGZEITSPEICHERUNG

Vor dem Hintergrund zum Teil jahrzehntelanger Aufbewahrungsfristen gilt es, geschäftsrelevante Aufzeichnungen eines digitalen Prozesses nach dem Stand der Technik sicher wie vertrauenswürdig aufzubewahren. Ein nach TR-ESOR zertifiziertes Produkt ermöglicht die beweiswerterhaltende Langzeitspeicherung basierend auf qualifizierten Zeitstempeln. Es gewährleistet die Integrität, die Authentizität und die Verkehrsfähigkeit der Dokumente. Die Richtlinie liegt demnächst in der Version 1.3 vor, die auch die Maßgaben der eIDAS-Verordnung umfasst.

EINSTIEG IN DIE PRAKTISCHE UMSETZUNG IM BSI

Seit November 2019 ist die Annahme der E-Rechnung für die unmittelbare Bundesverwaltung verpflichtend, also auch für das BSI. Rechnungen bis maximal 1.000 Euro (netto) können weiterhin in papierbasierter Form gestellt werden. Um die Vorteile einer einheitlichen digitalen Abwicklung der Rechnungsbearbeitung zu nutzen, hat sich das BSI für das ersetzende Scannen der Papierrechnungen nach TR-RESISCAN entschieden. Die gescannten Dokumente werden TR-ESOR konform persistent gespeichert. Um hierfür die notwendigen technischen und organisatorischen Umsetzungsschritte durchzuführen, sind Vertreter der Fachabteilungen, der hausinternen IT sowie Wissensträger der TR-RESISCAN am Projekt beteiligt. Das Projektteam wird durch die hauseigenen TR-Verantwortlichen für RESISCAN und TR-ESOR beraten. Im ersten Schritt wird dabei ein Scankonzept erarbeitet, das die Themen der Langzeitspeicherung mit aufgreift. Im Zuge der Erarbeitung des Scankonzepts ergeben sich dabei Aufgaben und Anpassungsbedarfe, die im Vorfeld einer operativen Umsetzung gelöst werden müssen.

Die Erkenntnisse, die sich aus der Entwicklung des Scankonzeptes ergeben, sollen Grundlage für ein Muster-Scankonzept sein, das dann durch weitere Organisationen und Behörden nachgenutzt werden kann. Das BSI unterstützt Behörden, die das ersetzende Scannen bei der Prozessdigitalisierung umsetzen möchten.

Hilfestellung gibt das Referat DI 15 „eID-Lösungen für die digitale Verwaltung“ unter resiscan@bsi.bund.de. ■

Weiterführende Links:

TR-RESISCAN
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03138/index_htm.html

TR-ESOR
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html

Wie sicher ist die Blockchain?

BSI Studie zu Blockchain-Anwendungen

von Dr. Manfred Lochter, Referat Vorgaben an und Entwicklung von Kryptoverfahren, und Jochen Rill, FZI Forschungszentrum Informatik, Karlsruhe

Blockchains sind seit einiger Zeit nicht nur Experten, sondern auch der breiten Öffentlichkeit vor allem durch die Kryptowährung Bitcoin bekannt. Welche Blockchain-Anwendungen gibt es aber überhaupt und wie sieht der Sicherheitsstandard existierender Angebote aus? Dazu hat das BSI eine umfassende Studie beauftragt und wichtige Erkenntnisse für ein umfassendes IT-Security-Lagebild für Blockchain-Anwendungen gewonnen.

Das BSI setzt sich seit 2017 intensiv mit dem Thema Blockchain auseinander. Nach der Veröffentlichung von Eckpunkten zur Sicherheit von Blockchain Anfang 2018 folgte 2019 eine umfangreiche Analyse des BSI („Blockchain sicher gestalten. Konzepte, Anforderungen, Bewertungen"), die unter Beteiligung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erstellt wurde.

NEUE STUDIE ZUR SICHERHEIT VON BLOCKCHAIN-ANWENDUNGEN

Um einen Überblick über existierende Blockchain-Anwendungen und deren Sicherheit zu gewinnen, hat das BSI 2018 das Forschungszentrum Informatik (FZI) mit einem Projekt zur „Sicherheitsuntersuchung ausgewählter Blockchain-Anwendungen" beauftragt. Dabei wurde zunächst ein Marktüberblick geschaffen und danach eine Reihe von Produkten exemplarisch auf ihre Sicherheitseigenschaften untersucht.

Im Rahmen der Marktanalyse wurden bei den gefundenen Angeboten u.a. die verwendeten Sicherheitsmechanismen, die Softwarequalität und die bisher bekannt gewordenen Sicherheitsvorfälle bewertet. Über 25 Prozent aller Angebote aus dem Blockchain-Ökosystem stammen aus den USA. Aus Deutschland stammen nur neun der im Rahmen der Marktanalyse ermittelten 303 Angebote (siehe Abbildung 1). Anschließend wurden, basierend auf den Ergebnissen der Marktsichtung und vorläufigen Bewertung, acht Blockchain-Angebote ausgewählt und einer umfassenden und detaillierten Sicherheitsanalyse unterzogen.

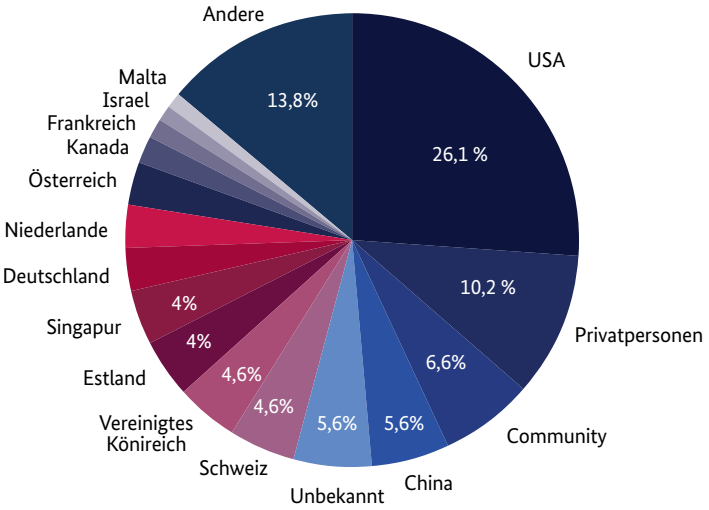


Abbildung 1

Dabei wurden verschiedene Arten von Angeboten, Anwendungsbereichen und Mechanismen abgedeckt. Ziel war es, eine angemessene Kombination aus theoretischen und praktischen Analysemethoden zu verwenden. Die Untersuchung beinhaltete als potenzielle Schwachstellen sowohl Programmfehler als auch Zufallszahlenerzeugung, Seitenkanäle, kryptografische Schwächen und auch produktspezifische zusätzliche Aspekte.

ERGEBNISSE DER SICHERHEITSANALYSE

Die Analyse und Bewertung lassen folgende allgemeinen Schlussfolgerungen zu:

- Es existieren so gut wie keine Angebote mit formalen Sicherheitsnachweisen, die wesentliche Teile des Angebots betreffen. Formale Sicherheitsnachweise existieren zwar für die eingesetzten kryptographischen Bausteine wie Verschlüsselungsverfahren oder Signaturfunktionen, viele Blockchain-Angebote versprechen jedoch weit darüber hinausgehende Sicherheitseigenschaften. Für diese Aussagen existieren in der Regel keine formalen Nachweise oder wissenschaftlichen Untersuchungen.

- Blockchain-Anwendungen spielen auf dem Markt kaum eine Rolle. Fast 80 Prozent aller untersuchten Anwendungen haben eine kleine oder sehr kleine Marktrelevanz. Auch hinsichtlich des Reifegrades bleiben Blockchain-Anwendungen hinter anderen Arten von Angeboten zurück: Nur knapp 20 Prozent aller Anwendungen sind in einem hohen oder sehr hohen Reifegrad, über ein Drittel aller Anwendungen sind bisher nicht über das Stadium einer Marketing-Webseite hinausgekommen.

- Existierende Angebote wurden bisher kaum öffentlichen Sicherheitsanalysen oder Penetrationtests unterzogen. Obwohl das Hauptverkaufsargument der meisten Blockchain-Angebote die Sicherheit ist, wurden nur in wenigen Einzelfällen vom Hersteller der Produkte unabhängige Sicherheitsuntersuchungen in Auftrag gegeben und deren Ergebnis veröffentlicht. In einigen wenigen weiteren Fällen wurden Sicherheitslücken von unabhängigen Forschern entdeckt. Diese wurden in fast allen Fällen schnell behoben. Eine Ausnahme bilden hier Hardware-Wallets und Blockchain-Clients, die überdurchschnittlich gut untersucht sind, jedoch zusammen weniger als 10 Prozent der Gesamtanzahl der untersuchten Angebote ausmachen.

- Blockchain-Clients und Hardware-Wallets haben den höchsten Entwicklungsstand. Für über 40 Prozent der untersuchten Hardware-Wallets und für 50 Prozent der untersuchten Blockchain-Clients existiert ein dokumentierter Prozess, um Sicherheitslücken zu melden. Eine große Anzahl der kommerziell verfügbaren Wallets und Clients wurde bereits einer Sicherheitsanalyse unterzogen. Diese Zahlen ergeben insbesondere vor dem Hintergrund Sinn, dass Sicherheitslücken in diesen Angeboten schnell zu einem Verlust von einer großen Menge Geld führen können.

- Mining-Hardware kommt aus China und Mining-Software von Privatpersonen. Über 70 Prozent der untersuchten Mining-Software wird von Privatpersonen entwickelt – der Hauptvertriebskanal ist ein öffentliches Forum. Die Hälfte der kommerziell verfügbaren Mining-Hardware kommt aus China; aus Israel, Schweden, Japan und den USA kommen jeweils nur ein bzw. zwei Produkte.

- Zahlungsverkehr und Spiele sind die Hauptanwendungsfelder von existierenden Blockchain-Anwendungen. Ein wesentlicher Teil der untersuchten Blockchain-Anwendungen (ca. 20 Prozent) ist für den Einsatz im Finanzsektor gedacht, bei dem zweitgrößten Teil handelt es sich um Spiele, die ihre Spieldaten in der Blockchain verwalten. Insbesondere die Anwendungsfelder Verwaltung, Internet of Things, Identitätsmanagement, Gesundheit und Energie, die häufig als Hauptverkaufsargument für Blockchain-Technologie genannt werden, sind bisher kaum von existierenden Blockchain-Anwendungen besetzt. Ein signifikanter Teil der Anwendungen (ca. 22 Prozent) ist überhaupt nicht in die klassischen Anwendungsfelder einzuordnen.

EVALUATION UND SCHLUSSFOLGERUNGEN

Sechs der acht detailliert untersuchten Blockchain-Angebote besitzen ein hohes Sicherheitsniveau. Im Rahmen des verfügbaren Untersuchungsaufwands dieser Studie konnten keine schwerwiegenden Schwachstellen gefunden werden. Ein untersuchtes Angebot ist jedoch fundamental unsicher, ein weiteres ist anfällig gegenüber Phishing-Angriffen.
Alle gefundenen Probleme wurden den jeweiligen Herstellern gemeldet. Reaktionen auf die Meldung von weniger kritischen Schwachstellen waren überwiegend positiv. Auf die Meldung der beiden kritischen Probleme erfolgte keine Reaktion. Keines der in diesen Fällen gemeldeten Probleme ist nach unserem aktuellen Kenntnisstand behoben.
Grundsätzliche Probleme, die im Rahmen der Studie aufgedeckt wurden, sind

- der hohe Grad an gemeinsam verwendeten Code-Bausteinen zwischen den untersuchten Angeboten, insbesondere was kryptographische Verfahren angeht,
- die ungewöhnliche Wahl der kryptographischen Basisprimitiven, sowie
- die hohe Anzahl an Abhängigkeiten zu externen Programmbibliotheken, die in veralteten Versionen (teilweise mit bekannten Sicherheitslücken) eingesetzt werden.

Zusammenfassend lässt sich sagen, dass die meisten der untersuchten Produkte und Technologien aus dem Blockchain-Ökosystem einen ungewöhnlich hohen Security-Reifegrad haben – insbesondere, wenn man das geringe Alter des Technologiefelds bedenkt. Die Gründe dafür lassen sich in der starken Fokussierung auf IT-Sicherheit und in dem hohen Finanzvolumen im Blockchain-Markt vermuten. Beide Faktoren machen es für IT-Sicherheitsexperten attraktiv, in dem Umfeld von Blockchain tätig zu werden. Hinzu kommt aber auch die Auswahl der zu untersuchenden Produkte.

Es ist allerdings auffällig, dass nur sehr wenige Konzepte und Lösungen aus dem Blockchain-Ökosystem bisher wissenschaftlich fundiert untersucht wurden. Das lässt sich insbesondere an der geringen Zahl veröffentlichter wissenschaftlicher Publikationen erkennen, die ein Peer-Review-Verfahren durchlaufen haben. Das ist vor allem deswegen problematisch, weil die Sicherheitsgarantien, die von verschiedenen Produkten gegeben werden, neuartig und häufig nicht vollständig verstanden sind. Sie sollen in der Regel durch eine Kombination von verschiedenen kryptographischen Maßnahmen erreicht werden. Würde man sich an der aus der kryptografischen Forschung bekannten Standardmethodik orientieren, wäre die Anfertigung eines formalen Sicherheitsnachweises erforderlich.

Bei der Produktevaluation hat sich gezeigt, dass bekannte Methoden aus dem klassischen Penetration Testing (wie z. B. statische Code-Analyse, Fuzzing und Reverse Engineering) auch für Blockchain-Produkte anwendbar sind. Eine Herausforderung dabei ist allerdings der hohe initiale Aufwand, der bereits notwendig ist, um ein Testsystems aufzusetzen. Da die Blockchain-spezifischen Code-Teile in vielen Produkten identisch sind, ist es fraglich, ob für Blockchain-Produkte eine eigene Testmethodik notwendig ist.

Es scheint zielführender, eine zielgerichtete Untersuchung der in geteilten Code-Bausteine durchzuführen, da die Ergebnisse eine Vielzahl von Produkten betreffen werden. Das betrifft insbesondere die unter vielen Produkten geteilte Implementierung der kryptographischen Primitiven, aber auch die „Bitcoin Improvement Proposals“ (BIP), die eine zu RFCs ähnliche Funktion im Blockchain-Ökosystem übernehmen. ■

Weiterführende Links:

https://www.bsi.bund.de/blockchain

Produktgetriebene Umsetzungsmöglichkeiten einer VS-Cloud

von Aljona Wehrhahn-Aklender, Referat Produkte und Systeme für Verschlusssachen (VS)

Die Cloud bietet viele Vorteile im Vergleich zu klassischen Rechenzentren, wie beispielsweise die ressourcenschonende Hochverfügbarkeit und schnelle Skalierbarkeit. Wenn allerdings neue Angriffsszenarien auf die IT-Sicherheit nicht berücksichtigt werden, kann die gesamte Infrastruktur kompromittiert werden. Am Beispiel eines Dokumentenmanagementsystems wird skizziert, mit welchen IT-Sicherheitskonzepten diesen Angriffsszenarien begegnet werden kann.

VERSCHLUSSSACHEN IN DER CLOUD

In der Bundesverwaltung wächst die Nachfrage nach Cloud-Rechenzentren. Ein Beispiel hierfür ist die IT-Konsolidierung des Bundes, bei der das zentrale Rechenzentrum zur Bereitstellung von IT-Diensten als Cloud umgesetzt wird. Durch die Wahl einer Cloud können die IT-Dienste (Services) bedarfsgerecht und beschleunigt zur Verfügung gestellt werden. Dabei sollen einige der IT-Dienste zur Verarbeitung von Daten mit dem Einstufungsgrad VS-NfD befähigt werden. In diesem Rahmen ist zu prüfen, welche IT-Sicherheitsprodukte in diesem IT-System IT-Sicherheitsfunktionen zum Schutz der Verschlusssache umsetzen und einer Zulassung bedürfen. Um relevante IT-Sicherheitsprodukte zu identifizieren, sind für benötigte Anwendungsfälle relevante Angriffsszenarien auf die Verschlusssache zu erfassen und daraus die Bedrohungslage abzuleiten. Zusätzlich müssen geltende organisatorische Rahmenbedingungen definiert und berücksichtigt werden.

MERKMALE EINER CLOUD

Eine Cloud ist eine hinsichtlich der dynamischen Verwaltung von IT-Ressourcen optimierte Ausprägung eines klassischen Rechenzentrums. Ein Rechenzentrum bietet zentral verwaltete IT-Ressourcen über eine Netzwerkverbindung und meistens für mehrere verschiedene Anwendergruppen (Mandanten) an. Eine Cloud verändert die IT-Infrastruktur des Rechenzentrums, indem es die Zuweisung der IT-Ressourcen abstrahiert und diese bedarfsgerecht und meistens vollständig virtualisiert in Form von IT-Diensten zur Verfügung stellt. Die IT-Dienste bieten hierzu eine standardisierte Schnittstelle nach außen, die sich ebenfalls für eine Automatisierung administrativer Prozesse eignet. Die IT-Ressourcen werden in einen gemeinsamen Ressourcenpool zusammengefasst und unter Anwendung von cloud-spezifischen Services durch Cloud-Infrastruktur-Komponenten verwaltet. So realisiert z.B. die Komponente zum Netzmanagement die Netzanbindung einzelner Instanzen über einen entsprechenden cloud-spezifischen Service. Die Komponenten können zentral administriert werden. Die zentrale Administration einer Cloud bietet zusätzlich ein einheitliches Monitoring an.

Dem Kunden können IT-Dienste aus unterschiedlichen Abstraktionsebenen zur Verfügung gestellt werden:

- Infrastruktur-as-a-Service (IaaS) stellt Infrastruktur (Speicher, Rechenkapazität, Netzwerkdienste) bereit,
- Plattform-as-a-Service (PaaS) bietet bereits vorkonfigurierte Ausführumgebungen,
- Software-as-a-Service (SaaS) sind IT-Dienste, die ganze Anwendungen abbilden.

Bei dem nachfolgenden Beispiel eines Dokumentenmanagementsystems (DMS) handelt es sich um ein SaaS. Neben den Servicemodellen, ist die Bereitstellungsform ein wesentliches Unterscheidungsmerkmal bei Clouds. Es wird unterschieden, ob eine Cloud im eigenen Rechenzentrum aufgebaut wird (On-Premise Private Cloud), ob ein Provider IT-Dienste für beliebige Mandanten (Public Cloud) oder für eine eingeschränkte Gruppe (Community Cloud) zur Verfügung stellt. Im Fall der Bundesverwaltung können nur Mandanten aus der Bundesverwaltung auf die Cloud zugreifen, was einen Zugriff über bundeseigene Netze begünstigt.

IT-SICHERHEIT IN DER CLOUD

Da es sich bei der Cloud um eine Client-Server-Architektur handelt, können, sofern keine Schutzmaßnahmen getroffen wurden, klassische Angriffe auf die Kommunikationsverbindung zwischen Client und Server durchgeführt werden. Außerdem bestehen klassische Angriffsmöglichkeiten auf die Anwendungsschicht, z. B. über Schadsoftware. Diese Angriffe sollten bei jedem Rechenzentrum in die Ermittlung der Bedrohungslage einfließen und über geeignete IT-Sicherheitsmaßnahmen adressiert werden.

Zusätzlich existieren in einer Cloud aufgrund der komplexen und dynamischen IT-Infrastruktur neue Angriffsszenarien.

Zur softwareseitigen Verknüpfung von Einzelsystemen zur mandantenfähigen Gesamtinfrastruktur werden verschiedenste Cloud-Infrastruktur-Komponenten benötigt. Diese Komponenten verfügen über eine hohe Anzahl an Services mit API-Schnittstellen, Verknüpfungen und Abhängigkeiten. Eine gleiche Komplexität weisen PaaS und SaaS auf. Es resultiert eine erhöhte Zahl an Möglichkeiten, schädlichen Programmcode unbemerkt in eine Cloud einzuschleusen.

Zudem kann durch die Virtualisierung von IT-Ressourcen die Reichweite eines erfolgreichen Angriffs zusätzlich erhöht werden, sofern die logische Separierung der Ressourcen IT-Sicherheitslücken aufweist. Eine IT-Sicherheitslücke wäre beispielsweise, wenn eine Separierung von Daten in Speichermedien nicht voll umfassend greift. Abbildung 1 zeigt einen Angriff, bei dem der Angreifer die Daten des Arbeitsspeichers des Opfers ausliest, indem er die logische Separierung überwindet.

Eine Cloud bietet aber auch eine Vielzahl an Möglichkeiten, um das IT-Sicherheitsniveau in einem Rechenzentrum zu steigern. Beispielsweise ermöglicht die Automatisierung schnellere Update-Zyklen, wodurch die Softwareaktualität steigt. Dies schützt vor Sicherheitslücken, die typischerweise in klassischen Rechenzentren durch veraltete Software entstehen. Außerdem wird durch die zentrale Administration der Gesamtinfrastruktur das IT-Sicherheitsmanagement vereinfacht, da z.B. eine Detektion von Sicherheitsvorfällen zentralisiert und umfassend erfolgen kann.

LÖSUNGEN FÜR EINE SICHERE CLOUD AM BEISPIEL DOKUMENTENMANAGEMENTSYSTEM (DMS)

Grundsätzlich sind bei einer Cloud im Bereich Datensicherheit die Integrität, Vertraulichkeit und Verfügbarkeit der Daten sowohl während des Transfers als auch am Endpunkt zu schützen. Weiterhin ist die Integrität und Verfügbarkeit der Cloud als Plattform sowie von bereitgestellten IT-Diensten sicherzustellen. Um den Angriffsszenarien in einer Cloud zu begegnen, können geeignete IT-Sicherheitsprodukte in die Cloud-Infrastruktur eingebunden werden. Sie zeichnen sich dadurch aus, dass sie wirksam schützen, ohne die Funktion der Cloud einzuschränken. Dies stellt insbesondere aktuelle VS-Produkte vor Herausforderungen, da diese nicht für eine virtualisierte, mandantenfähige und softwareseitig abstrahierte Rechenzentrumsinfrastruktur konzipiert sind. Um einen Überblick über den benötigten Funktionsumfang zu erhalten, sollte sich an IT-Sicherheitslösungen orientiert werden, die bereits erfolgreich im Markt agieren. Am Beispiel DMS lässt sich systematisch aufzeigen, wie die verschiedenen IT-Sicherheitsziele in einer Cloud adressiert werden können.

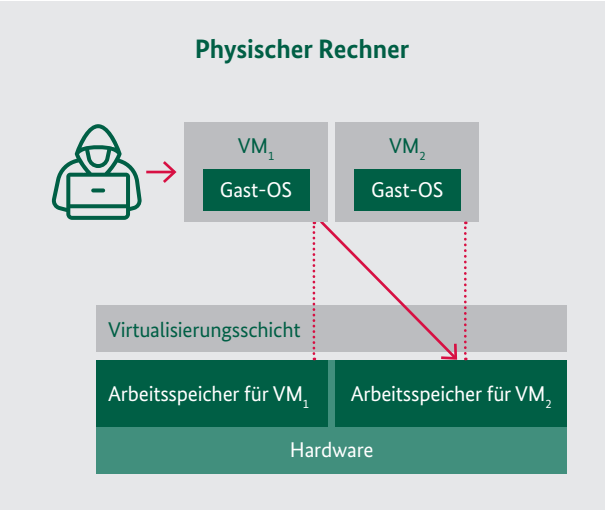


Abbildung 1

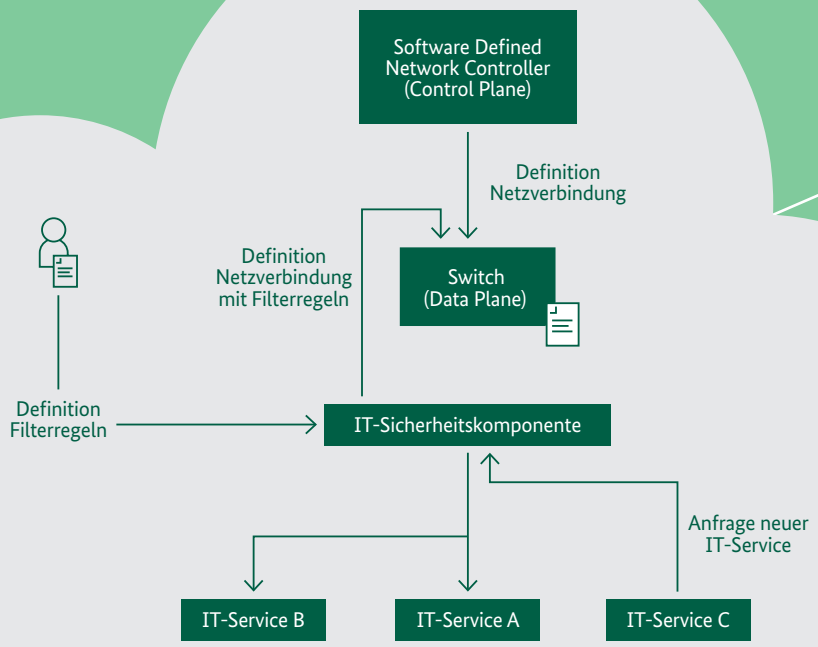


Abbildung 2: Dynamische Datenflusskontrolle, Umsetzungsbeispiel

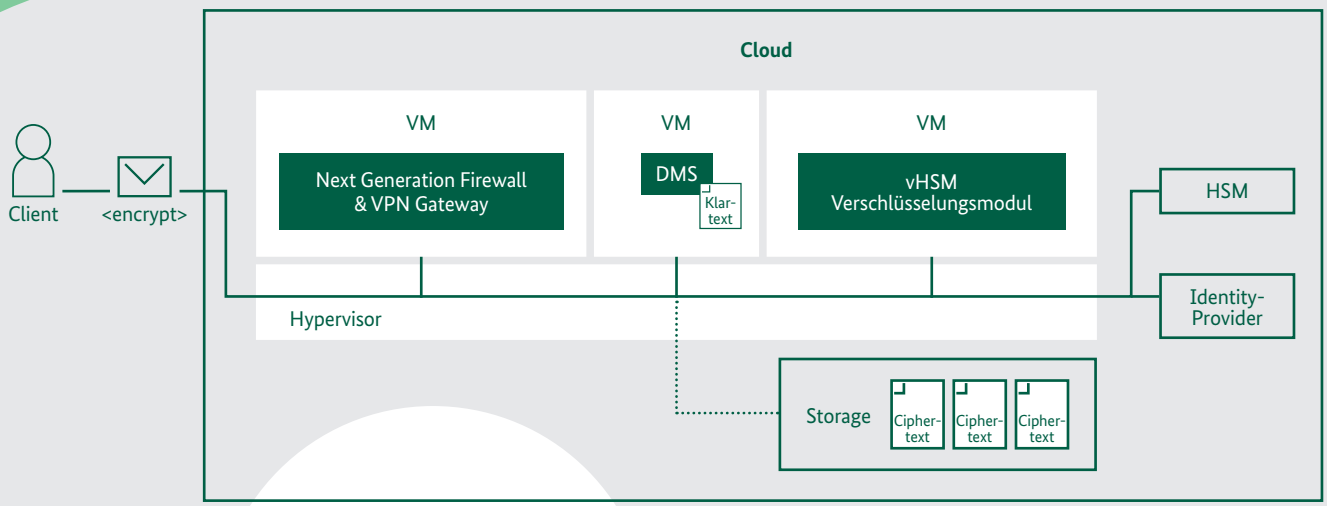


Abbildung 3: Datensicherheit auf der Cloud, Umsetzungsbeispiel

DATENSICHERHEIT

Die Datensicherheit in einer Cloud sollte bei allen Servicemodellen (SaaS, PaaS, IaaS) realisiert werden. Während des Datentransfers kann dies z. B. über klassische Verfahren wie einer verschlüsselten Übertragung über ein geeignetes Protokoll geschehen. Es muss sichergestellt werden, dass Netzwerkgrenzen innerhalb der internen Netzwerkkommunikation eingehalten werden. Hierfür existieren im Markt verschiedene Lösungen, die innerhalb von virtuellen Netzwerken Netzwerkregeln umsetzen. Diese Komponenten setzen auf virtuellen Netzen ab Layer 4 auf und ermöglichen ein feingranulares Management von Datenflüssen zwischen Identitäten (Next Generation Firewalls, Service Meshes). Sie können beispielsweise Software-Defined Networking (SDN) mit erweiterten Filterregeln ergänzen und dafür IP-Tables-Einträge erweitern. Abbildung 2 zeigt eine mögliche Architektur einer Next Generation Firewall.

Erreichen die Daten das DMS, ist zu unterscheiden, ob sie ausschließlich gespeichert oder ob sie auf der Cloud auch verarbeitet werden sollen. Im Fall einer reinen Datenspeicherung sollten die Daten vor Eintritt in die Cloud über ein hybrides Verschlüsselungsverfahren angemessen verschlüsselt werden. Ein hybrides Verschlüsselungsverfahren zeichnet sich dadurch aus, dass die Daten über einen symmetrischen Schlüssel geschützt werden, welcher wiederum durch ein asymmetrisches Verschlüsselungsverfahren abgesichert wird. Wenn mehrere Speichermedien verschiedener Provider zur Verfügung stehen, kann über eine zusätzliche, redundante Fragmentierung der Daten und dessen verteilte Ablage eine höhere Datenverfügbarkeit (Resistenz gegen den Ausfall einzelner Provider) realisiert werden.
Sollen die Daten auf der Cloud verarbeitet werden, sind sie zur Laufzeit vor unbefugten Zugriffen zu schützen. Im Markt setzen sich für die Zugriffssteuerung Mechanismen durch, bei denen die Authentisierung gegen einen Identity Provider erfolgt, der die restliche Zugriffskontrolle über ein integritätsgeschütztes Token als Identitätsnachweis (z.B. JSON Web Signature Tokens) verwaltet.

Zur Härtung des Zugriffsschutzes sollte durch die Cloud eine isolierte Ausführumgebung, z. B. über einen geeigneten Hypervisor, bereitgestellt werden. Außerdem muss für kryptografische Verfahren innerhalb der Cloud (z. B. für eine persistente Speicherung) sichergestellt werden, dass das Schlüsselmanagement auf die Dynamik der Cloud reagieren kann. Die Schlüsselerzeugung und die Schlüsselhaltung von initialen Schlüsselwerten (z. B. root/Master-Keys) kann für besonders schützenswerte Daten z. B. über ein netzseitig angebundenes Hardware Security Module (HSM) realisiert werden, sollte aber mit virtuellen Instanzen zur dynamischen Schlüsselverteilung ergänzt werden. Hierbei ist auf die gegenseitige Authentisierung zu achten. Abbildung 3 zeigt eine mögliche Einbettung von IT-Sicherheitsprodukten zum Schutz des DMS.

INTEGRITÄT VON PLATTFORM UND IT-DIENSTEN

Die hohe Komplexität einer Cloud erhöht die Gefahr von Softwareschwachstellen und Fehlkonfigurationen, die durch einen Angreifer ausgenutzt werden können. Um dieses Risiko zu minimieren, sollten IT-Maßnahmen zur Prävention mit IT-Maßnahmen zur Detektion kombiniert werden. Zur Prävention von Schwachstellen gibt es verschiedenste Tools, die an mehreren Stellen über den gesamten Lebenszyklus der Softwareentwicklung prüfen, ob im Code oder dessen Abhängigkeiten Softwareschwachstellen vorliegen. Dies ermöglicht Entwicklungsprozesse nach dem Vorbild der Secure Development Operations (SecDevOps) und verhindert, dass angreifbare Software in der Cloud vorliegt. Konfigurationsfehler können durch erhöhte Automatisierung reduziert werden. Um eine sichere Konfiguration, sowohl zum Zeitpunkt des Rollouts als auch im laufenden Betrieb, zu gewährleisten, können zusätzlich vollautomatisierte und regelmäßige Compliance-Überprüfungen über entsprechende Tools durchgesetzt werden. Diese Lösungen sollten durch ein umfangreiches Monitoring ergänzt werden, das optimalerweise auch eine Anomalie-Detektion anhand der Zugriffsgewohnheiten ermöglicht. ■

Cyber-Sicherheit in der Prozessindustrie

BSI und chemische Industrie arbeiten erfolgreich zusammen

von Klaus Biß, Marc Meyer, Jens Kluge und Andreas Erdrich, Referat Industrielle Steuerungs- und Automatisierungssysteme

In der chemischen Industrie wird der Schutz von Menschen und Umwelt mit fehlersicheren Einrichtungen der Prozessleittechnik erreicht. Neben dem Schutz vor Gefahren, die sich aus dem Produktionsprozess selbst ergeben, sind durch die zunehmende IT-Vernetzung mit wachsender Priorität auch Aspekte der Cyber-Sicherheit bei der funktionalen Sicherheit (Safety) zu berücksichtigen. In einem Arbeitskreis aus Vertretern der chemischen Industrie und dem BSI wird daher momentan ein IT-Grundschutz-Profil erstellt und an einer Demonstrationsanlage Cyber-Security umgesetzt.

Der Fokus des IT-Grundschutz-Profils Chemie liegt darauf, Prozessleittechnik-Sicherheitseinrichtungen (PLT-Sicherheitseinrichtungen) in Chemieanlagen gegenüber Cyber-Angriffen abzusichern. Daher werden Gefahren betrachtet, die direkt oder indirekt zu einer Kompromittierung der PLT-Sicherheitseinrichtungen führen können. Hierzu werden die bestehenden Leitsätze, Empfehlungen und Arbeitsblätter konkretisiert. Dabei handelt es sich um

- KAS 51 (Kommission für Anlagensicherheit - Leitfaden KAS-51 Maßnahmen gegen Eingriffe Unbefugter),
- EmpfBS 1115 (Ausschuss für Betriebssicherheit - Umgang mit Risiken durch Angriffe auf die Cybersicherheit von sicherheitsrelevanten MSR-Einrichtungen),
- NA 163 (IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen) und
- NA 169 (Automation Security Management in der Prozessindustrie).

Das Profil soll den Betreibern von Chemieanlagen erleichtern, ein Informationssicherheitsmanagementsystem (ISMS) für die funktionale Sicherheit auf Basis von IT-Grundschutz umzusetzen. Hierzu werden die PLT-Sicherheitseinrichtungen betrachtet, die diese Funktion übernehmen. Auch ohne eine gesonderte Betrachtung von Cyber-Angriffen werden für Chemieanlagen systematische, ganzheitlich angelegte Gefahrenanalysen der chemisch-verfahrenstechnischen Prozesse durchgeführt. Sie münden in eine belastbare Risikobewertung, so dass bereits wichtige Aspekte einer IT-Risikoanalyse vorweggenommen und entsprechende Schutzmaßnahmen ergriffen werden. Das IT-Grundschutz-Profil ergänzt dieses Schutzkonzept um die Härtung der PLT-Sicherheitseinrichtungen gegenüber Cyber-Gefahren.

Die Empfehlungen sollen sich in bestehende Prozesse integrieren lassen. So soll der Aufwand für den Betreiber reduziert und auch Prüfern aufgezeigt werden, welche Aspekte durch andere Standards und Regularien bereits erfüllt sein sollten. Dies erlaubt dem Betreiber, die dadurch freigewordenen Ressourcen zur Umsetzung weiterer Sicherheitsmaßnahmen einzusetzen.

Das Profil wird aus einem Hauptdokument sowie Anhängen bestehen. Das Hauptdokument beschreibt den Geltungsbereich sowie übergeordnete Ziele. Die Anhänge erläutern die Anforderungen. Hierzu gehören Überlegungen, Hintergründe und Entscheidungen zur Schutzbedarfsfestlegung, die Anforderungsanpassung an das industrielle Umfeld und eine Übersicht der Gefahren.

SCHUTZBEDARF

Abhängig von der relativen Höhe des Risikos wird PLT-Sicherheitseinrichtungen als Maß für deren geforderte Zuverlässigkeit ein Safety Integrity Level (SIL) zugewiesen. Die Höhe des SIL gibt dabei einen Hinweis auf die

Größenordnung des (ungeminderten) Risikos. Das IT-Grundschutz-Profil sieht allerdings hinsichtlich der Festlegung des Schutzbedarfs keine dem SIL entsprechende Differenzierung vor, da für die durch IT-Sicherheitsvorfälle verursachten Ausfallraten keine mit der funktionalen Sicherheit vergleichbare Datenbasis existiert. Daher wird im Profil ein hoher bis sehr hoher Schutzbedarf für den Geltungsbereich festgelegt. Dieser orientiert sich an der Kernabsicherung nach IT-Grundschutz.

REFERENZARCHITEKTUREN

Der Informationsverbund des IT-Grundschutz-Profils enthält alle essenziellen IT- und Operational Technology (OT-) Assets für PLT-Sicherheitseinrichtungen in einer chemischen Produktionsanlage. Die unterschiedlichen Lösungen zur Umsetzung einer PLT-Sicherheitseinrichtung werden schematisch in Form eines Netzstrukturplans für ein Produktionsnetz dargestellt. Der Betreiber wählt die für ihn am ehesten zutreffende Umsetzung aus.

BEISPIEL EINER REFERENZARCHITEKTUR UND ZONENEINTEILUNG

Bei der Konstruktion bzw. beim Aufbau der PLT-Sicherheitseinrichtung wird zwischen verschiedenen Sicherheitszonen unterschieden (siehe Abb. 1): Die Kern-PLT-Sicherheitseinrichtung (Zone A) umfasst die PLT-Sicherheitseinrichtung gemäß Definition in IEC 61511-1: Logiksystem, die Ein- und Ausgabebaugruppen inkl. Remote-I/O sowie die Aktoren und Sensoren. Verbindungen und ggf. vorhandene Netzwerkkomponenten (Kabel, Switches, etc.), die der Verbindung zwischen Geräten der Zone A dienen, werden gleichfalls dieser Zone zugeordnet. Im Zweifel gilt: Wenn die Hardware-, Software- oder Netzwerkkomponente notwendig ist, um die Sicherheitsfunktion auszuführen, zählt diese zu Zone A.

Komponenten, die für die Ausführung der Sicherheitsfunktion nicht notwendig sind, jedoch das Verhalten der Kern-PLT-Sicherheitseinrichtung beeinflussen können, werden der erweiterten PLT-Sicherheitseinrichtung (Zone B) zugeordnet. Typische Beispiele sind: Bedien-Eingabe-Panels, Visualisierungsstationen, das Programmiergerät (Engineering Station) für die PLT Sicherheitseinrichtung und das Asset Management System (AMS) bzw. Vorrichtungen zur Sensor/Aktor-Konfiguration sowie Gateways, Firewalls, Konverter und Router.

In der Produktionsumgebung befinden sich Komponenten und Systeme, die weder direkt noch indirekt der PLT-Sicherheitseinrichtung zuzuordnen sind, aber in Verbindung mit der Sicherheitsfunktion stehen können. ■

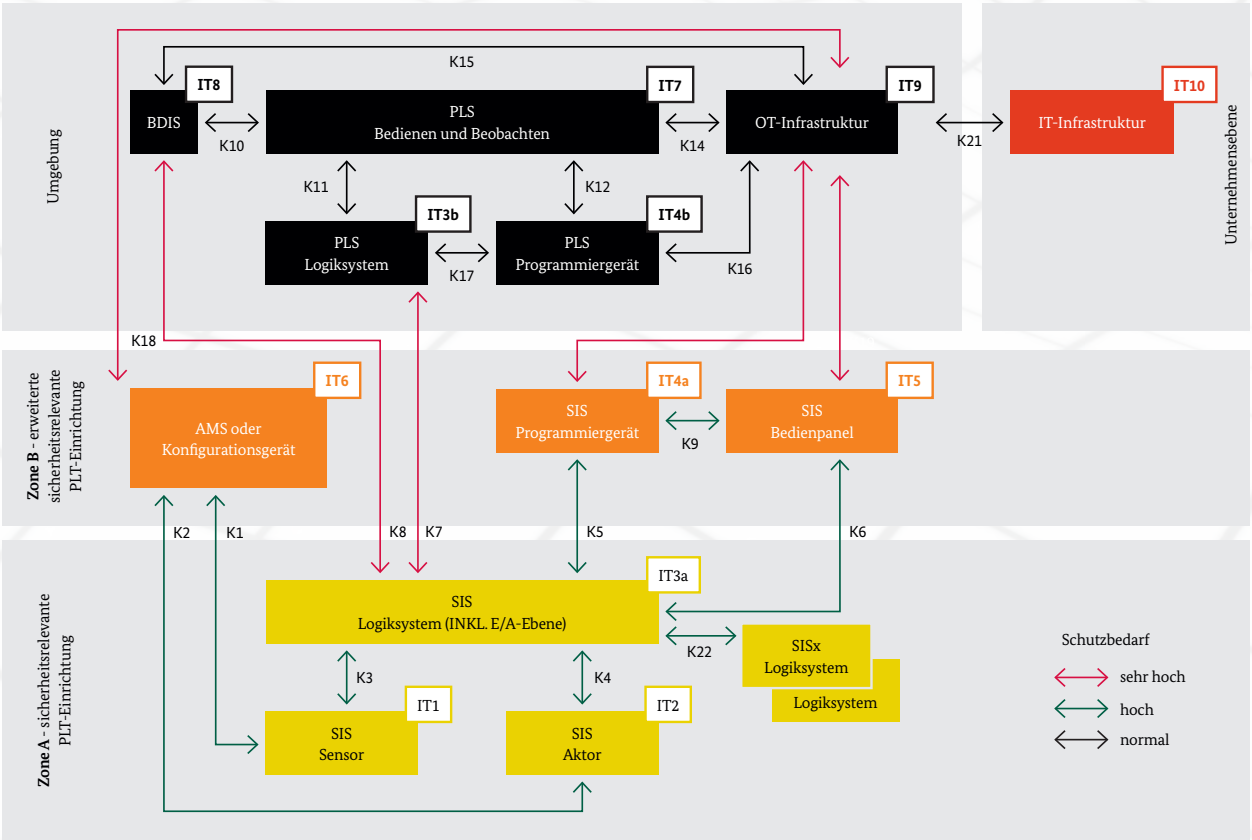


Abbildung 1: Netzstrukturplan für eine PLT-Sicherheitseinrichtung (SIS). Wesentliches Merkmal dieser Architektur ist, dass die Aufgaben der Produktion und SIS sowohl durch separate Programmiergeräte als auch Logiksysteme erfüllt werden. Der Schutzbedarf der Kommunikationsverbindung (K), aus Sicht der SIS, ist bei Zonenübergang oder kritischen Funktionen der verbundenen Komponente erhöht.

DEMOANLAGE ALS REFERENZIMPLEMENTIERUNG FÜR INDUSTRIE 4.0

Der Arbeitskreis Industrie 4.0 der Interessengemeinschaft Regelwerke Technik (IGR) betreibt eine Demoanlage, mit der die Einsatzmöglichkeit von Industrie 4.0-Anwendungen für Bestandsanlagen der Prozessindustrie erprobt werden kann (siehe Abbildung 2).

Bei ihrem Aufbau wurde Wert darauf gelegt, auf proprietäre Sonderlösungen weitestgehend zu verzichten und offene Standards einzusetzen bzw. diese zu etablieren. Die Demoanlage dient aber auch kooperierenden Herstellern zu Testzwecken von Neuentwicklungen industrieller Steuerungskomponenten auf Feldebene vor deren Markteinführung.

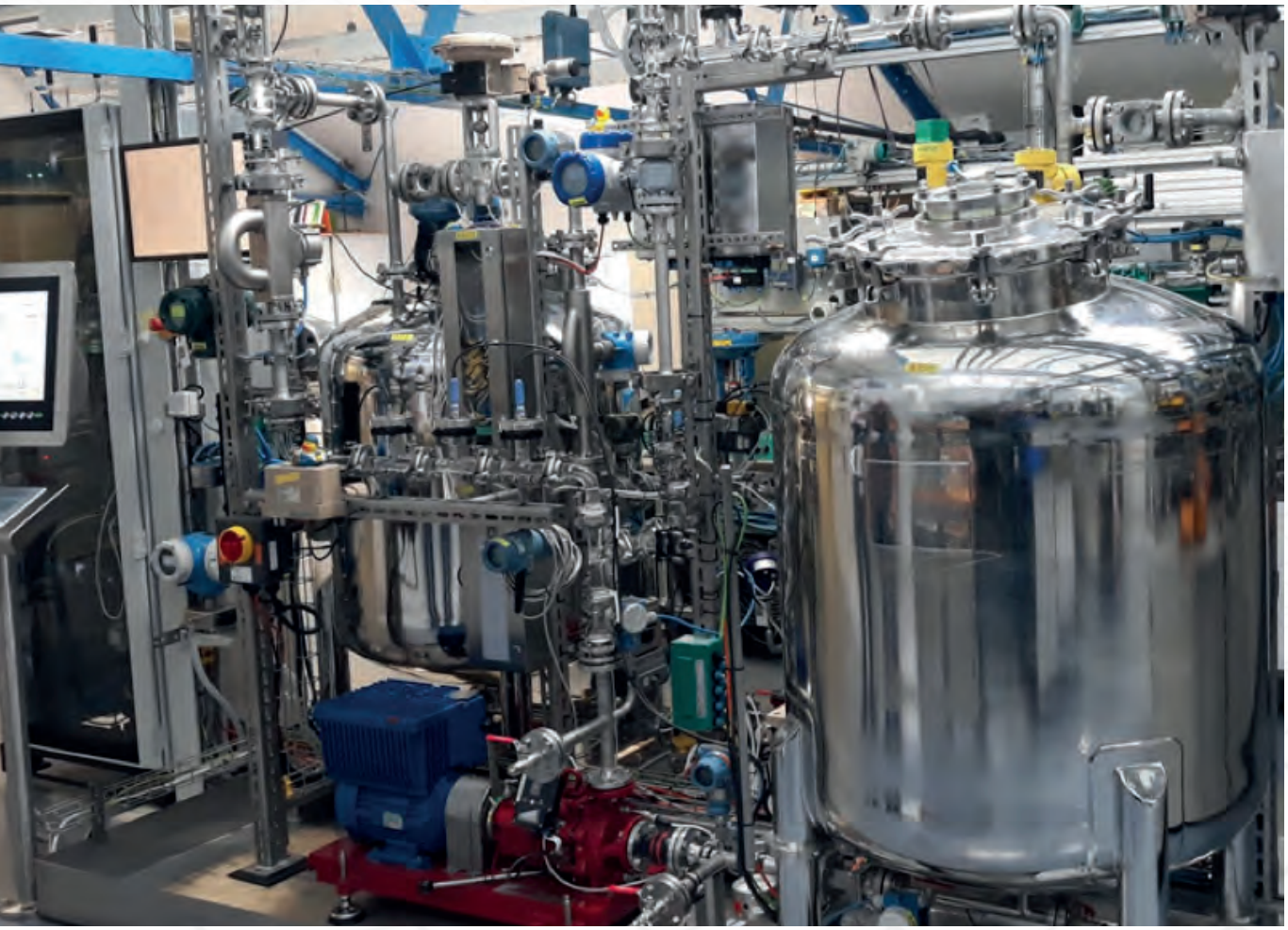


Abbildung 2: Demoanlage der IGR e.V. am Standort Frankfurt Höchst

Die Demoanlage bildet funktionell einen relativ simplen Prozess nach, der dem einer Brauerei ähnelt. Dabei kann eine Flüssigkeit zwischen zwei Tanks mittels elektrischer Pumpen umgefüllt werden. Füllstands-, Druck- und Durchflusssensoren erfassen dabei die zur Steuerung und Regelung der Anlage erforderlichen Parameter. Sämtliche Bauteile und Feldgeräte entsprechen den Anforderungen des Explosionsschutzes. Die Demoanlage ist allerdings mit Wasser befüllt und ermöglicht einen gefahrlosen Betrieb. Ein zentraler Gedanke war die Möglichkeit, gezielt Fehlerzustände in der Anlage erzeugen zu können. Durch diese spezielle Auslegung der Anlage sind fehlerhafte Betriebszustände wie Lufteinperlung, Kavitationseffekte, die Verspannung von Pumpenlagern und teilgefüllte Rohrleitungen gefahrlos möglich. Diese Szenarien zielen dabei insbesondere auf mögliche Anwendungen der Industrie 4.0 ab, die z. B. mittels Predictive Maintenance Ausfallzeiten vorhersagen und Schäden verhindern sollen. Zu diesem Zweck werden in der Demoanlage Prozessdaten über ein sogenanntes Edge-Gateway hier an Cloud-Dienste ausgeleitet, um z. B. rechenintensive Berechnungen wie Machine Learning zeiteffizienter durchführen zu können.

Weiterhin ist in der Demoanlage eine Referenzarchitektur der NAMUR Open Architecture (NOA) umgesetzt worden. In diesem offenen und herstellerunabhängigen Standard haben es sich die in der NAMUR organisierten Anwender aus der Prozessindustrie zur Aufgabe gemacht, bislang ungenutzte Daten über einen zweiten Kanal für eine Auswertung zugänglich zu machen.

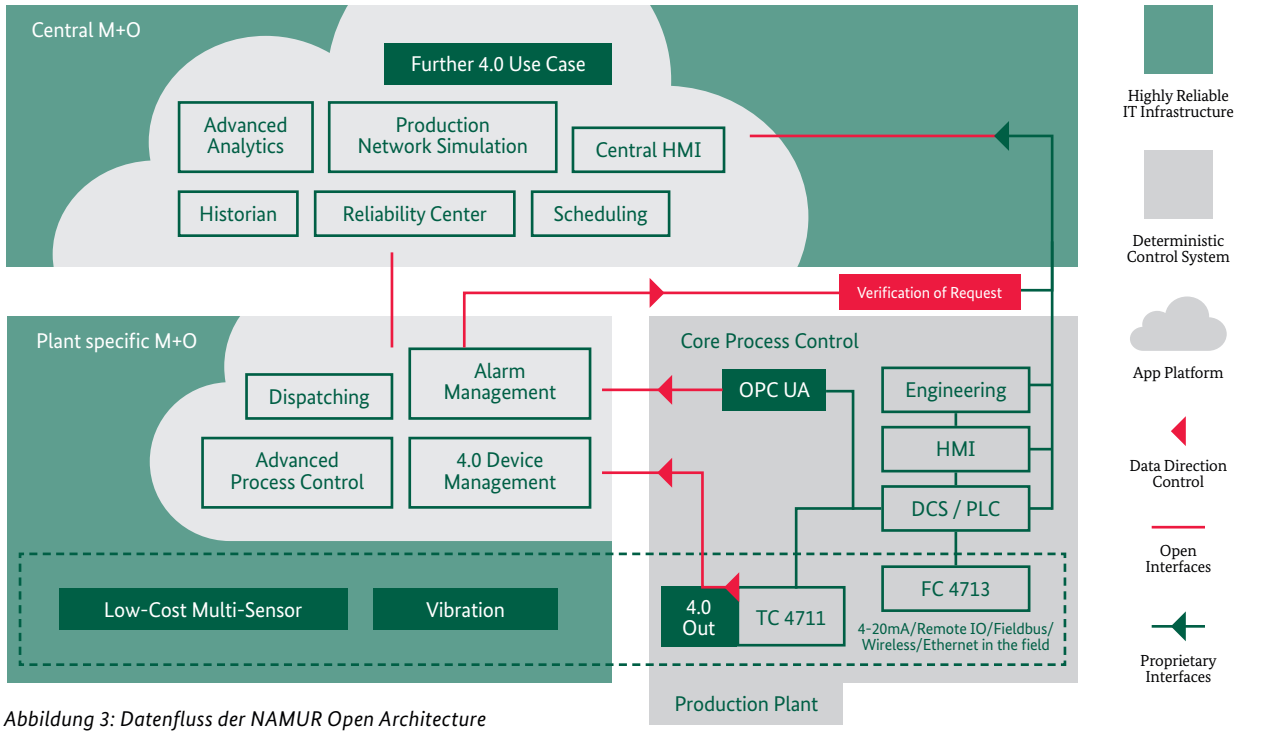


Abbildung 3: Datenfluss der NAMUR Open Architecture

Dadurch sollen Industrie 4.0-Anwendungen auch für Bestandsanlagen ermöglicht werden (siehe Abbildung 3).

Daten der Kern-Automatisierung (Core Process Control) sollen durch offene Schnittstellen in die Systemwelt für Monitoring und Optimierungsaufgaben exportiert werden können. Zusätzliche Sensorsignale werden durch einen zweiten Kommunikationskanal direkt an den bestehenden Feldgeräten abgeholt. Der Einsatz zusätzlicher Sensorik, die nicht Teil der Kern-Automatisierung ist, ermöglicht neue Monitoring- und Optimierungsfunktionen. An diese zusätzliche Sensorik bestehen deutlich niedrigere Anforderungen, z. B. bei der Verfügbarkeit.

MEHRWERT DER ZUSAMMENARBEIT

Das BSI unterstützt die IGR in den Arbeitskreisen Industrie 4.0 und IT/OT-Security sowie die NAMUR in den NOA-Arbeitskreisen in Bezug auf die IT-/OT-Sicherheit. Im Gegenzug kann die Demoanlage für eigene Untersuchungen genutzt werden. In diesem Rahmen sind einige studentische Arbeiten in Kooperation mit der IGR entstanden. In einer der Arbeiten wurde Kavitation als mögliches „Highest Consequence Event“ für einen zielgerichteten Angriff auf den Prozess gewählt. Dabei wurden Protokollschwächen im Prozessleitsystem identifiziert, die einen solchen Angriff ermöglichen. In einer anderen Arbeit wurden mehrere Softwareprodukte auf ihre Eignung untersucht, um Assets wie Hardware, Firmware und Software im industriellen Umfeld zu erkennen. Dabei konnte die Demoanlage gewinnbringend genutzt werden, um das im Rahmen der Arbeit erstellte Tool zu verifizieren.

In einer weiteren Arbeit wurde „Malcolm“, ein Open-Source-Projekt mit vielen Bestandteilen für das dynamische Erfassen von Assets, auf die Anwendbarkeit für den OT-Bereich evaluiert. Die Erkenntnisse dieser Arbeiten bieten zukünftig vielseitige Möglichkeiten, z. B. um zielgerichtete Angriffe auf den Prozess abzuwehren, dynamisches Erfassen von Assets in OT-Umgebungen zu ermöglichen oder ein Intrusion Detection System (IDS) mit den erhobenen Daten zu speisen.

PRAKTISCHE ZUSAMMENARBEIT IN DER PROZESSINDUSTRIE

Die Interessengemeinschaft Regelwerke Technik (IGR) e.V. wurde 2007 im Industriepark Höchst bei Frankfurt am Main gegründet und besteht heute aus mehr als dreißig Unternehmen und Dienstleistern aus der chemischen und pharmazeutischen Industrie. Die IGR ist selbst Mitglied in vielen nationalen und internationalen Gremien und Verbänden, wie beispielsweise International Electrotechnical Commission (IEC), International Organisation for Standardisation (ISO), Verband der Chemischen Industrie (VCI), Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE), Verband Deutscher Maschinen- und Anlagenbau (VDMA) und der Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V. (NAMUR). Der Arbeitskreis Industrie 4.0, in dem auch das BSI mitarbeitet, befasst sich thematisch mit der Umsetzbarkeit aus dem Blickwinkel der Automatisierung für sogenannte „Brownfield“-Anlagen. Dazu existiert eine Demoanlage Industrie 4.0 in den Laboratorien der Bilfinger Maintenance GmbH im Industriepark Höchst. ■

Die Erfolgsgeschichte geht weiter

Kriterienkatalog Cloud Computing (BSI C5) wird weiter verbessert

von Dr. Patrick Grete, Referat Virtualisierung und Cloud-Sicherheit

Sicheres Cloud Computing in einer digitalisierten Welt basiert auf wirksamen Sicherheitsmaßnahmen, die transparent und unabhängig geprüft Vertrauen schaffen. Der Kriterienkatalog C5 erfüllt diese Erwartungen: Bereits drei Jahre nach seiner Einführung hat sich ein Großteil der weltweit führenden Cloud-Anbieter die Einhaltung des BSI C5 nachweisen lassen.

Geboren wurde der „Kriterienkatalog Cloud Computing“ („Cloud Computing Compliance Criteria Catalogue“ - kurz BSI C5) aus dem Anliegen, Sicherheitsstandards und -nachweise zu entwickeln, die es dem öffentlichen Sektor (und insbesondere der Bundesverwaltung) ermöglichen, Cloud-Dienste zu nutzen. Dabei stellte das BSI fest, dass es einen formal nicht niedergelegten Konsens in der Cloud Community gab, welche Sicherheitseigenschaften ein Cloud-Dienst mindestens erfüllen muss. Der C5 bildet aus Sicht des BSI dieses Sicherheitsniveau ab.

Anfang 2016 veröffentlicht, gab es bereits Ende des Jahres den ersten Sicherheitsnachweis auf Basis des BSI C5. Weitere folgten rasch. Im Cloud-Monitor 2018 des BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien) und des Beratungsunternehmens KPMG wurde gefragt, inwieweit der BSI C5 bei der Auswahl eines Cloud-Anbieters relevant ist. In zwei Drittel der Antworten spielte der C5 eine Rolle, manchmal sogar als ein Muss-Kriterium. Dies spiegelt wider, dass neben dem öffentlichen Sektor auch Bereiche der Wirtschaft auf den BSI C5 setzen. Offensichtlich deckt er eine Nachfrage ab, die andere internationale Standards so nicht erfüllen konnten.

WAS IST DER BSI C5?

Der BSI C5 ist ein Prüfkatalog für Cloud-Dienste, bestehend aus Sicherheitskriterien, Transparenzinformationen und Hinweisen, wie deren Einhaltung in einem bestehenden Prüfverfahren nachgewiesen werden kann. Die Sicherheitskriterien stimmen in vielen Aspekten mit anderen international etablierten Standards überein, wie der ISO/IEC 27001. Im BSI C5 sind diese Kriterien für Cloud-Anbieter geschärft und decken weitere Bereiche ab. Insgesamt hat der BSI C5 über 120 solcher Sicherheitskriterien, die in 17 Abschnitten thematisch gegliedert sind.

Sicherheitsnachweise schaffen immer dann Vertrauen, wenn ein sachverständiger Dritter die Abdeckung von Sicherheitskriterien überprüft. Der BSI C5 bedient sich für das Audit und den Report der Normen, die für Wirtschaftsprüfer gelten. Dies sind die international etablierten Standards

ISAE 3000 und ISAE 3402 (ISAE - International Standard on Assurance Engagements). Aber auch hier ergänzt der BSI C5 noch einige Aspekte, indem er zusätzliche Kriterien stellt, wie z. B. an die Qualifikation des Auditteams. Die Kombination von Kriterien aus etablierten Sicherheitsstandards mit den Nachweismethoden der Wirtschaftsprüfer, eingeführt und begleitet durch als BSI als neutrale und weltweit anerkannte Cybersicherheitsbehörde des Bundes, macht den BSI C5 einzigartig und bildet die Grundlage für seinen Erfolg.

BSI C5:2020

Die schnell fortschreitende Entwicklung der Technik erforderte 2019, den BSI C5 zu überarbeiten und wo nötig anzupassen. Dafür bat das BSI viele Personen und Institutionen, sich intensiv mit dem BSI C5 auseinanderzusetzen und neue Ideen und Verbesserungsvorschläge zu formulieren. Hinzu kamen über drei Jahre Erfahrung mit dem C5 in Beratung, Anwendung und Prüfung. Nicht unerwähnt bleiben soll der EU Cybersecurity Act, der inzwischen verbindliche Anforderungen an EU-weite Zertifizierungsschemata stellt. Diese Erfahrungen und Vorgaben führten zu einigen Neuerungen im BSI C5.
Bei den Sicherheitskriterien kamen zwei neue Bereiche hinzu, andere wurden um wichtige Aspekte ergänzt:

- Der Bereich Produktsicherheit fokussiert auf die Sicherheit des Cloud-Dienstes selbst und nicht, wie der Rest des C5, auf dessen Erbringung. Diese Anforderungen decken Vorgaben aus dem EU Cybersecurity Act ab.
- Mit einem weiteren neuen Bereich, bei dem der Cloud-Anbieter seinen „Umgang mit staatlichen Ermittlungsbeschlüssen" nach einem ordentlichen Prozess aufbauen muss, wird die gerade im Cloud Computing oft gestellte Frage nach den Zugriffsmöglichkeiten staatlicher Stellen adressiert. Das BSI beabsichtigt hiermit, die Debatte zu versachlichen.
- Die Steuerung von Subdienstleistern, die im Cloud Computing zahlreich tätig sind, wurde nunmehr klarer geregelt. Das Thema DevOps – also die enge Verknüpfung von Entwicklung und Betrieb – findet nun ausreichend Niederschlag.

Auch die Anforderungen an den Sicherheitsnachweis wurden überarbeitet. Die C5-Reports müssen nun einem formalen Aufbau folgen, was das Lesen und Vergleichen erleichtert. Beim Audit ist nun auch die Methode des Direct Testings möglich, die es (kleineren) Cloud-Anbietern ohne ausgereiftes internes Kontrollsystem ermöglicht, ein C5-Testat zu erreichen. Auch Cloud-Anbieter, die ihre Dienste ohne eine eigene Infrastruktur als „Software as a Service" (SaaS) anbieten, können leichter ein C5-Testat erhalten, indem sie effizient auf die Sicherheitsnachweise ihres Infrastrukturanbieters aufbauen.

DIE ENTWICKLUNG GEHT WEITER

Kontinuierliche Auditierung, also die Prüfung durch automatisiert abrufbare Sicherheitsnachweise, ist ein sehr aktuelles Thema. Im BSI C5 sind mit der Überarbeitung jetzt die Grundlagen hierfür gelegt: Zu jedem hierfür geeigneten Kriterium gibt es neue Hinweise, ob und ggf. wie es bei einer kontinuierlichen Auditierung geprüft werden kann.

Im Cloud Computing ist die Schnittstelle zwischen Cloud-Anbieter und Cloud-Kunde sehr kritisch. Zum einen muss sie klar definiert sein, um Sicherheit zu gewährleisten, und zum anderen müssen Anbieter und Kunde die jeweiligen eigenen Anforderungen erfüllen. Mit den sog. korrespondierenden Kriterien wird dem Cloud-Kunden aufgezeigt, wie er aus einer bestehenden C5-Attestierung seines Cloud-Anbieters den größten Nutzen ziehen kann. Gleichzeitig bekommt der Cloud-Anbieter damit Hinweise, welche Fragen zur Sicherheit des Angebots seine (potenziellen) Kunden stellen werden. ■

Weiterführende Links:

https://www.bsi.bund.de/c5

DIGITALE GESELLSCHAFT

5G-Campus-Netzwerk bei BASF

Am Start für das Chemiewerk der Zukunft

von Harald Endres, Martin Schwibach und Volker Wagner, BASF

BASF hat vor Kurzem den Zuschlag für eigene 5G-Frequenzen erhalten und kann damit als eines der ersten Unternehmen in Deutschland ein firmeneigenes 5G-Netzwerk für industrielle Anwendungen aufbauen. Dabei ist Netzwerksicherheit für die digitale Transformation von größter Bedeutung.

BASF und auch die gesamte Chemiebranche befinden sich mitten im Prozess der digitalen Transformation. Ein wesentlicher Baustein ist der Aufbau und Betrieb eines eigenen 5G-Campus-Netzwerkes. Im Gegensatz zu den bisherigen Mobilfunknetzwerken zielt 5G vor allem auch auf industrielle Anwendungen. Selbstfahrende Fahrzeuge, autonome Roboter sowie vollständig automatisierte Produktionsprozesse werden digitale Wertschöpfungsketten ermöglichen. 5G unterstützt dabei die Kommunikation mit höchster Bandbreite, garantierter Zuverlässigkeit und minimalen Antwortzeiten. Mit 5G bricht für BASF ein neuer Abschnitt im digitalen Zeitalter an.

STARTSCHUSS FÜR DEN AUFBAU EINES EIGENEN 5G-NETZWERKS

BASF war bei der Bundesnetzagentur gemeinsam mit den Verbänden, wie dem Verband der Chemischen Industrie (VCI), dem Zentralverband Elektrotechnik und Elektronikindustrie (ZVEI) und dem Verband Deutscher Maschinen- und Anlagenbau (VDMA), einer der Treiber dafür, dass ein Viertel der verfügbaren 5G-Frequenzen für industrielle Anwendungen bereitgestellt werden. Ende November erhielt BASF als eines der ersten deutschen Unternehmen die Genehmigung für ein lokales 5G-Netz am Standort Ludwigshafen. Nach der Frequenzvergabe beginnt BASF nun mit den Vorbereitungen für den Aufbau der notwendigen Infrastruktur. Wie diese zukünftig genau auszusehen hat, wird in den kommenden Monaten im Rahmen eines Pilotprojektes erarbeitet.

EINSATZMÖGLICHKEITEN VON 5G

Beispiele für den Einsatz von 5G sind Assistenzsysteme für mobiles Arbeiten, der Einsatz von Drohnen oder Remote-Operation-Systemen – das heißt Systemen für Fernzugriff und -bedienung. Dies verspricht vor allem für die Instandhaltung der Anlagen und Maschinen einen großen Nutzen. Schon heute werden dazu Tablets oder auch Datenbrillen genutzt. Auch für den Betrieb von selbstfahrenden Schwerlast-Fahrzeugen auf dem BASF-Gelände in Ludwigshafen wird 5G benötigt. Hier ist der Einsatz von bis zu zwanzig dieser Fahrzeuge geplant. Um die Sicherheit zu gewährleisten, werden sie über eine zentrale Leitstelle überwacht. Dazu müssen viele Daten wie beispielsweise Videobilder in Echtzeit übertragen werden.

NETZWERKSICHERHEIT IST FÜR DIE DIGITALE TRANSFORMATION VON GRÖSSTER BEDEUTUNG

Cyber-Sicherheit bekommt mit dem weiteren Ausbau automatisierter Produktionsprozesse eine besondere Relevanz. Bei der Vernetzung industrieller Anwendungen werden IT-Systeme der Produktion nach dem Grundsatz der Segregation oft isoliert von Standard IT-Netzwerken und dem Internet gebaut und betrieben. Mit dem eigenständigen - von öffentlichen Mobilfunknetzwerken unabhängigen - Frequenzbereich für industrielle 5G-Netzwerke hat die Bundesnetzagentur den Rahmen dafür geschaffen, auch bei 5G-Netzwerken die etablierten Cyber-Sicherheitsmaßnahmen umzusetzen. Während der Schutz vertraulicher Daten wichtig für Unternehmen ist, um den Abfluss von Geschäftsgeheimnissen zu vermeiden, haben die Verfügbarkeit und Integrität von Daten eine herausragende Stellung beim Betrieb automatisierter Produktionsanlagen.

CHEMIE – EINE BRANCHE MIT AUSGEPRÄGTEM RISIKOBEWUSSTSEIN

Gerade im Rahmen ihrer Produktionsprozesse können Unternehmen aus der chemischen Industrie auf ein ausgeprägtes Risikobewusstsein zurückgreifen und haben umfassende Maßnahmen zur Produkt- und Anlagensicherheit implementiert. Nicht nur die umfangreichen, geltenden rechtlichen Rahmenbedingungen, sondern auch unsere Responsible-Care-Leitlinien sind Grundlage unseres Bewusstseins der gesellschaftlichen Verantwortung für Produkt- und Arbeitssicherheit in zunehmend digital gestützten Produktionsprozessen. BASF nimmt die zunehmende Professionalisierung von Cyber-Angriffen sehr ernst.

Wir arbeiten deshalb mit diversen Partnern zusammen und haben ein enges, weltweit geknüpftes Netz an Experten aus Cyber-Sicherheitsfirmen, staatlichen Einrichtungen und Hochschulen sowie anderen Industrieunternehmen, um sicherzustellen, dass wir uns im Rahmen des Möglichen gegen denkbare Attacken verteidigen können.

DIE NÄCHSTEN SCHRITTE

Derzeit finden Gespräche mit unterschiedlichen Lieferanten und Mobilfunkbetreibern statt, mit denen BASF das 5G-Netz für Produktionsanlagen und Logistik aufbauen wird. Ein zentrales Thema ist die Funktionalität und die Verfügbarkeit der 5G-fähigen Geräte, die derzeit noch nicht auf dem Markt zur Verfügung stehen. Dazu zählen beispielsweise Themen wie Zuverlässigkeit und Sicherheit. Die 5G-Geräte müssen industrietauglich sein und beispielsweise in explosionsgefährdeten Bereichen zum Einsatz kommen können. Security by Design ist für BASF daher nicht nur ein Schlagwort, sondern ein Paradigma. ■

Harald Endres

Harald Endres, Vice President Cyber-Security und CISO für die BASF Gruppe. Dies beinhaltet die IT- und OT-Cyber-Sicherheit, Informationsschutz, Risikomanagement, Security Architektur und Awareness.

Martin Schwibach

Martin Schwibach, Director Industrial Connectivity und Industrial Mobility, verantwortet die technologische Entwicklung und den Betrieb von digitalen Lösungen wie 5G im Produktionsumfeld der BASF.

Volker Wagner

Volker Wagner ist Vice President Group Security bei der BASF SE. Sein beruflicher Schwerpunkt liegt auf der Entwicklung und Umsetzung von Sicherheitsstrategien.

Cyber-Sicherheit für die Digitalisierung der Energiewirtschaft

Rollout intelligenter Messsysteme beginnt

von Stefan Vollmer, Andy Neidert und Michael Brehm, Referat Cyber-Sicherheit für die Digitalisierung der Energiewirtschaft

Das BSI hat die technische Möglichkeit zum Einbau intelligenter Messsysteme festgestellt und damit die Freigabe für deren Rollout erteilt. Damit wird ein wichtiger Meilenstein für die Digitalisierung der Energiewende erreicht. Denn mit dem Einbau von intelligenten Messsystemen wird ein wesentlicher Beitrag geleistet, um die Klimaschutz- und Energiewendeziele erreichen zu können. Gemeinsam mit den Unternehmen der Energiebranche werden BSI und BMWi diesen Rollout voranbringen und zusätzlich technische Eckpunkte für weitere Bausteine des intelligenten Energienetzes der Zukunft bestimmen.

Um die Klimaschutz- und Energiewendeziele erreichen zu können, muss das Energieversorgungssystem digitalisiert werden. Die damit verbundenen Herausforderungen an das intelligente Energienetz der Zukunft sind enorm. Anstelle von wenigen Großkraftwerken soll eine Vielzahl von kleinen, dezentralen Erzeugungsanlagen und flexiblen Verbrauchseinrichtungen in das intelligente Energienetz integriert werden. Weiterhin werden auch auf Verbraucherseite durch den Hochlauf der Elektromobilität sowie die Wärmewende steuerbare und flexible Kundeneinrichtungen entstehen. Flexibilität im zukünftigen Smart Grid ist nötig, um Erzeugung und Verbrauch aufeinander abzustimmen.

DAS INTELLIGENTE MESSSYSTEM: EIN WICHTIGER BAUSTEIN FÜR DIE ENERGIEWENDE

Um diese Ziele erfolgreich umsetzen zu können, muss das Verteilnetz auf Basis intelligenter Messsysteme (iMSys) stufenweise digitalisiert werden. Denn durch die Verwendung von iMSys – und der damit einhergehenden Verwendung von zertifizierten Smart Meter Gateways - werden zukünftig wichtige Systeme des Energienetzes über eine sichere Kommunikationsinfrastruktur vernetzt. Zugleich wird Cyber-Angriffen auf solche Systeme wirksam begegnet. Durch den Einsatz von iMSys können Netzzustandsdaten erhoben werden, sodass die Transparenz über die Leistungsflüsse im Verteilnetz entsteht. Zudem können flexible Verbrauchseinrichtungen (Wärmepumpen, Elektromobile usw.) und dezentrale Erzeugungsanlagen zukünftig über das iMSys gesteuert und somit netz- und marktdienlich eingesetzt werden.

Nur wenn die dezentralen Erzeugungs- und Verbrauchsanlagen über das iMSys gesteuert werden, kann der Anteil erneuerbarer Energien in den Netzen weiter erhöht und beispielsweise die für die Elektromobilität notwendige Ladeinfrastruktur ohne einen umfangreichen und kostenintensiven Netzausbau integriert werden.

MARKTANALYSE UND FESTSTELLUNG DER TECHNISCHEN MÖGLICHKEIT

Damit der Rollout intelligenter Messsysteme in Deutschland beginnen kann und die Marktakteure ihre Pflichten nach dem Messstellenbetriebsgesetz (MsbG) erfüllen können, steht die stufenweise Einführung von iMSys unter dem Vorbehalt der sogenannten Feststellung der technischen

Möglichkeit. Sie wird durch das BSI auf Basis einer Marktanalyse nach § 30 MsbG getroffen.

Seit Ende letzten Jahres stehen drei zertifizierte SMGWs (Power Plus Communications GmbH, Sagemcom Dr. Neuhaus GmbH & Co KG, EMH metering GmbH) zur Verfügung und können zusammen mit einer modernen Messeinrichtung als intelligentes Messsystem eingesetzt werden.

Mit der Aktualisierung der Marktanalyse und der Veröffentlichung der Feststellung der technischen Möglichkeit zum Einbau intelligenter Messsysteme am 31. Januar 2020 hat das BSI den Startschuss für den Beginn des gesetzlich verpflichtenden Rollouts gegeben. Zunächst müssen Messstellenbetreiber die etwa vier Millionen Stromkunden mit einem intelligenten Messsystem ausstatten, die einen Jahresstromverbrauch zwischen 6.000 kWh und 100.000 kWh haben. Dafür haben die Messstellenbetreiber nach Feststellung der technischen Möglichkeit insgesamt acht Jahre Zeit. Mindestens zehn Prozent dieser Pflichteinbaufälle müssen jedoch innerhalb der ersten drei Jahre mit einem intelligenten Messsystem ausgestattet werden.

UNTERSTÜTZUNG DES ROLLOUTS - ERWEITERUNG DER EINSATZBEREICHE DES IMSYS

Um die SMGW-Kommunikationsplattform für das zukünftige Smart Grid weiterzuentwickeln, sind die folgenden vier zentralen Fragestellungen zu berücksichtigen:

- Wie kann eine effiziente und sichere Systemintegration (Netz und Markt) von dezentralen Erzeugungsanlagen (PV, Biogas, Windkraft) sowie flexiblen Verbrauchseinrichtungen (Ladeinfrastruktur, Wärmepumpen, Nachtspeicherheizungen, Heimspeicher) ermöglicht werden?
- Wie können Ladevorgänge an privaten, halböffentlichen und öffentlichen Ladeinrichtungen sicher authentifiziert, gemessen und abgerechnet werden?
- Wie kann eine sichere Systemintegration (Netz und Markt) auch für bidirektionales Laden ermöglicht werden?
- Wie können spartenübergreifende Messungen und Abrechnungen dynamischer Tarife und komplexer Lieferprodukte (Mieterstrom etc.) sowie Mehrwertdienste im Bereich Submetering (Heizkostenverteiler, Sensoren, Aktoren) ermöglicht werden?

Hierzu hat das BSI ein Projekt zur „Produkt- und Systemarchitektur-Analyse für die fortschreitende Digitalisierung des intelligenten Netzes der Energiewende“ gestartet. Es soll weitere Einsatzbereiche des iMSys analysieren und technische Eckpunkte ermitteln. Darin werden die System- und Kommunikationsarchitekturen beschrieben und Anforderungen an die grundlegenden Sicherheitsfunktionen der Komponenten gestellt. Im Anschluss wird der Anpassungsumfang hinsichtlich der aktuellen BSI-Standards in Form von Technischen Richtlinien und Schutzprofilen bestimmt. Um eine aktive Einbeziehung der Energiebranche zu gewährleisten, werden verschiedene Dialogplattformen (Umfragen, Task Forces und Arbeitsgemeinschaften) durch das Projekt durchgeführt (vgl. BSI-Magazin 2019-02).

Mit der Veröffentlichung der technischen Eckpunkte wird somit die Basis für die Weiterentwicklung der BSI-Standards geschaffen, um für ein sicheres, intelligentes Energienetz der Zukunft wichtige Standards zielführend festzulegen. ■

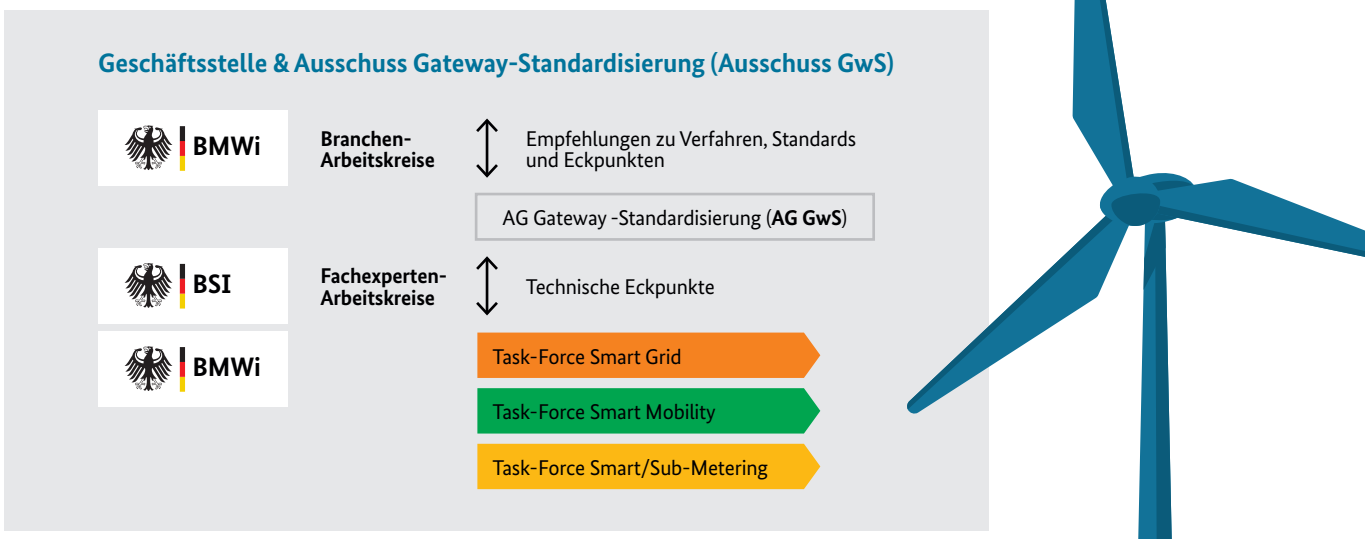


Abbildung 1: Dialogplattformen für die Standardisierung der SMGW-Kommunikationsplattform. Mit der Veröffentlichung der technischen Eckpunkte wird somit die Basis für die Weiterentwicklung der BSI-Standards geschaffen, um für ein sicheres, intelligentes Energienetz der Zukunft wichtige Standards zielführend festzulegen.

„Verbraucher sind auf eine sichere IT angewiesen“

Interview mit Wolfgang Schuldzinski, Vorstand der Verbraucherzentrale NRW

Im Verfahren der VZ NRW gegen MediaMarkt bezüglich des Verkaufs von Smartphones mit Sicherheitslücken hat das OLG Köln die Berufung gegen das Urteil des LG Köln zurückgewiesen. Was bedeutet dies für die Informationssicherheit der Verbraucherinnen und Verbraucher?

Mit dem Verfahren wollten wir erreichen, dass Verbraucherinnen und Verbraucher zum Zeitpunkt des Kaufs eines Smartphones im Geschäft darüber informiert werden, ob das Betriebssystem des Geräts Sicherheitslücken aufweist und ob für dieses noch Sicherheitsupdates zur Verfügung gestellt werden. Leider verneint das Gericht eine solche Informationspflicht der Händler u.a. weil die Beschaffung der Informationen beim Hersteller für den Händler zu aufwendig sei. Nach EU-Recht werden Händler ab 2022 zwar verpflichtet sein, für Smartphones und andere smarte Geräte Sicherheitsupdates für einen bestimmten Zeitraum zur Verfügung zu stellen. Bis dahin bleiben die Verbraucherinnen und Verbraucher aber weitgehend schutzlos, da sie meist nicht in der Lage sind, den Sicherheitsstand eines Geräts zu bewerten. Sie laufen somit vorerst weiterhin Gefahr, ein bereits mit Sicherheitslücken behaftetes Gerät zu erwerben und mit diesen Lücken mangels Updates leben zu müssen.

Wie bewerten Sie das vergangene Jahr 2019 aus Sicht eines Verbraucherschützers?

Das letzte Jahr hat wieder einmal deutlich gemacht, dass IT-Sicherheit und Datenschutz für Verbraucherinnen und Verbraucher von enormer Bedeutung sind. Je mehr die Digitalisierung den Verbraucheralltag durchdringt, desto größer werden die Angriffsmöglichkeiten. Ich verkenne nicht, dass Verbraucherinnen und Verbraucher teilweise allzu sorglos agieren und auch sie ihren Beitrag zur IT-Sicherheit leisten müssen. Fehlt es aber bei Soft- und Hardware bereits an der IT-Sicherheit, haben Verbraucherinnen und Verbraucher keine Chance, sich gegen Hackerangriffe oder andere kriminelle Maßnahmen zu wehren. Verbraucherinnen und Verbraucher sind auf eine funktionierende und vor allem sichere IT angewiesen. Sie müssen der eingesetzten Technik vertrauen dürfen.

Dies betrifft besonders auch die Smart-Home-Produkte, die im Verbraucheralltag heute schon gegenwärtig sind. Wird dieses Vertrauen durch sichere Technik nicht aufgebaut oder mit unsicherer Technik wieder verspielt, hat dies unmittelbaren Einfluss auf die Akzeptanz digitaler Geschäftsmodelle. Viele Unternehmen haben sich im letzten Jahr bereits besser aufgestellt, aber die zahlreichen Datenskandale des Jahres 2019 zeigen, dass hier noch viel Luft nach oben ist.

Welche besonderen Herausforderungen sehen Sie für 2020?

Eine der größten Herausforderungen liegt im Einsatz Künstlicher Intelligenz. Fragen der Ethik, der Fairness von Algorithmen und auch ungeklärte Haftungsfragen fordern einen verantwortungsvollen Umgang mit der KI. Aber Verantwortung ohne eine Instanz, vor der man sich rechtfertigen muss, ist wohlfeil. Relevante algorithmenbasierte Entscheidungsprozesse sollten daher durch ein unabhängiges, staatlich legitimiertes Kontrollsystem überwacht werden. Dies sollte 2020 auf den Weg gebracht werden.

Was erwartet Verbraucherinnen und Verbraucher im kommenden Jahr?

Viele Menschen sind unsicher im Umgang mit dem Internet, weil ihnen die notwendigen digitalen Kompetenzen fehlen. Die Verbraucherzentrale NRW wird daher auch im nächsten Jahr durch Vorträge in Schulen, bei Initiativen und in ihren Beratungsstellen Verbraucherinnen und Verbraucher für den Schutz der Privatsphäre sensibilisieren und ihnen Instrumente zur digitalen Selbstverteidigung an die Hand geben. Kompetenz genügt aber nicht, wenn bei elektronischen Produkten nicht erkennbar ist, ob sie nach dem Stand der Technik sicher sind oder wie lange sie gepatcht werden. Diese Informationen sind aber für gute und informierte Kaufentscheidungen wichtig. Wir benötigen daher aussagekräftige Sicherheitskennzeichnungen am Produkt, aber auch weitere Sicherheitsstandards für verbraucherrelevante Produktgruppen als Basis für zuverlässige Sicherheitskennzeichnungen.

„Eine der größten Herausforderungen liegt im Einsatz Künstlicher Intelligenz."

verbraucherzentrale
Nordrhein-Westfalen

Kurzprofil Wolfgang Schuldzinski

Geboren 1960 in Düsseldorf studierte Wolfgang Schuldzinski Rechtswissenschaften an den Universitäten zu Köln und Tübingen. Nach dem zweiten juristischen Staatsexamen begann er 1995 seine Tätigkeit bei der Verbraucherzentrale Nordrhein-Westfalen. Von 2008 bis 2014 leitete er hier als Mitglied der Geschäftsleitung den Bereich Markt und Recht. Im Juli 2014 übernahm er die Position des Vorstands und legt seitdem einen besonderen Schwerpunkt auf Verbraucherschutz bei digitalen Themen. Wolfgang Schuldzinski ist unter anderem Vorsitzender des Arbeitskreises der Verbraucherzentralen aller Bundesländer sowie Mitglied im Verwaltungsrat des Verbraucherzentrale Bundesverbandes, des Kuratoriums der Stiftung Warentest und im WDR-Rundfunkrat.

Wie sieht die künftige Zusammenarbeit der Verbraucherzentrale NRW mit dem BSI aus?

Grundlage unserer Zusammenarbeit ist das gemeinsame Ziel, die Informationssicherheit für Verbraucherinnen und Verbraucher zu stärken, ihnen beim Umgang mit Missbräuchen zur Seite zu stehen und Internetsabotage wirksam zu bekämpfen. Dies werden wir auch 2020 durch Zusammenarbeit bei der Veröffentlichung von sicherheitsrelevanten Verbraucherinformationen in den Kanälen des BSI und der Verbraucherzentrale fortführen. Wir vertrauen bei unseren Verbandsklageverfahren weiterhin gerne auf den technischen Sachverstand des BSI. Wir sind zudem Teil der Allianz für Cyber-Sicherheit und werden auch weiterhin beim Schutz vor Phishing-Mails mit unserem „Phishing-Radar" eng mit dem BSI kooperieren.

HINTERGRUND: URTEIL DES OLG KÖLN

Das Oberlandesgericht Köln hat im Oktober 2019 entschieden, dass Händler beim Verkauf von Smartphones nicht über etwaige Sicherheitslücken des Betriebssystems, noch über das Fehlen von Sicherheitsupdates für die Software aufklären müssen. Anlass der Klage der Verbraucherzentrale NRW war ein im Jahr 2016 durch Media Markt verkauftes Smartphone des Typs Mobistel Cynus T6 8 GB mit dem Betriebssystem „Android 4.4.2 Kitkat", welches nach technischer Prüfung des BSI mehrere Sicherheitslücken im Betriebssystem aufwies, womit die Nutzung ein Sicherheitsrisiko für die Verbraucherinnen und Verbraucher darstellte. Der Händler hat zum Zeitpunkt des Verkaufs weder auf die Sicherheitslücken, noch auf die nicht zu Verfügung stehenden Sicherheitsupdates hingewiesen.

„Mein Leben ist passwortgebunden“

Projekt untersucht wirksame Schutzmaßnahmen für Online-Accounts

von Ines Schieferdecker und Hanna Heuer, Referat Cyber-Sicherheit für den Bürger

Starke Passwörter, Zwei-Faktor-Authentisierung, Passwortmanager - obwohl solche technischen Schutz- und Hilfsmaßnahmen vorhanden sind, werden Online-Accounts immer wieder kompromittiert. Dies lässt eine Diskrepanz zwischen dem verfügbaren Wissen zum Schutz von Online-Accounts und dem tatsächlichen Sicherheitsverhalten der Anwenderinnen und Anwender vermuten. Ihre Bedürfnisse, Ängste und Herausforderungen rund um das Thema Account-Schutz zu verstehen und darauf basierend wirksame Informationsmaterialien und Hilfestellungen zu entwickeln, ist Ziel eines gemeinsamen Projektes des Bundeskanzleramts und des BSI.

Welche pVoraussetzungen müssen erfüllt sein, damit der Einzelne Wissen in Handeln umsetzt? Menschen beginnen dann eine Handlung, wenn sie davon überzeugt sind, dass sie die Herausforderung aus eigener Kraft erfolgreich bewältigen können. Diese Selbstwirksamkeitserwartung mit Bezug auf den sicheren Umgang mit Online-Accounts zu fördern, steht im Mittelpunkt des Projektes. Zentrale Fragestellungen sind u. a., wie man Bürgerinnen und Bürger vor dem Hintergrund ihres Wissens, ihrer konkreten Lebenssituation und ihrer Handlungsziele dazu befähigen kann, ihre Online-Accounts besser zu schützen, worin Hindernisse liegen, wie ihre Risikowahrnehmung ausgeprägt ist und ob Empfehlungen so verständlich dargestellt sind, dass das eigene Handeln zur Sicherheit der genutzten Online-Accounts beiträgt.

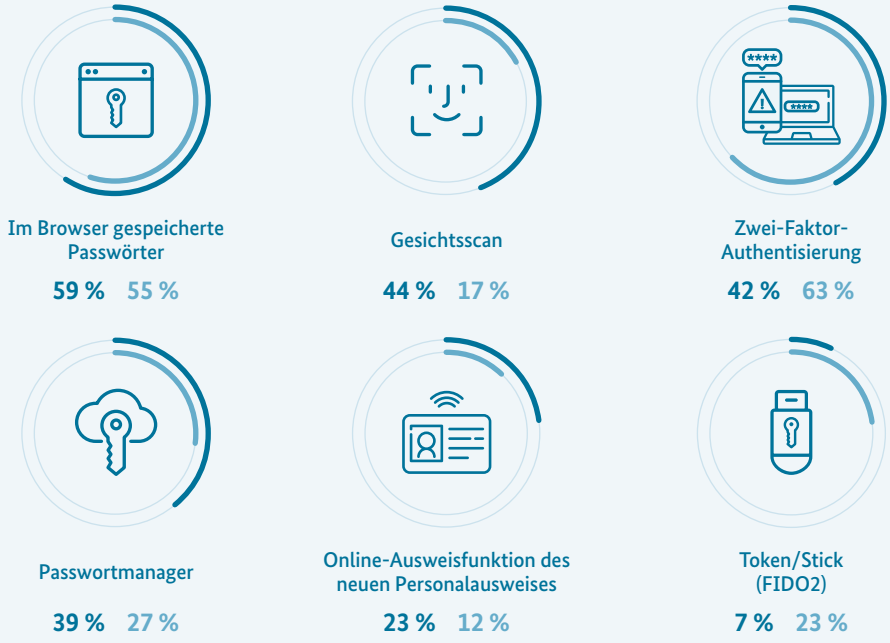
„WENN HACKER EINEN ACCOUNT KNACKEN WOLLEN, SCHAFFEN DIE DAS.“

Diese Interviewaussage spiegelt wider, was viele Internetnutzer und -nutzerinnen empfinden, wenn sie an den Schutz ihrer E-Mail-, Social Media- oder Onlineshopping-Accounts denken: Sie sehen sich (gezwungenermaßen) einer immer komplexer werdenden Technik ausgesetzt, glauben eher nicht, dass sie sich vor Hackern und Cyber-Kriminellen wirkungsvoll durch z. B. Passwörter schützen können oder dass sie persönlich ein Ziel von Hackern sind und erleben Accountschutz als Hindernis im Alltag. Gleichzeitig fehlt Wissen, z. B. ab wann ein Passwort als relativ sicher gilt. Aus zehn Gruppendiskussionen mit insgesamt 100 Teilnehmern, aufgeteilt nach fünf Altersgruppen und Geschlecht, konnten in der ersten Projektphase diese und weitere Erkenntnisse zum Umgang mit Passwörtern, zu Handlungsbarrieren und der Risikowahrnehmung gewonnen werden. Diese flossen in den Fragebogen einer repräsentativen Online-Befragung ein.

„ICH HABE MEHR ALS FÜNFZIG ACCOUNTS. WIE SOLL ICH MIR DA ALLE PASSWÖRTER MERKEN?“

Gerade die Menge an Passwörtern, die in verschiedenen Kontexten, ob zuhause oder unterwegs, abrufbar sein müssen, stellt für die Befragten eine Herausforderung dar. Knapp vier Fünftel der Befragten (78 %) nutzen bis zu 20 Online-Accounts, die mit einem Passwort geschützt werden müssen. Dem begegnen drei Viertel der Befragten (74 %) mit dem Ansatz, sich Passwörter selber zu merken. Rund ein Drittel (34 %) notiert sich Passwörter auf Papier, 15 % speichern sie in einem Passwortmanager (Mehrfachnennungen waren möglich). Nutzerinnen und Nutzer tendieren dazu, ihre Online-Konten nicht optimal zu schützen, obwohl sie es nach eigener Aussage besser könnten.

Welche der folgenden Möglichkeiten kennen Sie, um sich bei einem Online-Konto anzumelden?* Und welche davon nutzen Sie tatsächlich? Auswahl der Ergebnisse, Mehrfachnennungen möglich:



* n = 995, 16 Jahre und älter, Durchführungszeitraum 26.10. bis 3.11.2019

Aufgrund der Vielzahl der genutzten Online-Konten, erleben sie sich in einer Situation der kognitiven Überforderung. Diese besteht in der begrenzten Merkfähigkeit. Neben Zeit und Aufwand wird die Generierung eines sicheren Passwortes nicht als Hauptbarriere gesehen, sondern die Anforderung, eine hohe Anzahl an Accounts zu managen.

„ICH BIN MISSTRAUISCH GEGENÜBER PASSWORTMANAGERN."

Von den 39 Prozent der Befragten, die Passwortmanager kennen, nutzt nur knapp ein Drittel (27 %) derartige technische Hilfsmittel, um starke Passwörter zu erstellen und sich bei Online-Accounts anzumelden. Hauptgrund für die Nichtnutzung solcher Software sind Vorbehalte (67 %). Besonders stark wiegt dabei die Sorge, dass ein Hacker mit einem Schlag an alle verwendeten Passwörter gelangen könnte (78 %), Skepsis gegenüber der Seriosität der Anbieter solcher Programme ist ebenfalls verbreitet (58 %, Mehrfachnennungen möglich).

Insgesamt besteht Verwirrung, was technische Hilfsmittel (z. B. Passwortmanager) und einzelne Sicherheitsverfahren (TAN, Code etc.) leisten können und was die dafür verwendeten Begriffe genau bedeuten. Mehr Information wünschen sich die Befragten vornehmlich in Form von praktischen Tipps, wie man bei sehr vielen Konten sicher seine Passwörter handhabt und Empfehlungen, welche Software für den Schutz von Online-Konten geeignet ist. Dabei wird dem Staat eine besondere Verantwortung zugeschrieben.

MASSNAHMEN ENTWICKELN UND TESTEN

Auf Grundlage dieser und weiterer Erkenntnisse erarbeitet das Projektteam derzeit gemeinsam mit Fachkolleginnen und -kollegen aus dem BSI Informationsmaterial und Hilfestellungen für Bürgerinnen und Bürger. In einer weiteren Projektphase wird im Feld – also unter realistischen Anwendungsbedingungen – getestet, inwiefern diese Materialien helfen, IT-Sicherheitskompetenz zu fördern sowie Einstellungen und Verhalten positiv zu beeinflussen, so dass Online-Accounts besser geschützt werden. Hierzu läuft derzeit die Akquise externer Partner. ■

Weiterführende Links:

https://www.bundesregierung.de/breg-de/themen/wirksam-regieren/schutz-von-online-konten-1732360

BSI-Basistipp

Checklisten für den Ernstfall

Schritt-für-Schritt-Hilfe der Polizeilichen Kriminalprävention und des BSI

28 Prozent der von Kriminalität im Internet Betroffenen gaben 2019 an, dass sie Opfer von Phishing geworden sind. Das ergab die Umfrage „Digitalbarometer 2019“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK). Bei Phishing-Angriffen stehen neben Bankkunden insbesondere auch Kunden von Online-Händlern oder Bezahlsystemen im Fokus. Da sich mit den abgegriffenen Daten Einkäufe und Zahlungen tätigen lassen, ist es wichtig, dass Betroffenen schrittweise und verständlich vermittelt wird, was in einem solchen Ernstfall zu tun ist.

Ziel und Handlungsversprechen des Digitalbarometers war, die gemeinsame Aufklärungsarbeit von ProPK und BSI zu stärken und dabei die Ergebnisse der Befragung zu berücksichtigen. Vor diesem Hintergrund haben die Partner eine gemeinsame Checklistenreihe aufgelegt, mit der sie sich gezielt an die Opfer von Kriminalität im Internet wenden. Die erste Ausgabe gibt Phishing-Opfern erste Notfallmaßnahmen an die Hand und listet Schritt für Schritt auf, was sie tun sollten, wenn ihre Daten abgegriffen wurden. Im Zentrum steht die Frage: Was sollte ich also tun, wenn Kriminelle meine sensiblen Daten abgegriffen haben?

Eine zweite Anleitung befasst sich mit Reaktionen auf Betrug beim Onlinebanking. Weitere Checklisten, die Opfern von Kriminalität im Internet als Hilfe zur Selbsthilfe dienen können, werden von den Partnern gemeinsam erarbeitet und veröffentlicht.

Checkliste für den Phishing-Fall

Das sollten sie tun, wenn …

… Sie Zahlungsdaten weitergegeben haben:

- Sperren Sie Ihr Bankkonto.
- Kontrollieren Sie die Umsätze Ihres Bankkontos und setzen Sie sich mit Ihrer Bank in Verbindung.
- Nutzen Sie nach der Entsperrung ausschließlich neue Passwörter als PINs für Ihr Konto.

… Sie Zugangsdaten zu anderen Konten, z. B. Online-Shops, weitergegeben haben:

- Vergeben Sie ein neues Passwort.
- Nehmen Sie Kontakt mit dem Anbieter auf.
- Überprüfen Sie zudem, ob Zahlungsdaten betroffen waren und nehmen Sie dementsprechend auch Kontakt mit Ihrer Bank auf.

Weiterführende Links:

https://www.bsi-fuer-buerger.de/phishing-checkliste

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 personenbezogenen 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. die 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 | www.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: https://www.bsi.bund.de/datenschutzrechtliche-hinweise

IMPRESSUM

Herausgeber:	Bundesamt für Sicherheit in der Informationstechnik (BSI) 53175 Bonn
Bezugsquelle:	Bundesamt für Sicherheit in der Informationstechnik (BSI) Referat WG24 – 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:	März 2020
Texte und Redaktion:	Nora Basting und Mark Schulz, Bundesamt für Sicherheit in der Informationstechnik (BSI); FAKTOR 3 AG
Konzept und Gestaltung:	FAKTOR 3 AG Kattunbleiche 35 22041 Hamburg www.faktor3.de
Druck:	Appel und Klinger Druck & Medien GmbH Bahnhofstraße 3 96277 Schneckenlohe Internet: www.ak-druck-medien.de
Artikelnummer:	BSI-Mag 20/711-1
Bildnachweise:	Titel: GettyImages © gremlin_E+; S. 2: Stephan Kohzer/BSI; S. 4, oben: BSI; S. 4, unten: Fotolia © aerogondo; S. 5, BSI; S. 7: GettyImages © Image Source; S. 9: ENISA; S. 10/11: GettyImages ©Yuichiro Chino_Moment, AdobeStock; S. 12: GettyImages ©gremlin_E+; S. 14: GettyImages ©gremlin_E+; S. 15: © Thomas Mohr; S. 17: © Thomas Mohr; S. 18/19: BSI; S. 20: Fotolia @ Syda Productions; S. 24: GettyImages © ryccio_DigitalVision Vectors; S. 26: GettyImages © erhui1979_DigitalVision Vectors; S. 28/29: GettyImages © sarayut; GettyImages © republica_E+; GettyImages © Morsa Images_DigitalVision; GettyImages © Inti St Clair; GettyImages © Erik Isakson_DigitalVision6; GettyImages © deepblue4you_E+; GettyImages © Dan Dalton_Caiaimage; GettyImages © Busakorn Pongparnit_Moment; S. 31: © Markus Feger; Composing © Jens Ripperger; S. 32, oben: GettyImages © Ralf_Hiemisch-keineKollektion; S. 32, unten: GettyImages © amtitus_DigitalVision Vectors; S. 35/36: BSI; S. 38/39: BSI, Bundesministerium des Innern, für Bau und Heimat; S. 40: GettyImages ©alengo_E+; S. 42/43: Bundeswehr/Martina Pump; S. 44: Composing und Mockups FAKTOR 3 AG; S. 46: GettyImages © oxygen_Moment; S. 49: GettyImages © oxygen_Moment; S. 50-52: FAKTOR 3 AG; S. 56: BSI; S. 60/61: BASF; S. 62/63, unten: FAKTOR 3 AG; S. 65: Verbraucherzentrale NRW; S. 68: Composing FAKTOR 3 AG;

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