



Bundesamt  
für Sicherheit in der  
Informationstechnik

Deutschland  
Digital•Sicher•BSI•

BSI-Magazin 2022/01

# Mit Sicherheit



Im Blickpunkt:  
**10 Jahre Allianz für  
Cyber-Sicherheit**

## Cyber-Sicherheit

Digitale Transformation leben:  
Interview mit Nancy Faeser

## IT-Sicherheit in der Praxis

Die Neupositionierung  
des IT-Grundschutzes in der  
Bundesverwaltung

## Digitale Gesellschaft

Schwachstellen und ihre  
Auswirkungen auf die  
Lieferkette



*Sehr geehrte Leserinnen und Leser,*

in den letzten Ausgaben des BSI-Magazins haben wir uns vielfach mit dem Digitalisierungsschub durch die Coronapandemie auseinandergesetzt. Infolge des russischen Angriffskriegs auf die Ukraine ist nun erneut und eindrücklich sichtbar, wie zentral Cyber-Sicherheit für Unternehmen, Institutionen und – denken wir z. B. an Desinformationskampagnen – nicht zuletzt auch für Verbraucherinnen und Verbraucher durch die digitale Vernetzung vieler Bereiche geworden ist.

Cyber-Angriffe gehören neben Naturkatastrophen und Betriebsunterbrechungen weltweit zu den drei größten Geschäftsrisiken. Bundesinnenministerin Nancy Faeser macht in dieser Ausgabe des BSI-Magazins deutlich, dass Angriffe auf digitale Infrastrukturen zudem längst ein gebräuchliches Mittel in Konfliktsituationen sind. Sie weist aber auch darauf hin, dass wir dem nicht schutzlos ausgeliefert sind – unter anderem, weil die Mitarbeiterinnen und Mitarbeiter der Cyber-Sicherheitsbehörden mit großem Engagement an Aufklärung und Prävention arbeiten.

Für den Schutz unserer IT-Infrastrukturen sorgt auch Europas größte Public-private-Partnership, die in diesem Jahr ihren zehnten Geburtstag feiert. Hinter der Gründung der „Allianz für Cyber-Sicherheit (ACS)“ stand das Ziel, die Vernetzung nicht auf Kritische Infrastruktur zu beschränken, sondern Wirtschaftsunternehmen und andere wichtige Akteure einzubeziehen. Das ist eindrucksvoll gelungen: Die ACS ist in diesen zehn Jahren nicht nur ein Netzwerk mit aktuell über 6.000 Teilnehmern geworden, sondern auch ein umfangreiches Informationsportal, über das sich Menschen und Institutionen unkompliziert über die wichtigsten Fragen der Informations- und Cyber-Sicherheit informieren können.

Auf diesem breiten Fundament werden wir unsere Angebote speziell für kleine und mittlere Unternehmen (KMU) ausbauen. Denn diese haben – wie wir alle – den Wunsch nach mehr Informationssicherheit. Leider fehlen KMU oft die personellen Kapazitäten dafür. Als die Cyber-Sicherheitsbehörde des Bundes beziehen wir alle Stakeholder in unsere Arbeit ein, damit Prävention, Detektion und Reaktion bei Angriffen künftig zu immer mehr Sicherheit in der Digitalisierung führen. So sichern wir nicht nur den Wirtschafts- und Wissenschaftsstandort Deutschland ab, sondern ermöglichen es auch Nutzerinnen und Nutzern, sich sicher im digitalen Raum zu bewegen.

Ich wünsche Ihnen eine interessante Lektüre.

Ihr



**Arne Schönbohm,**

*Präsident des Bundesamts für Sicherheit in der Informationstechnik*





# Inhalt

## Aktuelles

### Cyber-Sicherheit

<b>Interview mit Bundesinnenministerin Nancy Faeser .....</b>	<b>08</b>
Cyber-Sicherheit im Luftverkehr .....	12
Log4j: Die Gefahr bleibt .....	14
BSI-Standards für die Beschaffung sicherer Cloud-Dienste .....	16
Das Internet im Wandel .....	18

### IM BLICKPUNKT: 10 Jahre Allianz für Cyber-Sicherheit

10 Jahre Allianz für Cyber-Sicherheit .....	20
Interview mit Harald Niggemann .....	24
Interview mit Stephan Blank .....	28
Interview mit Sebastian Artz .....	30
Das Cyber-Sicherheitsnetzwerk .....	31

### Das BSI

<b>Vielfalt schafft Mehrwert beim BSI .....</b>	<b>34</b>
Gemeinsam stark – Interview mit BSI-Präsident Arne Schönbohm .....	37
Impulse für die sichere Digitalisierung Deutschlands – Der 18. Deutsche IT-Sicherheitskongress .....	38
Der Beirat Digitaler Verbraucherschutz .....	40
Ein digitaler Dialog in Zeiten der Pandemie .....	42

### IT-Sicherheit in der Praxis

Einführung des IT-Sicherheitskennzeichens .....	44
VS-IT: Eingestuft und gut geschützt .....	48
Inстанz für die Sicherheit biometrischer Verfahren .....	52
<b>Die Neupositionierung des IT-Grundschutzes in der Bundesverwaltung .....</b>	<b>55</b>
Workshop-Reihe Prüfung von KI-Systemen .....	58
NESAS als 5G-Zertifizierungsverfahren .....	60

### Digitale Gesellschaft

Die vernetzte Stadt – Informationssicherheit für Smart Cities .....	62
Cyber-Sicherheit in der öffentlichen Verwaltung – Interview mit Boris Pistorius und BSI-Präsident Arne Schönbohm .....	64
<b>Schwachstellen in Produkten und ihre Auswirkungen auf die Lieferkette .....</b>	<b>66</b>
Cyber-Sicherheit in der Lieferkette der Automobilindustrie .....	70
<b>Moderne Messenger – heute verschlüsselt, morgen interoperabel? .....</b>	<b>72</b>
BSI Basis-Tipp: Sichere Onlineshops erkennen .....	74

## Cyber-Resilienz stärken

# Virtuelle Roadshow für Kommunen in Sachsen

Zum Auftakt einer virtuellen Roadshow durch die Bundesländer hat das BSI Anfang Mai gemeinsam mit der Sächsischen Staatskanzlei die erste virtuelle Veranstaltung für die Kommunen im Freistaat Sachsen ausgerichtet. Im Rahmen der „Roadshow Kommunen“ wurden die insgesamt 180 Teilnehmenden aus unterschiedlichen Städten und Gemeinden in Sachsen für die aktuelle Bedrohungslage sensibilisiert. Mit Hilfe kostenloser E-Learning-Programme erhielten sie konkrete Handlungsempfehlungen, mit denen sie die

Cyber-Resilienz innerhalb ihrer Kommunen erhöhen können. Die „Roadshow Kommunen“ des BSI wird im Laufe des Jahres in anderen Bundesländern fortgesetzt. BSI-Präsident Arne Schönbohn sagt dazu: „Wir freuen uns über das große Interesse der sächsischen Kommunen an der ‚Roadshow Kommunen‘, die wir bundesweit mit interessierten Bundesländern durchführen. Der gut besuchte Auftakt in Sachsen hat gezeigt, dass wir mit unserem Angebot einen Nerv getroffen haben.“

## Fokusthema im „Bericht zum Digitalen Verbraucherschutz 2021“

# Das vernetzte Auto der Zukunft



Im Frühjahr 2022 ist die BSI-Jahrespublikation „Bericht zum Digitalen Verbraucherschutz“ erschienen. Der inhaltliche Schwerpunkt der zweiten Ausgabe liegt in den besonderen Anforderungen an die IT-Sicherheit im Automobilbereich aus dem Blickwinkel des Digitalen Verbraucherschutzes. Der Bericht enthält außerdem wissenschaftliche Erkenntnisse über das IT-Sicherheitsverhalten von Verbraucherinnen und Verbrauchern und informiert seine Leserinnen und Leser über wesentliche Sicherheitsvorfälle und -risiken am digitalen Verbrauchermarkt im Berichtszeitraum 2021.

## Weitere Informationen:



[https://www.bsi.bund.de/DE/Service-Navi/Publikationen/DVS-Bericht/dvs-bericht\\_node.html](https://www.bsi.bund.de/DE/Service-Navi/Publikationen/DVS-Bericht/dvs-bericht_node.html)

## BSI-Kampagne

## Alltagsheldinnen und -helden der IT-Sicherheit

Vor rund einem Jahr haben wir zusammen mit dem BMI unter dem Motto #einfachBSIchern unsere bundesweite Kampagne für mehr IT-Sicherheit gestartet. Dabei haben wir plakativ die Frage gestellt, ob Verbraucherinnen und Verbraucher in ihrem digitalen Alltag gut abgesichert sind. Die Motive der Kampagne zeigten digitale Anwendungen wie die digitale Shopping-Tour oder den online stattfindenden Spieleabend. Die Kampagne sollte so zum Nachdenken anregen und für IT-Sicherheitsthemen sensibilisieren.

Das Motto #einfachBSIchern machte dabei deutlich, dass es nicht kompliziert sein muss, die eigenen Accounts und Geräte abzusichern. Denn selbst wer die eigenen Geräte für noch nicht gut abgesichert hält, kann das IT-Sicherheitsniveau mit einfachen Tipps schon erheblich steigern. Mit dem so gewonnenen Wissen ist es dann auch leicht möglich, andere in puncto IT-Sicherheit zu unterstützen. Hier setzt die neue Kampagne an. Egal, ob eine Oma ihrer Enkelin dabei hilft, sicher online zu shoppen, eine Gamerin ihrer Community Sicherheits-Tipps vermittelt oder ein „smartes“ Pärchen seinem Freundeskreis wichtige Kniffe für ein sicheres Smarhome erklärt – wir sind uns sicher, dass Verbraucherinnen und Verbraucher die eigentlichen digitalen Alltagsheldinnen und -helden sind.



Wir alle können dazu beitragen, das IT-Sicherheitsniveau in Deutschland zu erhöhen. Indem jeder und jede die eigenen Geräte und Accounts absichert und Freundinnen, Freunden oder der Familie dabei unter die Arme greift.

Das BSI unterstützt dabei mit Tipps zu verschiedenen Themen wie Onlineshopping, Social Media, Home-Office, Smarhome und Onlinegaming. Unter [www.einfachabsichern.de](http://www.einfachabsichern.de) sind neben hilfreichen Tipps auch alle bisherigen Inhalte der bundesweiten IT-Sicherheitskampagne zu finden.

## Starke Partnerschaft

## BSI und Saarland kooperieren für mehr Cyber-Sicherheit

Das BSI und das Saarland intensivieren ihre Zusammenarbeit. BSI-Präsident Arne Schönbohm und der Chief Information Officer (CIO) des Saarlandes, Ammar Alkassar, unterzeichneten am 21. Februar 2022 eine Kooperationsvereinbarung zur Stärkung der Cyber- und Informationssicherheit.

Die 24-Punkte-Erklärung sieht u. a. vor, die „Cyberwehr Saarland“ und das Cyber-Sicherheitsnetzwerk des BSI eng miteinander zu verzahnen. Zudem haben sich beide

Partner darauf geeinigt, stärker für den Digitalen Verbraucherschutz zusammenzuarbeiten. Das BSI eröffnete bereits im Juni 2021 einen Stützpunkt in Saarbrücken und unterstützte das Saarland auch bei der Absicherung der Landtagswahl am 27. März 2022.

Die Kooperationsvereinbarung ist nach der mit Niedersachsen die zweite, die das BSI mit einem Bundesland abgeschlossen hat.



# Digitale Transformation leben

Cyber-Sicherheit für alle gesellschaftlichen Akteure sichern

Nancy Faeser, Bundesministerin des Innern und für Heimat, über aktuelle Herausforderungen im Bereich der Cyber-Sicherheit und wie die Digitalisierung von Gesellschaft, Staat und Verwaltung gelingen kann. Ein Interview in bewegten Zeiten.

*Woraus ergeben sich Ihres Erachtens die größten Herausforderungen in der Cyber-Sicherheit?*

**Nancy Faeser:** Mit Blick auf die Cyber-Sicherheit müssen wir im Auge haben, dass alle Lebensbereiche zunehmend digitalisiert sind. Das heißt: Das Thema Cyber-Sicherheit betrifft uns überall, auch in vielen alltäglichen Bereichen. Schadprogramme werden zudem immer ausgefeilter und Cyber-Angriffe immer gezielter ausgeführt. Cyber-Angriffe sind mittlerweile leider auch ein

gebräuchliches Mittel in Konfliktsituationen, wie uns der Krieg in der Ukraine aktuell bitter vor Augen führt.

*Welche Ziele enthält Ihr Programm „Digitales Deutschland“ zum Thema Cyber-Sicherheit? Wie sieht die zeitliche Perspektive der Agenda aus und welche konkrete Rolle kommt dem BSI hierbei zu?*

**Faeser:** Mit unserem Digitalprogramm legen wir die Schwerpunkte für die Bereiche Digitale Gesellschaft, Digitale Verwaltung und Cyber- und Informationssicherheit für





### **Kurzvita Nancy Faeser**

*Bundesministerin des Innern und für Heimat*

Nancy Faeser wurde 1970 in Bad Soden am Taunus geboren. Nach ihrem Abitur absolvierte sie das Studium der Rechtswissenschaft an der Johann Wolfgang Goethe-Universität in Frankfurt. Von 2000 bis 2007 arbeitete Nancy Faeser bei der internationalen Wirtschaftskanzlei Clifford Chance und seit 2007 bei der Wirtschaftskanzlei GÖRG Rechtsanwälte.

Nancy Faeser ist seit 1988 Mitglied der SPD und seit 1993 Mitglied des Kreistages des Main-Taunus-Kreises.

die aktuelle Legislaturperiode bis 2025 fest. Mit unseren Maßnahmen wollen wir die Digitalisierung von Gesellschaft, Staat und Verwaltung deutlich vorantreiben und beschleunigen. Und zugleich wollen wir die gesellschaftlichen Fragen dabei im Blick behalten und unsere technologischen Chancen nutzen.

Im Bereich Cyber- und Informationssicherheit ist es entscheidend, dass wir die Cybersicherheitsarchitektur modernisieren und harmonisieren. Dazu zählt u. a. die Stärkung der Digitalen Souveränität, aber auch die Weiterentwicklung der Cybersicherheitsstrategie und des Informationssicherheitsrechts.

*Dem BSI kommt bei der Umsetzung des Programms eine bedeutende Rolle zu. So wollen wir das BSI zu einer Zentrale in der Informationssicherheit ausbauen.*

Wir wollen die föderale Zusammenarbeit deutlich vertiefen. Bund und Länder sollen auf Dauer angelegt und institutionalisiert kooperieren können. Das umfasst die laufende gegenseitige Unterrichtung und Auskunftserteilung, wechselseitige Beratung, Unterstützung und Hilfeleistung. Hierzu zählen auch gemeinsame Informationssysteme zwischen Bund und Ländern. Wir stärken das BSI erneut in seiner Rolle. Das ist gut und wichtig!

*Mit dem Angriff auf die Ukraine haben die Sicherheitsbehörden auch die Schutzmaßnahmen zur Abwehr etwaiger Cyber-Attacken hochgefahren und relevante Stellen sensibilisiert. Wie läuft die Kooperation der Behörden im Nationalen Cyber-Abwehrzentrum?*

**Faeser:** Die zuständigen Behörden beobachten die Situation in der Ukraine und deren Auswirkungen auf deutsche Stellen permanent sehr genau und stimmen sich hierzu intensiv im Nationalen Cyber-Abwehrzentrum ab. Es leistet damit einen sehr wertvollen Beitrag in der aktuellen Situation. Ich habe den Eindruck, dass die Zusammenarbeit unserer Behörden von hohem – auch persönlichem – Einsatz und einem Ziel geprägt ist: gemeinsam größtmögliche Sicherheit im Cyber-Raum zu gewährleisten. Dafür möchte ich mich bei allen Mitarbeiterinnen und Mitarbeitern bedanken, denen in dieser Lage viel abverlangt wird.

*Ein Themenschwerpunkt dieser Magazin-Ausgabe ist das zehnjährige Bestehen der Allianz für Cyber-Sicherheit, einer BSI-Initiative, die sich an Unternehmen wendet. Wie sind die Unternehmen im Hinblick auf eine sichere Gestaltung der Digitalisierung und Cyber-Sicherheit aufgestellt?*

**Faeser:** Die Allianz für Cyber-Sicherheit (ACS) ist eine herausragende Initiative. Allein die Reichweite mit einer Teilnehmerzahl von über 6.000 Unternehmen und Organisationen spricht für sich. Die Teilnehmenden profitieren natürlich von den Angeboten, die die ACS durch die Partner und das BSI bereitstellen. Dennoch ist längst nicht jedes Unternehmen gut oder wenigstens ausreichend

im Hinblick auf die Cyber-Sicherheit aufgestellt. Da bedarf es noch einiger Aufklärungsarbeit und schließlich der Umsetzung höherer Standards in den Unternehmen. Cyber-Sicherheit beginnt in der Chefetage und muss für alle Bereiche mitgedacht werden, da dies ein bereichsübergreifendes Thema ist. Entsprechende Empfehlungen und Informationsangebote, aber auch Dienstleister sind vorhanden. Es fehlt häufig die Umsetzung, was sicher auf unterschiedliche Gründe, wie knappe Ressourcen, zurückzuführen ist.

Für das BSI wird das – angesichts des Fachkräftemangels und des Umgangs mit sehr unterschiedlichen kleinen und mittelständischen Unternehmen – bedeuten, die Angebote weiter auszubauen und zu verbessern. Dazu gehört ein modernes Information Sharing, das die derzeitigen einzelnen Kommunikationskanäle des BSI auf einer Plattform bündelt und eine bi- und multidirektionale Kommunikation zwischen den Beteiligten ermöglicht. Ein weiterer Nutzen wäre, dass die Bundesregierung ein digitales Lagebild erhält und in der Folge Sachverhalte besser bewerten kann und schneller auskunftsfähig ist.

**Die umfassende Digitalisierung der Verwaltung ist ein wichtiges Thema auf Ihrer Agenda. Was ist aus Ihrer Sicht das Fundament einer solchen umfassenden Digitalisierung? Wie kann diese noch sicherer gestaltet werden?**

**Faeser:** Erstens muss die Digitalisierung ein kultureller Bestandteil der Verwaltung werden. Die Verwaltung muss die digitale Transformation verinnerlichen und leben. Digitalisierung darf nicht mehr nur punktuell in einzelnen Projekten angegangen werden. Im EU-Vergleich zeigt sich, dass Deutschland die Versäumnisse der früheren Jahre noch nicht aufholen konnte. Das wollen wir ändern. Mit der Umsetzung des Onlinezugangsgesetzes (OZG), der EU-Single-Digital-Gateway-Verordnung, dem Registermodernisierungsgesetz, der Digitalisierung des Personalausweises und der IT-Konsolidierung des Bundes, um nur ein paar zu nennen, haben wir im BMI große Reformvorhaben zu stemmen. Das OZG ist das bis dato größte Modernisierungsprojekt der deutschen Verwaltung. Dazu müssen sich Politik und Verwaltung der digitalen Transformation auf allen Ebenen annehmen.



Ein weiterer Aspekt ist, dass wir eine neue Form der Zusammenarbeit etablieren. Die OZG-Umsetzung hat mit ihrem arbeitsteiligen Vorgehen zwischen Bund und Ländern viel Tatkraft und Willen zum Aufbruch mobilisiert. Auf diese neu entstandenen Strukturen können wir zukünftig aufbauen und für die Verwaltungsdigitalisierung viel bewirken.

Ein dritter Aspekt ist die Nutzerorientierung, die bei der Digitalisierung von Verwaltungsleistungen im Fokus steht. Wir werden Online-Services für Bürgerinnen und Bürger sowie Unternehmen zügig so digital verfügbar machen, dass wir ihren Alltag spürbar erleichtern.





Beispielsweise werden mit der Verknüpfung der Verwaltungsportale von Bund und Ländern zu einem Portalverbund sämtliche Leistungen deutschlandweit für alle Nutzenden mit nur wenigen Klicks sicher und einfach erreichbar sein.

Diese drei Aspekte bilden – neben vielen anderen – aus meiner Sicht das Fundament einer umfassenden Verwaltungsdigitalisierung.

Was wir hierzu zwingend benötigen, ist die sichere, föderale Kommunikation zwischen allen Beteiligten. Hierzu gehört selbstverständlich auch die Nutzung

eigener Infrastrukturen als Träger der Kommunikation. Hierzu hat mein Ministerium die Netzstrategie 2030 der öffentlichen Verwaltung erarbeitet. Diese Netzstrategie adressiert nicht nur die Bundesverwaltung, sondern betrachtet die Kommunikation der gesamten öffentlichen Verwaltung. Das ist die grundlegende Voraussetzung für eine umfassende medienbruchfreie Digitalisierung der öffentlichen Verwaltung. ■



### **Digitales Deutschland**

*Souverän. Sicher. Bürgerzentriert.*

So lautet der Titel des digitalpolitischen Programms, das Bundesinnenministerin Nancy Faeser im April 2022 vorgestellt hat. Darin werden in der aktuellen Legislaturperiode Ziele gesetzt für eine weitere Digitalisierung der Verwaltung, eine Stärkung der Cyber-Sicherheit und einen Digital-Check für Gesetze des Bundes in der laufenden Legislaturperiode.

So will die Ministerin erreichen, Deutschland moderner, bürgernäher und digitaler zu machen.

Zur Modernisierung der nationalen Cybersicherheitsarchitektur soll unter anderem das BSI zur Zentrale in der Informationssicherheit ausgebaut werden. Das Bundesministerium des Innern und für Heimat ist mit seinen Zuständigkeiten für Cyber-Sicherheit, Digitalisierung der Verwaltung und Datenpolitik ein Schlüsselressort für die Modernisierung des Staates.

# Cyber-Sicherheit im Luftverkehr



## Ein neuer Aufgabenbereich für das BSI

von Dr. Dina Truxius, Projektgruppe Luftsicherheit

Cyber-Angriffe auf den Luftverkehr – ein Thema, das an Science-Fiction erinnert. Die Projektgruppe Luftsicherheit zeigt, an welchen Stellschrauben gedreht werden muss, um ein einheitliches IT-Sicherheitsniveau an Flughäfen zu erreichen.

**F**liegen gilt als sicherste Art der Fortbewegung. Doch diese Sicherheit kommt nicht von ungefähr, sondern ist das Ergebnis einer kontinuierlichen Anpassung der Technik sowie der Einführung einer konsequenten Sicherheitskultur. Durch den Digitalisierungsdruck, der auch den Luftverkehr betrifft, werden mehr und mehr IT-Systeme eingesetzt und vernetzt. Das bedeutet, dass Cyber-Angriffe im Luftverkehr nicht mehr nur Fiktion sind, sondern zu einer realen Bedrohung werden könnten. Aus diesem Grund muss die Luftsicherheit nun ebenfalls die Informationssicherheit mitbetrachten.

### Luftsicherheit, Flugsicherheit, Flugsicherung und Informationssicherheit

Die Luftverkehrsbranche ist seit jeher stark reguliert und weist ein besonders hohes Sicherheitsbewusstsein und eine entsprechende Sicherheitskultur auf. Doch was ist Sicherheit, was bedeutet sie für die Branche und wie wird sie realisiert? Wichtige Komponenten, von einzelnen Schrauben bis hin zu vollständigen Systemen, sind doppelt und dreifach ausgelegt. Neben dieser gesetzlich festgelegten Redundanz sind häufige Wartungen, Zulassungsverfahren und Audits ständige Begleiter des Luftverkehrs. So komplex die rechtlichen Anforderungen sind, so irreführend können die fachlichen Begriffe sein. Daher ist zu unterscheiden, ob es sich bei dem deutschen Begriff „Sicherheit“ um Aspekte handelt, die in der Branche selbst unter die englischen Begriffe „Safety“ oder „Security“ fallen. Unter Luftsicherheit („Security“) wird im Bereich der zivilen

Luftfahrt die Abwehr von äußeren Gefahren bezeichnet. Mit „Safety“ hingegen ist die Flugsicherheit, also die technische und betriebliche Verkehrssicherheit von Flugzeugen, gemeint. Von den beiden zuvor genannten Begriffen zu unterscheiden ist die Flugsicherung, die als sichere und geordnete Verkehrslenkung im Luftraum definiert ist.

Durch die Ergänzung der EU-Durchführungsverordnung DVO (EU) 2015/19983 werden seit dem 1. Januar 2022 die in den §§ 5 (Personen- und Gepäckkontrolle), 8 (Flughafenbetreiber), 9 (Luftfahrtunternehmen) und 9a (sichere Lieferkette) Luftsicherheitsgesetz (LuftSiG) genannten Akteure nun auch hinsichtlich der Informationssicherheit reguliert. Ziele der Verordnung sind der Schutz und die Absicherung des zivilen Luftverkehrs vor Cyber-Angriffen, insbesondere in Bezug auf Flugzeugentführungen, Sabotageakte und terroristische Anschläge. Hierzu zählt vorrangig der Schutz von kritischen informations- und kommunikationstechnischen Systemen und Daten (KIKS). Darunter fallen auch Präventivmaßnahmen wie der Schutz vor und die Erkennung von Cyber-Angriffen sowie der angemessene, praktikable und rechtzeitige Austausch von Informationen zu Schwachstellen oder Schadsoftware. Das bedeutet konkret, dass die Akteurinnen und Akteure künftig die Informationssicherheit ihrer KIKS bei der Zulassung mitbetrachten und schrittweise ein gewisses IT-Sicherheitsniveau ihrer Organisation aufweisen und dauerhaft gewährleisten müssen.



### **Spannende Aufgaben für das BSI im Bereich der Luftsicherheit**

Das Bundesministerium des Innern und für Heimat (BMI) ist Deutschlands oberste Luftsicherheitsbehörde. Es hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) per Aufgabenübertragungserlass mit der Koordinierung und Steuerung der Maßnahmen zur Informationssicherheit in der Luftsicherheit für die nach §§ 5 und 8 LuftSiG regulierten Betreiber in Deutschland betraut, worunter insgesamt 28 Flughafenbetreiber fallen. Zur Gestaltung und Umsetzung der neuen Aufgaben wurde im September 2021 die Projektgruppe Luftsicherheit (PG LuSi) im BSI gegründet, die den Auf- und Ausbau des neuen Betätigungsfelds übernommen hat.

Gemeinsam mit dem BMI und den Ländern hat das BSI Grundsätze erarbeitet, um den Anforderungen der DVO gerecht zu werden. Diese sehen vor, dass die Betreiber ab 2024 ein nachweisbares IT-Sicherheitsniveau erreicht haben müssen, das mindestens der Basisabsicherung und ab 2027 der Standardabsicherung nach BSI-IT-Grundschutz oder einem vergleichbaren internationalen Standard entspricht. Darüber hinaus wurden u. a. weitere Vorgaben für die nach § 8 LuftSiG regulierten Unternehmen und Hilfsangebote für die Länder entwickelt sowie ein Warn- und Meldewesen aufgebaut. Künftig werden BSI-seitig auch Auditoren für die Sicherheitsaudits im Rahmen des Nationalen Qualitätsprogramms (NQP) gestellt.

In dem im November 2021 gegründeten Expertenkreis „Cyber-Sicherheit im Luftverkehr“ trifft Luftsicherheitsexpertise auf Cyber-Sicherheitsexpertise. Der Kreis soll durch vertrauensvollen Austausch als Kompetenzcluster für die luftsicherheits- und cyber-sicherheitsrelevanten Themen und deren weitere Gestaltung in Deutschland dienen und richtet sich genauso an Flughafenbetreiber wie an Expertinnen und Experten aus Forschung, Wirtschaft und Verwaltung.

In den kommenden Jahren werden dem BSI zudem weitere spannende Aufgaben im Bereich der Luftsicherheit zuteilwerden. ■

#### **Weitere Informationen:**



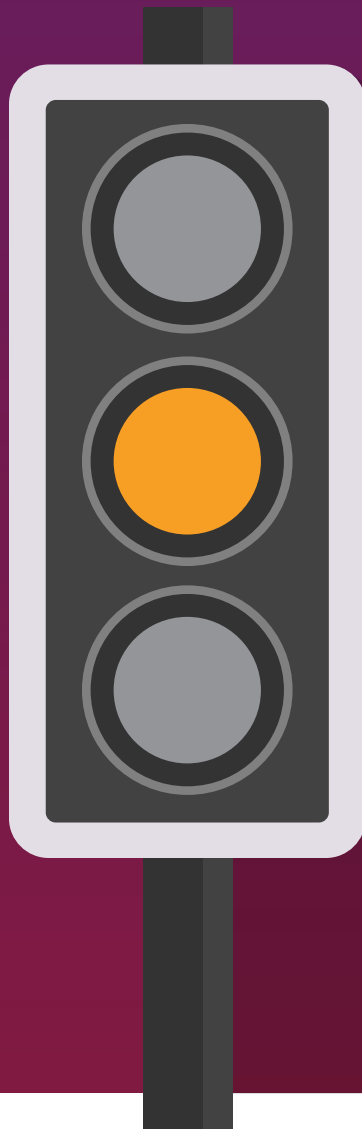
[https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Weitere\\_regulierte\\_Unternehmen/LuSi/Luftsicherheit\\_node.html](https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Weitere_regulierte_Unternehmen/LuSi/Luftsicherheit_node.html)

# Log4j: Die Gefahr bleibt

**Von Alarmstufe Rot auf Gelb herabgestuft**

*von Marco Krambrich, Referat Nationales IT-Lagezentrum, Analysen und Prognosen*

Der Umgang mit Schwachstellen ist und bleibt eine der größten Herausforderungen der Informationssicherheit. Cyber-Kriminelle sind aufgrund ihrer technischen Möglichkeiten dazu fähig, solche Schwachstellen gezielt auszunutzen – und sie lassen praktisch nichts unversucht, das auch zu tun. Eine der schwersten Lücken der jüngsten Vergangenheit tat sich im Dezember 2021 auf – in der Java-Bibliothek Log4j. Die Schwachstelle veranlasste das BSI zum Ausrufen der kritischen Warnstufe Rot. Eine Zwischenbilanz.



**I**m Dezember 2021 wurde in der weit verbreiteten Java-Bibliothek Log4j eine Schwachstelle (CVE-2021-44228) mit dem höchsten Kritikalitätswert gemäß Common Vulnerability Scoring System (CVSS) von 10,0 entdeckt. „Diese kritische Schwachstelle hat möglicherweise Auswirkungen auf alle aus dem Internet erreichbaren Java-Anwendungen, welche mit Hilfe von Log4j Nutzeranfragen protokollieren“, kommentierte das BSI damals und warnte: „Wer nicht patcht, geht enorme Risiken ein. Kompromittierte Systeme können zu Cyber-Angriffen mit hoher Schadenswirkung führen.“ Um dieser Warnung den nötigen Nachdruck zu verleihen, aktivierte die Cyber-Sicherheitsbehörde des Bundes das Nationale IT-Krisenreaktionszentrum und vergab zusätzlich die Warnstufe Rot.

Die Java-Bibliothek Log4j ist in zahlreichen Anwendungen implementiert und definiert einen quelloffenen Quasi-standard zum Protokollieren von Daten. Ihre große Verbreitung, eine hohe Marktdurchdringung sowie die einfache Möglichkeit, sie auszunutzen, machen diese Schwachstelle so gefährlich.

Bereits am 10. Dezember 2021 informierte das BSI umfassend über diesen Sachverhalt. Warnmeldungen wurden fortlaufend aktualisiert und durch öffentlich verfügbare Dokumente mit Anleitungen zu Prävention und Schadensbeseitigung auf der BSI-Webseite ergänzt. Da viele Softwareanbieter zeitnah Patches und Workarounds für ihre Produkte veröffentlicht hatten und zudem die erwartete Ausnutzung der Lücke über die Weihnachtsfeiertage in Deutschland ausblieb, stufte das BSI bereits am 12. Januar 2022 die IT-Bedrohungslage auf die Stufe Gelb herunter. Es gibt allerdings weitere Hinweise darauf, dass die Schwachstelle weltweit ausgenutzt wird. Daher sollten grundsätzlich Auffälligkeiten auch weiter beobachtet werden.

### **Informationssicherheit ist die Grundlage für eine erfolgreiche Digitalisierung**

Log4j verdeutlicht die Bedeutung von Softwarequalität für die IT-Sicherheit. Die Verbesserung der Softwarequalität ist ein wichtiger Beitrag zur Erhöhung der IT-Sicherheit als Grundlage einer erfolgreichen Digitalisierung.

Softwarehersteller sollten daher im eigenen Interesse daran (mit)arbeiten, schnellstmöglich und konsequent herstellerseitig einen Prozess für den Umgang mit Meldungen über Schwachstellen in ihren IT-Produkten und Systemen zu etablieren, einen sogenannten Coordinated-Vulnerability-Disclosure-(CVD-)Prozess. Dieser ermöglicht es Sicherheitsforschenden, die Schwachstellen in IT-Produkten entdeckt haben, diese an eine zentrale Adresse

zu melden und bei der Behebung und geeigneten Veröffentlichung von Patches zu unterstützen. Große CVD-Fälle haben gezeigt, dass viele Hersteller nur mit sehr viel Mühe feststellen können, welche Bibliotheken und andere Dritthersteller-Software in ihren Produkten und über die gesamte Wertschöpfungskette hinweg eingesetzt werden. Das BSI fordert daher eine zielgerichtete Umsetzung von Maßnahmen für eine bessere Softwarequalität in IT-Produkten. Dazu unterstützt das BSI aktiv Konzepte wie beispielsweise Software Bill of Materials (SBOM) und Common Security Advisory Framework (CSAF), um CVD-Prozesse zu optimieren (siehe Artikel auf S. 66).

Verantwortung kommt aber auch den Anwenderunternehmen zu: Sie haben einen aktiven Part dabei, ihre eigenen IT-Systeme und -Netze zu schützen. Wer das nicht tut, geht enorme Risiken ein, denn Produktionsausfälle infolge eines Cyber-Angriffs können schnell existenzbedrohend sein. Gemäß dem Motto des diesjährigen IT-Sicherheitskongresses muss Cyber-Sicherheit daher Cheffinnen- und Chefsache sein und mit ausreichenden Ressourcen zum festen Bestandteil des eigenen Risikomanagements gemacht werden.

### **Wie geht es weiter?**

Mit dem IT-Sicherheitsgesetz 2.0 hat das BSI zusätzliche Aufgaben bei der Entdeckung von Sicherheitslücken und der Abwehr von Cyber-Angriffen übernommen.

Zudem misst die Regierungskoalition der Cyber- und Informationssicherheit in Deutschland einen sehr hohen Stellenwert zu und hat dies im aktuellen Koalitionsvertrag mehrfach zum Ausdruck gebracht. Vorgaben wie „Security by Design“ und „Security by Default“ sind ebenso Teil des Vertrages wie die Einführung eines wirksamen Schwachstellenmanagements unter Federführung eines gestärkten BSI und die Ausweitung der Herstellerhaftung für Schäden durch IT-Sicherheitslücken.

Die Voraussetzungen für eine sichere Digitalisierung sind also geschaffen. Es gilt jetzt, diesen Weg konsequent weiter zu beschreiten. ■

### **Weitere Informationen:**



[https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Webanwendungen/log4j/log4j\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Webanwendungen/log4j/log4j_node.html)

# BSI-Standards für die Beschaffung sicherer Cloud-Dienste

**Mit den EVB-IT Cloud werden Behörden bei der Beschaffung sicherer Cloud-Dienste unterstützt**

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

Cloud-Dienste sind längst ein wichtiger Bestandteil moderner und agiler IT. Dabei hat sich vor allem der BSI C5 in den vergangenen Jahren weltweit als Sicherheitsstandard für Cloud-Dienste etabliert. Die Beschaffung als vorwiegend juristisches Thema wird dabei selten als „einfach“ oder „agil“ bezeichnet. Mit den neuen EVB-IT Cloud könnte sich das ändern.



**C**loud-Dienste zeigen auf, was die Digitalisierung oder auch die digitale Revolution in der Realität bedeuten können. Sie lassen sich mit den Fabriken der industriellen Revolution vergleichen: Wo vorher individuelle Produkte eine eher lokale Wirtschaft prägten,

kam mit den Fabriken im Zuge der industriellen Revolution die Massenproduktion und damit die Fertigung einheitlicher Produkte auf. Wo früher Dienstleister ihre individuellen IT-Serviceleistungen erbracht haben, übernehmen heute standardisierte Cloud-Dienste diese



Aufgabe. Analog zu einheitlichen Produkten aus industrieller Fertigung mit definierten Eigenschaften lässt sich auch bei Cloud-Diensten der Anspruch auf Erfüllung einheitlicher Sicherheitseigenschaften formulieren.

### Sichere Cloud-Dienste sicher nutzen: BSI C5 und Mindeststandard

Das zu übernehmen, ist die Aufgabe des BSI, das damit maßgeblich die IT-Sicherheit im Zeitalter der Digitalisierung gestaltet. Der Cloud Computing Compliance Criteria Catalogue – kurz C5 – des BSI ist ein Katalog von Sicherheitskriterien, ergänzt um einen effizienten Nachweisweg über ein Testat durch unabhängige Prüfer. Diesen Nachweis (und seine Auswertung anhand einer eigenen Risikobewertung) hat das BSI mit dem Mindeststandard zur Nutzung externer Cloud-Dienste für Stellen des Bundes bei Cloud-Beschaffungen verbindlich gemacht. Bestimmte Aspekte, worüber im C5-Prüfbericht lediglich informiert wird, werden bei der Beschaffung festgelegt. Hierzu zählen Gerichtsstand, Lokalisation der Daten, Verfügbarkeit des Dienstes und beteiligte Unterauftragnehmer.

### Was noch fehlte: Hilfe für die Beschaffungsstellen

Es zeigte sich, dass in der Reihe von Dokumenten (C5, C5-Bericht, Mindeststandard) noch etwas fehlte. Denn die Beschaffungsstellen mussten diese Anforderungen in beschaffungskonforme Texte überführen und hatten Schwierigkeiten, eigene Vertragsbestandteile auszuhandeln. Genau dies ändert sich mit den EVB-IT Cloud.

### Was sind EVB-IT?

EVB-IT ist die Abkürzung für „Ergänzende Vertragsbestandteile für die Beschaffung von IT-Leistungen“. Diese bestehen aus einem Vertragsformular, Allgemeinen Geschäftsbedingungen und einem oder mehreren Mustern. Es gibt mehrere EVB-IT für verschiedene Anwendungsfälle. Sie werden vom Bundesministerium des Innern und für Heimat (BMI) entworfen und mit dem Branchenverband der deutschen Informations- und Telekommunikationsbranche (Bitkom e. V.) bis zum Einnehmen verhandelt.

Das besondere an EVB-IT ist die Verbindlichkeit. Alle Bundesbehörden sind gemäß § 55 Bundeshaushaltsordnung (BHO) und der zugehörigen Verwaltungsvorschrift zur Anwendung der EVB-IT verpflichtet. Auch für Landesbehörden sehen die entsprechenden Haushaltsordnungen vergleichbare Verpflichtungen vor. Entsprechend hart und intensiv wird über die Einzelheiten von EVB-IT verhandelt.

### Einblicke in die EVB-IT Cloud

Die EVB-IT Cloud wurden Ende 2021 zwischen BMI und Bitkom ausgehandelt und in der Sitzung der Konferenz der IT-Beauftragten am 16. Dezember 2021 angenommen. Auch der IT-Planungsrat hat mit dem Beschluss 2022/01 vom 11. Februar 2022 die Anwendung der EVB-IT Cloud empfohlen.

Die genauen Inhalte der EVB-IT Cloud darzustellen, ist eher Gegenstand von Seminaren zum Vergaberecht und würde an dieser Stelle zu weit führen. Es lassen sich jedoch einige wesentliche Punkte hervorheben:

- Die EVB-IT Cloud sind für alle gängigen Cloud-Service-Modelle (Infrastructure as a Service, Platform as a Service, Software as a Service und Managed Cloud-Services) anwendbar.
- Die Einhaltung der C5-Sicherheitskriterien in der jeweils gültigen Fassung ist integraler Bestandteil.
- Die aus dem BSI-Mindeststandard „Nutzung externer Cloud-Dienste“ stammende Anforderung nach Aushandlung von eigenen Prüfungsrechten und Leistungsreports wurde aufgenommen.
- Der BSI-Mindeststandard legt ein besonderes Augenmerk auf die Unterauftragnehmer des Cloud-Dienstes. Auch hier stützen sich die EVB-IT Cloud auf den C5-Kriterienkatalog. Unterauftragnehmer, die für die Erfüllung der C5-Kriterien wichtig sind, müssen genannt und vertraglich vereinbart werden. Ein Wechsel der Unterauftragnehmer muss vom Cloud-Anbieter mitgeteilt werden, und sollte dieser für den Nutzer nicht akzeptabel sein, hat er ein außerordentliches Kündigungsrecht.
- In den EVB-IT Cloud wird die Verfügbarkeit der Cloud-Dienste durch die Verfügbarkeitsklassen des BSI-Hochverfügbarkeitskompendiums definiert. Als Standard ist die Verfügbarkeitsklasse VK-1 (99 Prozent) festgelegt.
- Zu den EVB-IT Cloud gibt es als Anlagen Checklisten, bei denen verschiedene optionale Details ausgewählt werden können, wie z. B. das Löschen von Kundendaten zum Vertragsende.

### Fazit

Mit den EVB-IT Cloud ist der Dreiklang „BSI C5 – BSI-Mindeststandard – EVB-IT Cloud“ vervollständigt und alle Stellen des Bundes damit gut gerüstet, Cloud-Dienste mit nachgewiesener Sicherheit mit standardisierten Vertragsbestandteilen zu beschaffen und sicher zu nutzen. Die EVB-IT Cloud nutzen die hohe Standardisierung der Cloud-Dienste, um die Beschaffung zu vereinfachen. Da der BSI C5 so weit im Markt verbreitet ist, steht den Auftraggebern bereits eine große Anzahl Cloud-Services zur Verfügung, die potenziell konform mit den EVB-IT Cloud sind. ■

### Weitere Informationen:



[https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle\\_EVB-IT/aktuelle\\_evb\\_it\\_node.html#doc4623280bodyText3](https://www.cio.bund.de/Web/DE/IT-Beschaffung/EVB-IT-und-BVB/Aktuelle_EVB-IT/aktuelle_evb_it_node.html#doc4623280bodyText3)

# Das Internet im Wandel

## Konsolidierung und Zentralisierung – Fluch oder Segen?

von Markus de Brün, Referat Sicherheit in Internet-Infrastrukturen und -Diensten

**Offenheit und Dezentralisierung sind kombiniert das Erfolgsrezept des Internets und haben es zu dem gemacht, was es heute ist. Doch aktuell erleben wir einen Wandel, der mit diesen Prinzipien bricht.**



**D**as Internet ist ein weltweites Netz aus Netzen vieler einzelner Betreiber. Offene Standards ermöglichen, dass jeder sein eigenes Netz mit dem Internet verbinden oder Anwendungen darauf entwickeln kann. Eine Dienstleistung lässt sich im Internet von überall aus der Welt anbieten. Das Internet fördert so den Wettbewerb zwischen Anbietern. Dank der Offenheit des Internets lassen sich neue Ideen und Dienstleistungen schnell realisieren. Dieses Prinzip der „Permissionless Innovation“ hat das Internet geprägt und es zu dem gemacht, was es heute ist.

### Paradigmenwechsel

Aktuell erleben wir jedoch einen Paradigmenwechsel: weg von Offenheit und Dezentralisierung hin zu Bestrebungen nach Geschlossenheit und Konsolidierung. Insbesondere in den letzten Jahren gab es eine zunehmende Konsolidierung von Anbietern. Damit ging eine Zentralisierung der angebotenen Dienste einher. Der Skaleneffekt („Economics of Scale“) treibt diesen Trend weiter voran. Anbieter mit großen Infrastrukturen und zahlreichen Kundinnen und Kunden können Dienste kostengünstiger anbieten als neue Mitbewerber. So binden die großen Anbieter immer mehr Neukundinnen und -kunden an sich und wachsen damit noch weiter.

Auf der offenen Plattform Internet haben sich zunehmend Dienste entwickelt, die von vornherein nicht auf Interoperabilität setzen und so dem eigentlichen Gedanken des Internets zuwiderlaufen. Soziale Netzwerke sind

ein Beispiel für diese Entwicklung. Die Anbieter, die sich durchsetzen, haben häufig einen großen Marktanteil und kein Interesse, ihre Plattform für andere zu öffnen. Sie profitieren von einer großen Basis aus Nutzerinnen und Nutzern, die sie für Neueinsteigerinnen und Neueinsteiger im Vergleich zu den kleinen Anbietern interessanter macht.

### Rollenwechsel

Auch in der Internet-Infrastruktur und bei ihren Betreibern gibt es Veränderungen. So verantworten aktuell fünf sogenannte Hypergiants schätzungsweise die Hälfte des Internetverkehrs. Dafür waren Anfang der 2000er-Jahre noch tausende Anbieter notwendig.

Auch wurden früher transozeanische Kabel von großen Internet Providern (Tier-1-Provider) in Auftrag gegeben. Für eine weltweite Erreichbarkeit musste ein Content-Anbieter (z. B. ein Anbieter eines sozialen Netzwerks) auf die Dienste großer Tier-1-Provider zurückgreifen. Inzwischen haben große Content-Anbieter aber eine höhere Reichweite als die meisten Tier-1-Provider. Und auch Seekabel werden inzwischen zunehmend von Content-Anbietern in Auftrag gegeben.

### Vorteile und Nachteile der Konsolidierung

Große Unternehmen haben die finanziellen und personellen Ressourcen, um neue Standards einzuführen, die beispielsweise kürzere Latenzen oder mehr Sicherheit versprechen. Die Namensauflösung mittels des Domain Name Systems (DNS) ist hierfür ein gutes Beispiel:



Verschlüsselte DNS-Protokolle wurden zuerst von Betreibern der großen DNS-Resolver implementiert.

Ein Dienst mit vielen Nutzerinnen und Nutzern ist jedoch auch immer ein lohnendes Ziel für Angriffe – etwa um persönliche Daten abzugreifen. Zudem stellt die technische Abhängigkeit von einzelnen Dienstleistern einen möglichen Single Point of Failure dar. Der Ausfall eines zentralen Dienstleisters hat oft gravierende und globale Folgen. Dies wurde deutlich, als Facebook/Meta samt allen Diensten im Oktober 2021 mehrere Stunden offline war. Störungen bei Dienstleistern wie Akamai oder Fastly hatten Ausfälle zahlreicher Webseiten zur Folge.

#### **Bezug zur Standardisierung**

Die meisten der offenen Standards und Protokolle im Internet, die es Anbietern ermöglicht haben, ihre Dienste zu entwickeln, werden von der Internet Engineering Task Force (IETF) spezifiziert. Viele Anbieter beteiligen sich selbst an der Standardisierung neuer Protokolle, verfolgen dabei aber oft eigene Interessen. So verändern oder erweitern einige Anbieter bestehende Standards, um sie an ihre eigenen Bedürfnisse anzupassen.

Andere Anbieter lehnen Standardisierung und offene Protokolle bewusst ab. Sie verwenden proprietäre Protokolle für ihre Anwendungen, selbst wenn offene Standards verfügbar sind. Diese Entwicklung ist folgewidrig, da sogar proprietäre Anwendungen ohne die offenen Basistechnologien der IETF global nicht möglich wären.

#### **Infrastruktur, Ausfallszenarien und Konsolidierung**

Eine Konsolidierung auf Anbieterseite kann den Nutzerinnen und Nutzern viele Vorteile bieten. Doch aus dem Segen kann schnell ein Fluch werden. Eine starke Zentralisierung wirkt sich negativ auf die Resilienz des Internets aus und erleichtert die Aggregation von Nutzerdaten. Die verschiedenen Aspekte wurden im Rahmen einer BSI-Studie detailliert beleuchtet. Neben den Änderungen in der Internet-Infrastruktur wurden auch weitreichende Internetstörungen der letzten Jahre betrachtet. Darauf aufbauend wurden fiktive Ausfallszenarien sowie deren potenzielle Auswirkungen und die Abhängigkeiten von internationalen Kabelverbindungen analysiert. Die Studie schließt mit einem Blick über den IT-Tellerrand ab und diskutiert die wirtschaftlichen und gesellschaftlichen Aspekte der Konsolidierung des Internets. ■

#### **Weitere Informationen:**



Die von den Firmen Leitwert GmbH und link-lab GbR erstellte Studie ist verfügbar unter:  
[www.bsi.bund.de/dok/zwiback](http://www.bsi.bund.de/dok/zwiback)

**10 Jahre Allianz für  
Cyber-Sicherheit**



# 10 Jahre Allianz für Cyber-Sicherheit

**Europas größte Public-private-Partnership im Bereich Cyber-Sicherheit für die Wirtschaft  
feiert zehnjähriges Jubiläum**

*von Agnieszka Pawlowska, Referat Cyber-Sicherheit für die Wirtschaft und Allianz für Cyber-Sicherheit*

Die IT-Sicherheit der deutschen Wirtschaft ausbauen und ihre Resilienz im Kampf gegen Cyber-Angriffe stärken – diese Idee steht hinter der Allianz für Cyber-Sicherheit (ACS). Vor zehn Jahren wurde die ACS vom BSI und dem IT-Branchenverband Bitkom e.V. ins Leben gerufen.

**D**as Risikobewusstsein von Unternehmen in Bezug auf Cyber-Kriminalität wächst. Laut Umfragen zählen Cyber-Angriffe weltweit zu den drei größten Geschäftsrisiken. Auch die finanziellen Schäden für deutsche Unternehmen infolge eines Cyber-Angriffs haben sich mit 223 Milliarden Euro seit 2019 mehr als verdoppelt. Das BSI verdeutlicht in seinem jährlichen Lagebericht die angespannte bis kritische Bedrohungslage.

Als Cyber-Sicherheitsbehörde des Bundes gestaltet das BSI Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Für den Bereich Wirtschaft galt vor

zehn Jahren noch: Unternehmen aus dem Bereich der Kritischen Infrastruktur legten bereits durch ihre existenzsichernde Bedeutung ein besonderes Augenmerk auf die Bedeutung von Informationssicherheit. Ein großer Teil der deutschen Unternehmen, insbesondere kleine und mittlere Unternehmen (KMU), musste erst nach und nach für die Cyber-Sicherheit sensibilisiert werden. Cyber-Angriffe waren in den 2000er-Jahren in den Augen vieler Unternehmensverantwortlicher eine eher abstrakte Bedrohung und der Glaube, das eigene Unternehmen sei zu klein für einen solchen Angriff, war weit verbreitet. Es galt also, die Perspektive der Zielgruppe zu ändern und sie für Risiken zu sensibilisieren.

Der Schlüssel zum Erfolg lag 2011 in der Gründung einer Plattform zum Austausch zwischen dem BSI und den Wirtschaftsunternehmen. Eine Public-private-Partnership sollte die Expertise und Erfahrung des BSI und der Unternehmen in Deutschland bündeln und Prävention mit Best-Practice-Produkten sowie Informationen und Handreichungen vorantreiben.

#### Eine Idee überzeugt – viel Rückenwind für eine Kooperationsplattform

Der Gründungsgedanke der ACS war geboren. Bald fand sich ein starker Partner aus dem privaten Sektor: Gemeinsam mit dem Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien (Bitkom e.V.) konnte das BSI die Idee konkretisieren und anhand von Prüfkriterien kritisch beleuchten.

Außerdem wurde im BSI aus dem damaligen KRITIS-Referat „Schutz Kritischer Infrastrukturen und Cyber-Sicherheit in der Wirtschaft“ eine Projektgruppe gegründet. Diese Ausgründung spiegelt die auch heute noch natürliche Nähe zu dem KRITIS-Bereich wider. Die Erfahrungen mit den Unternehmen, vor allem auch durch den Kooperationskreis UP KRITIS, konnten so in die Aufbauarbeit mit einfließen.

## Allianz für Cyber-Sicherheit



Das Logo der ACS: Ein starkes Netzwerk sendet Cyber-Sicherheit in Richtung Unternehmen in Deutschland

Zu den ersten Ergebnissen gehört die Grundstruktur der ACS, die im Kern noch bis heute Bestand hat, und natürlich der Name: Allianz für Cyber-Sicherheit, kurz ACS. Das Konzept der Teilnehmer und Partner – damals noch Handlungspartner – bietet Unternehmen mit Sitz in Deutschland die kostenlose Möglichkeit zur aktiven Mitgestaltung und Nutzung aller Vorteile der ACS. Unternehmen, Organisationen und Institutionen teilen als Partner ihre Cyber-Sicherheitsexpertise mit dem Netzwerk. Durch ihre Angebote schaffen sie einen Mehrwert für die Teilnehmer und belegen gleichzeitig ihre Fachkompetenz sowie ihr Engagement für das Ziel der ACS: die Erhöhung der Cyber-Sicherheit am Wirtschaftsstandort Deutschland.

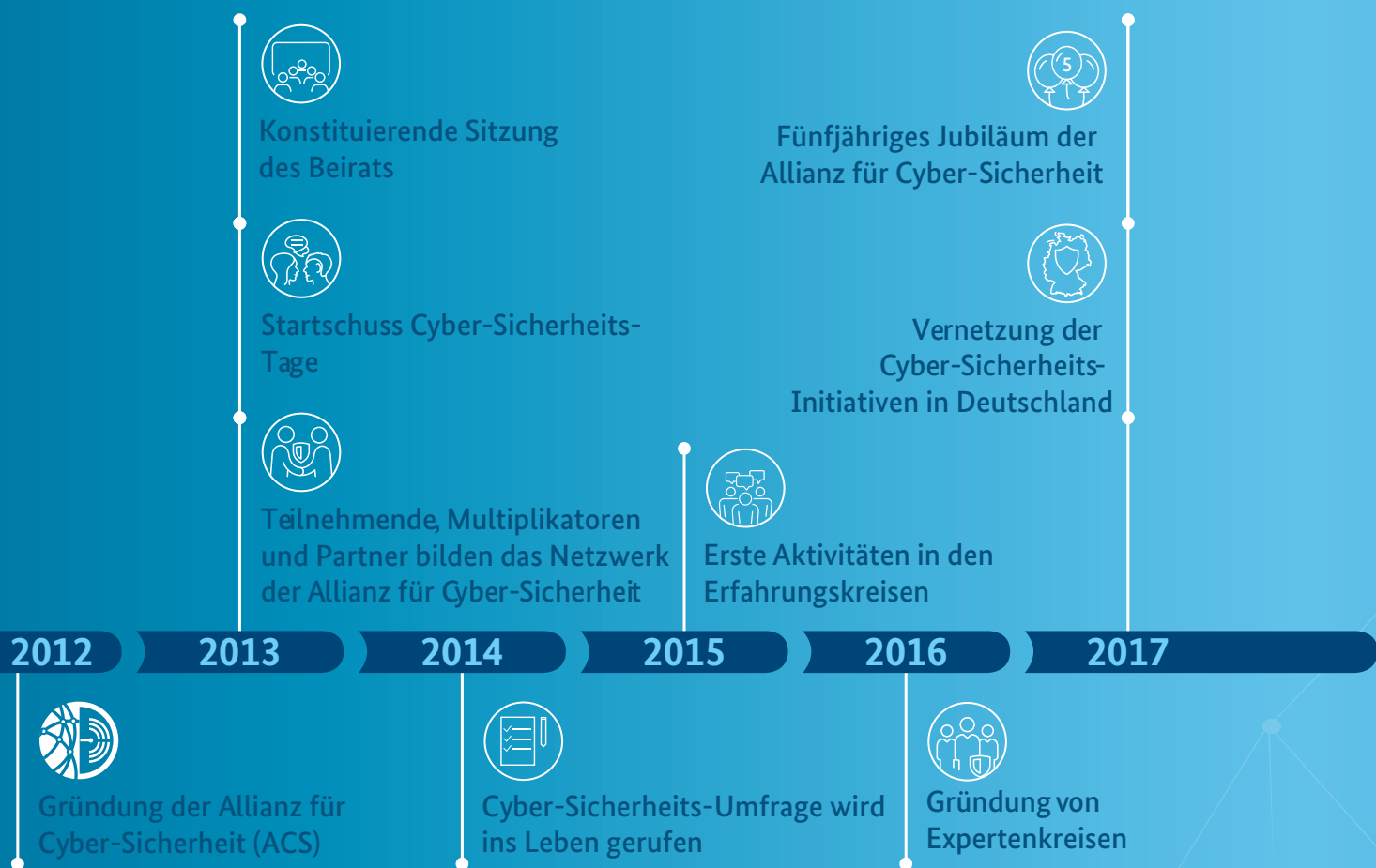


Als Nächstes wurde die Idee der Multiplikatoren entwickelt. Institutionen wie z. B. Verbände, Kammern, Vereine, Initiativen und Netzwerke oder Medienpartner, die sich besonders engagieren möchten, können durch ihren öffentlichkeitswirksamen Einsatz für die ACS die Bedeutung von Cyber-Sicherheitsmaßnahmen unterstreichen. Zudem geben sie Informationen zur Cyber-Sicherheit an die eigenen Mitglieder weiter oder führen Veranstaltungen in Kooperation mit der ACS durch. Sie tragen dazu bei, die Reichweite der ACS in Deutschland zu erhöhen.

Gründungsidee, Konzeption und Ausgestaltung gingen in rasantem Tempo voran. Bereits im Februar 2012 war die ACS bereit für die Pilotphase. Im März 2012 kündigten der damalige BSI-Präsident Michael Hange und der damalige Präsident des Bitkom, Dieter Kempf, auf der CEBIT im März 2012 in Hannover die Gründung der ACS an. Dies erfolgte offiziell auf der it-sa 2012 in Nürnberg im Anschluss an eine erfolgreiche Pilotphase, in der bereits viele Teilnehmer gewonnen und auch erste Partnerbeiträge initiiert werden konnten.

**Netzwerke schützen Netzwerke – durch Informationen, Austausch und Vermittlung von Kompetenzen**  
 Erfolgreiche Präventionsarbeit hängt auch von aktuellen Informationen sowie einem guten Zugang zu diesen ab. Als hierzu wichtiges Instrument wurde die Idee von ACS-Veranstaltungen entwickelt. Diese sollten vor Ort zu aktuellen Cyber-Sicherheitsthemen informieren und den Austausch aller Interessierten fördern. Des Weiteren lag eine vordringliche Aufgabe der Projektgruppe darin, eine Website sowie weitere geeignete Kommunikationsstrukturen zu schaffen, mit denen die Angebote der ACS ihre Zielgruppe erreichen. Seit 2012 stellt die ACS ein breites Informationsangebot sowie tagesaktuelle Warnmeldungen zur Verfügung. Zusätzlich bieten monatliche Lagebilder im Mitgliederbereich der Website Informationen zur Bedrohungslage in Deutschland. So können Unternehmen schneller auf Cyber-Risiken reagieren und unternehmensschädliche Auswirkungen mindern.

Ein weiteres Herzstück der ACS-Webseite ist der Informationspool. Beiträge des BSI und Publikationen von ACS-Partnern tragen durch praktische Tipps und Hilfe-



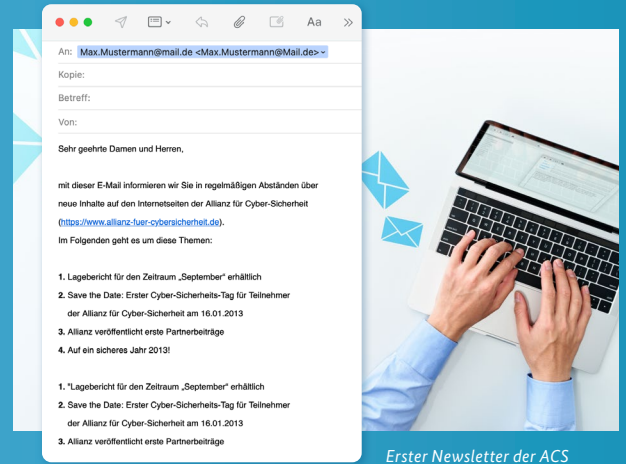
stellungen zur Erhöhung des Cyber-Sicherheitsniveaus bei. Speziell für den Infopool wurde das kompakte Format der Cyber-Sicherheits-Empfehlungen (CS-Empfehlungen) entwickelt.

Eine der ersten Empfehlungen war beispielsweise die BSI-CS 002, ein Papier mit Sofortmaßnahmen zur Abwehr von DDoS-Angriffen.

Kurze Zeit später wurde ein weiterer Kommunikationskanal etabliert, um neben der Website die Zielgruppe der ACS besser anzusprechen. Am 30. November 2012 wurde zum ersten Mal der Newsletter der ACS verschickt. Die ersten Artikel wurden händisch per Mail verschickt, an maximal 200 Empfängerinnen und Empfänger auf einmal. Dies wäre heutzutage bei einem Empfängerkreis von über 8.000 Kontakten nicht mehr denkbar.

Die Themen des ersten Newsletters umfassten bereits die Kernangebote, die die ACS bis heute kennzeichnen: Prävention durch Information und aktuelle Lagebilder, der vertrauensvolle Austausch in verschiedenen Formaten sowie die Vermittlung von Kompetenzen, beispielsweise durch Partnerangebote.

2012 startete die Allianz für Cyber-Sicherheit ihre Erfolgsgeschichte. In der Startphase, Februar 2012, gab es 56



angemeldete Teilnehmende, ein Jahr später bereits 574. Bis zum heutigen Tag hat sich die ACS rasant entwickelt. Heute ist sie mit über 6.000 Teilnehmenden die größte Public-private-Partnership in Europa.

Weitere Informationen:



[https://www.allianz-fuer-cybersicherheit.de/Web/ACS/DE/Informationen-und-Empfehlungen/Informationspool/informationspool\\_formular.html?nn145680](https://www.allianz-fuer-cybersicherheit.de/Web/ACS/DE/Informationen-und-Empfehlungen/Informationspool/informationspool_formular.html?nn145680)



# „Damit wir die richtigen Signale senden können, müssen wir zuhören“

Interview mit Harald Niggemann, Bundesamt für Sicherheit in der Informationstechnik



**Dr. Harald Niggemann** ist Cyber Security Strategist beim Bundesamt für Sicherheit in der Informationstechnik (BSI). Er befasst sich mit Grundlagen und strategischen Fragestellungen der Cyber-Sicherheit und hat die Anfänge der ACS von der ersten Stunde an begleitet.

**2012 wurde die ACS gegründet. Was war und ist die Idee hinter dieser Initiative?**

Cyber-Sicherheit betrifft alle Gesellschaftsbereiche und kann deshalb nur erfolgreich sein, wenn der Staat gemeinsam mit der Wirtschaft und der Zivilgesellschaft diese Herausforderung angeht. Im Bereich des Schutzes der Kritischen Infrastrukturen hatte das BSI ja bereits mit dem UP KRITIS sehr gute Erfahrungen hinsichtlich der Vernetzung mit privatwirtschaftlichen Akteurinnen und Akteuren gesammelt. Öffentlich-private Partnerschaften leisten einen wesentlichen Beitrag dazu, ein gemeinsames Verständnis für das Themenfeld zu schaffen, den Informationsfluss zu verbessern und Erfahrungen auszutauschen, um nur drei von vielen Aspekten zu nennen. Hinter der Gründung der Allianz für Cyber-Sicherheit stand daher die Erkenntnis, dass sich die gesellschaftliche Vernetzung des BSI nicht auf die Kritischen Infrastrukturen beschränken darf. Das BSI brauchte eine Vernetzungsplattform, die offen für alle deutschen Akteurinnen und Akteure ist. Dabei wurde schnell klar, dass wir zwar Anleihen beim UP KRITIS nehmen konnten, aber das Konzept ließ sich nicht direkt auf eine solche breite Plattform übertragen. Eine Erweiterung des UP KRITIS schied somit aus, und die Allianz für Cyber-Sicherheit wurde als neue und ergänzende Plattform ins Leben gerufen.

**Wer aus dem BSI war an der Gründung der ACS beteiligt?**

Als Leiter der damaligen Abteilung „Cyber-Sicherheit“ hat Dr. Hartmut Isselhorst den Aufbau der Allianz für Cyber-Sicherheit initiiert und in der ersten Zeit seitens des BSI maßgeblich vorangetrieben. Gerade am Anfang waren natürlich viele Fragen offen, daher haben wir Unterstützung aus unterschiedlichen Bereichen des BSI gesucht und auch gefunden. Als Beispiele sind hier sicherlich die Bereiche Sicherheitsberatung, Technikrends, operative Cyber-Sicherheit und IT-Grundschutz zu nennen. Mit den Aufbauarbeiten wurde das damalige KRITIS-Referat beauftragt. Mitentscheidend für die erfolgreiche Startphase war zudem die Unterstützung aus dem Referat für Presse- und Öffentlichkeitsarbeit. Ohne diese breite Zusammenarbeit wäre es uns nicht gelungen, die Initiative mit Leben zu füllen und eine „Marke“ zu etablieren. Schließlich mussten auch Ressourcen bereitgestellt werden, und das BMI hat die Arbeiten ebenfalls mit Interesse verfolgt. Deshalb war es natürlich wichtig, dass auch die Amtsleitung und unsere Verwaltungsabteilung hinter der Initiative standen. Darüber hinaus haben sich zahlreiche weitere Kolleginnen und Kollegen aus dem BSI aktiv in die Allianz für Cyber-Sicherheit eingebracht.

**Welchen Herausforderungen musste sich die ACS zu Beginn stellen und wie hat die Wirtschaft auf diese neue Initiative reagiert?**

Eine der großen offenen Fragen zu Beginn war: Wie erreichen wir unsere zukünftigen Zielgruppen? Es gibt in Deutschland mehrere Millionen Unternehmen und viele andere Organisationen. Nur ein Prozent dieser Akteure an die ACS zu binden, wäre ein zu ambitioniertes Ziel gewesen. Glücklicherweise waren wir mit dieser Herausforderung nicht allein, sondern konnten auf die Erfahrung und die Unterstützung des IT-Branchen-

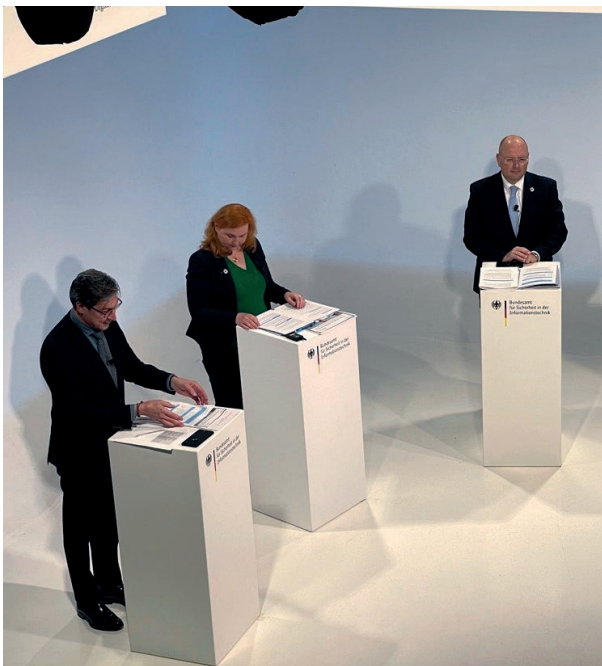


verbands Bitkom zurückgreifen, den wir frühzeitig als Gründungspartner gewinnen konnten. Dieser Schulterschluss hat uns nach vorne katapultiert, denn wir konnten plötzlich das riesige Netzwerk von Bitkom für die ACS nutzen. Dazu gehörten auch die Kontakte des Bitkom zum Bundesverband der Deutschen Industrie (BDI) und zu anderen Branchenverbänden. Bitkom und BSI sind in der Folge bei zahlreichen Anlässen gemeinsam für die ACS eingetreten und konnten auf diese Weise frühzeitig einen vergleichsweise hohen Bekanntheitsgrad der ACS erzielen.

Eine weitere wichtige Frage war, wie die ACS mit existierenden Initiativen mit ähnlicher Zielsetzung umgehen sollte. Aus meiner persönlichen Sicht war es damals entscheidend, dass die ACS sehr klar als integrierende Plattform und nicht als Konkurrenz zu bestehenden Strukturen aufgetreten ist. Existierende Initiativen konnten mit Hilfe der ACS ihre Reichweite und ihr Leistungsangebot verbessern, ohne befürchten zu müssen, die mühsam aufgebauten Vertrauensverhältnisse aufgeben zu müssen. Dies hat die Akzeptanz sicherlich gefördert.

#### ***Woran erinnern Sie sich, wenn Sie an die Anfänge der ACS denken?***

Ich war im Jahr 2012 Strategiereferent von Dr. Isselhorst. Dabei war es oft meine Aufgabe, den Advocatus Diaboli zu spielen, also mögliche Gegenargumente bei unseren Planungen vorzutragen, damit das Konzept möglichst tragfähig wird. Meine Erinnerungen an die ACS sind deshalb geprägt von vielen großen Mindmaps und von Arbeits-sitzungen gemeinsam mit Bitkom. Als dann irgendwann die ersten Flyer mit ACS-Logo auf dem Tisch lagen, waren sowohl Begeisterung als auch Erleichterung spürbar.



Pressekonferenz zur Vorstellung der BSI-Wirtschaftsumfrage im April 2021: Pressesprecher Matthias Gärtner, ACS-Mitarbeiterin Agnieszka Pawlowska und BSI-Präsident Arne Schönbohm (v.l.n.r.)

#### ***Was waren die ersten Produkte und Formate der ACS?***

Um in Vorleistung zu gehen und andere Organisationen anzuregen, selbst Beiträge in die ACS einzuspeisen, haben wir bereits relativ früh über den Informationspool nachgedacht. Durch das bestehende umfangreiche Informationsmaterial des BSI konnten wir eine Grundausrüstung bereitstellen, die dann durch die Beiträge der Partnerorganisationen ergänzt wurde. Voraussetzung dafür war natürlich ein geeigneter Webauftritt der ACS mit durchsuchbarem Dokumentenkatalog. Durch ein gemeinsames Projekt mit der BSI-Öffentlichkeitsarbeit konnte der Webauftritt zeitnah realisiert und sukzessive mit erweiterten Funktionen ausgestattet werden.

Ebenfalls sehr früh konzipiert wurden eigene Veranstaltungen der ACS. Unterschieden haben wir hierzu zwischen großen, breit aufgestellten Tagungen einerseits und regionalen bzw. themenbezogenen Kreisen andererseits. Dabei haben wir uns sicherlich auch von den Erfahrungen des UP KRITIS leiten lassen. Die Definition der Rollen „Partner“ und „Multiplikator“ war dann eine logische Folgerung aus den ersten Schwerpunkten „Informationspool“ und „Veranstaltungen“.

#### ***Die ACS hat sich rasant entwickelt. Aktuell sind es rund 6.000 Teilnehmende. Wie haben Sie sich im Gründungsjahr die Zukunft der ACS bei ihrem zehnjährigen Jubiläum vorgestellt?***

Die Informationstechnik und die Informationssicherheit sind sehr schnelllebige Gebiete. Es gibt viele Initiativen, die kommen und gehen. Der größte Erfolg der ACS ist es deshalb aus meiner persönlichen Sicht, dass es die ACS heute noch gibt! Das beweist für mich, dass sie einen tatsächlichen Bedarf deckt, dass das Konzept tragfähig ist und dass viele Teilnehmende dadurch einen echten Mehrwert erzielen. Die Zahl von mehr als 6.000 Teilnehmenden ist natürlich ebenfalls ein beeindruckender Erfolg, mit dem ich vor zehn Jahren sicherlich nicht gerechnet habe. Vielleicht war es auch gut, dass wir uns damals gar nicht so sehr mit der fernen Zukunft beschäftigt, sondern uns auf die aktuellen praktischen Fragen konzentriert haben. Die pragmatische Zusammenarbeit, sowohl abteilungsübergreifend im BSI als auch gemeinsam mit Bitkom, war aus meiner Sicht ein wesentlicher Erfolgsfaktor.

#### ***Was möchten Sie der ACS noch mit auf den Weg geben?***

Das BSI hat viele Formate, mit denen es Signale an Wirtschaft und Gesellschaft sendet, beispielsweise die Zertifizierung, die Lageberichte, den IT-Grundschutz oder die Technischen Richtlinien etc. Damit wir aber die richtigen Signale senden können, müssen wir auch zuhören. Nur wenn wir Bedarfe, Probleme und Feedback kennen, können wir dauerhaft gute Lösungen bereitstellen. Neben den vielen anderen Vorteilen, die die ACS bietet, ist sie für mich auch eine gute Plattform, um das Feedback der Wirtschaft und der Gesellschaft entgegenzunehmen. Ich wünsche der ACS, dass sie diese wichtige Aufgabe auch in Zukunft wahrnimmt. ■



**VERHALTEN BEI IT-NOTFÄLLEN**

**Ruhe bewahren & IT-Notfall melden**  
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:  
\_\_\_\_\_

Wer meldet?  
\_\_\_\_\_

Welches IT-System ist betroffen?  
\_\_\_\_\_

Wie haben Sie mit dem IT-System gearbeitet?  
Was haben Sie beobachtet?  
\_\_\_\_\_

Wann ist das Ereignis eingetreten?  
\_\_\_\_\_

Wo befindet sich das betroffene IT-System?  
(Gebäude, Raum, Arbeitsplatz)  
\_\_\_\_\_

**Verhaltenshinweise**

Weitere Arbeit am IT-System einstellen  
Beobachtungen dokumentieren  
Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

**Was tun bei einem IT-Notfall? Mit der IT-Notfallkarte haben Sie die ersten Schritte griffbereit.**  
Der Dialog der Cyber-Sicherheits-Initiativen reagiert auf die große Nachfrage: Die IT-Notfallkarte gibt es in den Sprachen Englisch, Spanisch, Französisch, Italienisch, Polnisch, Türkisch, Mandarin und Vietnamesisch.

### Zehn Jahre ACS – zehn Jahre starke Netzwerke

In den Gründungspapieren der ACS heißt es: „Die Cyber-Sicherheitslage ist kritisch. Erforderlich ist ein gemeinschaftliches Handeln, um dieser Bedrohung in der Breite geeignete Maßnahmen entgegenzusetzen.“ Dieses gemeinschaftliche Handeln, die Kooperation von Staat, Wirtschaft und Forschung, bildet den Kern der Allianz für Cyber-Sicherheit.

Dieser kooperative Ansatz fußt auf drei Säulen: Informationen erhalten, Erfahrungen austauschen, Kompetenzen erwerben. Darauf baut die Allianz für Cyber-Sicherheit bis heute ihre Arbeit auf.

### Geballte Cyber-Sicherheit unter dem Dach der ACS

Teilnehmende profitieren vom gesammelten Wissen des Netzwerks und dem vertrauensvollen Erfahrungsaustausch. Außerdem können sie durch zahlreiche Partnerangebote Cyber-Sicherheitskompetenzen erwerben und ausbauen. Über die zahlreichen Kommunikationskanäle wie die Website, den Newsletter, Social Media und auch den Podcast CYBERSNACS erhalten Interessierte ein breites Informationsangebot.

In themenbezogenen Erfahrungskreisen können sich IT-Verantwortliche mit anderen Cyber-Sicherheitsexpertinnen und -experten austauschen. Beim Dialog der Cyber-Sicherheits-Initiativen treffen sich bereits seit 2017 regelmäßig deutsche IT-Sicherheits-Initiativen unter der Federführung der ACS, um mögliche gemeinsame Projekte und Synergieeffekte zu identifizieren.

In diesem Rahmen wurde beispielsweise 2019 ein „Service-Paket“ für das IT-Notfallmanagement entwickelt. Auf besonders großes Interesse stieß hierbei die IT-Notfallkarte.

Ein weiteres Highlight aus der Veranstaltungsreihe der ACS sind die deutschlandweit stattfindenden Cyber-Sicherheits-Tage (CST). Jede Veranstaltung befasst sich mit einem aktuellen Thema der Cyber-Sicherheit wie Industrial

Security oder Digitalisierung am Arbeitsplatz. In Fachvorträgen kann das einzelne Thema aus unterschiedlichen Blickwinkeln beleuchtet und ggf. in begleitenden Kurzworkshops oder Diskussionsrunden vertieft werden. Großzügige Kommunikationspausen bieten viele Möglichkeiten zur Stärkung des Netzwerkes. Die Cyber-Sicherheits-Tage finden in Kooperation mit den Multiplikatoren der ACS an wechselnden Standorten im gesamten Bundesgebiet statt. Auf dem ersten Cyber-Sicherheits-Tag in Bonn im Jahr 2013 wurde das erste Partnerangebot der ACS vorgestellt. Seit 2014 fanden pro Jahr mindestens vier Cyber-Sicherheits-Tage mit jeweils bis zu 200 Teilnehmerinnen und Teilnehmern statt. Dabei stach der 29. Cyber-Sicherheits-Tag besonders hervor. Er richtete sich vor allem an die Multiplikatoren der Allianz. Gemeinsam mit dem Deutschen Industrie- und Handelskammertag lud die ACS zur Veranstaltung im Haus der Deutschen Wirtschaft ein. Über 330 Vertreterinnen und Vertreter nahmen daran teil und besuchten die Ausstellungsstände im Rahmen des European Cyber Security Month (ECSM).

Die ACS arbeitet stets daran, ihre Formate weiterzuentwickeln. Zu Beginn der Coronapandemie wurde deswegen nach neuen Veranstaltungsmöglichkeiten gesucht. Dabei haben sich die digitalen Cyber-Sicherheits-Web-Talks als Erfolgsmodell erwiesen. Mitglieder der ACS sprechen hier mit Expertinnen und Experten aus Wirtschaft und Forschung in kurzen Web-Seminaren über Cyber-Sicherheitsthemen, wie beispielsweise sichere Backups oder auch Schwachstellen-Management.

### Weitere Informationen zum zehnjährigen Jubiläum der ACS:



<https://www.allianz-fuer-cybersicherheit.de/zehnjahre>

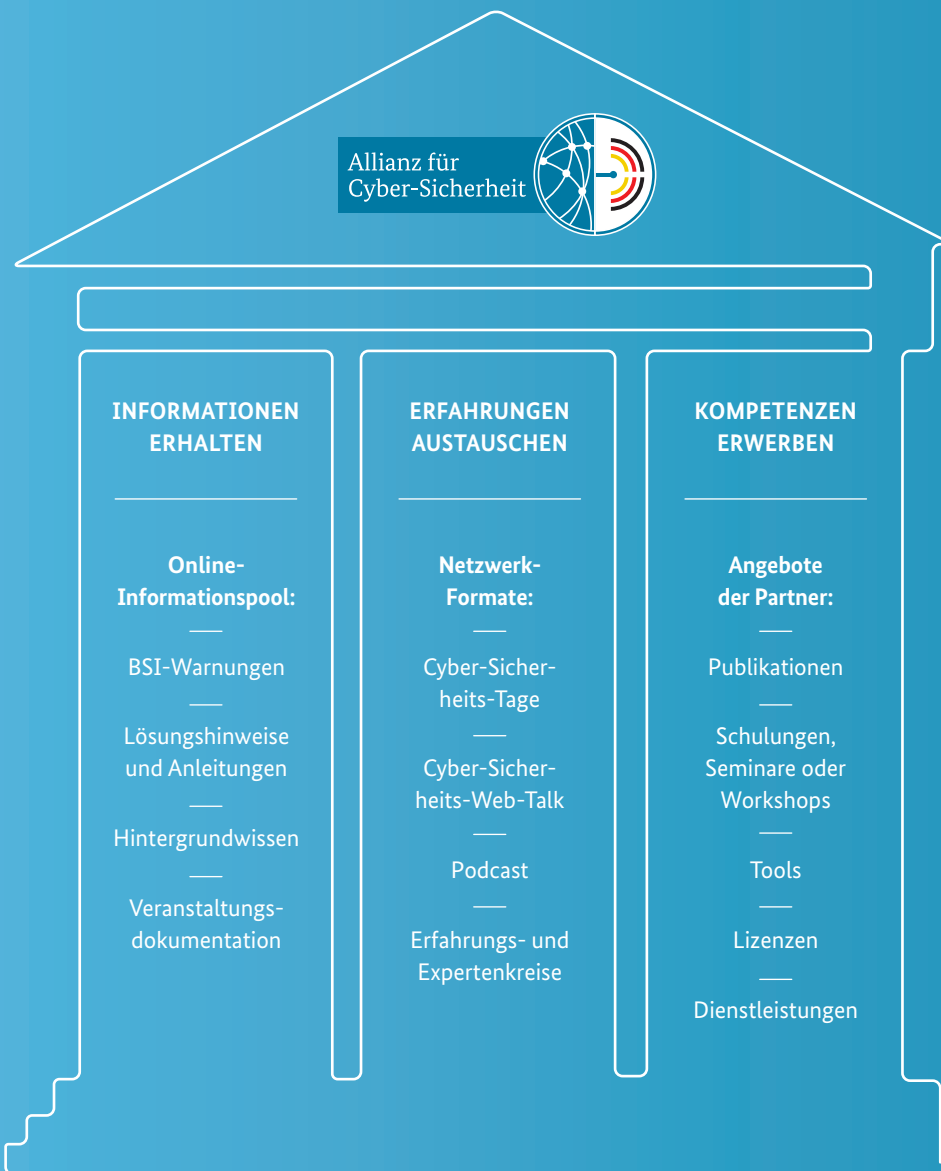
Zum zehnjährigen Jubiläum hat die ACS ihr Leitbild formuliert:

*„Unsere Vision ist Cyber-Sicherheit auf die Straße zu bringen. Durch mehr Thought Leadership und zielgerichtete Hilfe zur Selbsthilfe wollen wir unsere Wirkungsmöglichkeiten verstärken – in Deutschland und international.“*

Die digitalen Bedrohungen nehmen seit der Anfangszeit der ACS an Intensität und Professionalisierungsgrad zu.

Wirtschaftstreibende, die sich jetzt mit Cyber-Sicherheit beschäftigen, tragen dazu bei, das eigene Unternehmen dauerhaft zu sichern. Denn es ist mehr denn je an der Zeit, die eigenen Schutzschilde hochzunehmen und in die Cyber-Sicherheitsprävention zu investieren.

Hierbei unterstützt das gesamte Netzwerk: Teilnehmer, Partner, Multiplikatoren und Mitarbeitende der ACS-Geschäftsstelle arbeiten mit Blick auf die Zukunft daran, den gemeinsamen Wissensschatz allen Interessierten zur Verfügung zu stellen und kontinuierlich weiterzuentwickeln. ■



Teilnehmer werden:



<https://www.allianz-fuer-cybersicherheit.de/registrierung>

Cyber-Sicherheits-Web-Talk:



<https://www.allianz-fuer-cybersicherheit.de/webtalk>

# Einsatz für eine cyber-sichere Zukunft im Handwerk

Interview mit Stephan Blank, Zentralverband des Deutschen Handwerks, Fachbeirat ACS



**Stephan Blank**, Diplom-Wirtschaftsingenieur und Master of Business Administration (MBA), ist seit 2016 Referatsleiter für Digitalisierung im Zentralverband des Deutschen Handwerks. Der Digitalisierungs- und Innovationsexperte gestaltet in seiner Funktion als Konsortialleiter im Mittelstand-Digital Zentrum Handwerk die digitale Transformation im Handwerk aktiv mit.

## **Die Arbeit der ACS wird durch einen Beirat begleitet. Wie ist der Beirat zusammengesetzt und was ist seine Funktion?**

Im Beirat der ACS sind zahlreiche Spitzenverbände und Organisationen der deutschen Wirtschaft vertreten. Gemeinsam bilden sie ein starkes Netzwerk für Cyber-Sicherheit und bringen die Expertise ihres Wirtschaftszweigs und die Bedarfe der Unternehmen in die Allianz mit ein. Hier kommen Stakeholder aus allen Bereichen der deutschen Wirtschaft zusammen und gestalten die strategische Ausrichtung der ACS mit – aus ganz unterschiedlichen Perspektiven. Das fördert den Erfahrungsaustausch untereinander und über die eigenen Branchengrenzen hinweg und schmiedet zugleich neue Allianzen für mehr Cyber-Sicherheit in der deutschen Wirtschaft.

## **Sie sind als Fachbeirat Teil der ACS. Was macht der Fachbeirat?**

Der Fachbeirat setzt die strategischen Ziele des Beirats um und gestaltet unterjährig das Arbeitsprogramm der ACS mit. Die verschiedenen Perspektiven, Erfahrungswerte und Kompetenzen der Fachbeiräte tragen zu einem multilateralen Austausch innerhalb der Allianz bei. Darüber hinaus unterstützen die Fachbeiräte die ACS bei der Entwicklung praxisnaher Angebote für mehr Cyber-Sicherheit in der Wirtschaft.

Der Zentralverband des Deutschen Handwerks (ZDH) engagiert sich dabei für die Interessen und Bedarfe des Handwerks – sowohl die der Handwerksorganisationen als auch die der über eine Million Handwerksbetriebe.

## **Welches Projekt, das Sie bisher mit der ACS realisiert haben, war Ihr „Lieblingsprojekt“?**

BSI und ZDH verbindet durch das gemeinsame Engagement im Rahmen der ACS eine langjährige Partnerschaft, in der Projekte umgesetzt, Veranstaltungen durchgeführt und verschiedene Angebote für das Handwerk geschaffen wurden. Unser „Lieblingsprojekt“ ist der Routenplaner für Cyber-Sicherheit im Handwerk. Das ist ein praxisorientierter Leitfaden mit Handlungsempfehlungen aus dem IT-Grundschutzprofil für Handwerksbetriebe des BSI. Der Routenplaner wurde im März 2019 veröffentlicht und ist inzwischen ein bewährtes Instrument, insbesondere in der handwerklichen Beratung kommt er zum Einsatz und auch Handwerksbetriebe analysieren mit dem Routenplaner den Status ihrer Cyber-Sicherheit. Als Printbroschüre war der Routenplaner so erfolgreich, dass er inzwischen weiterentwickelt wurde und Handwerksbetrieben und den Beraterinnen und Beratern der Handwerksorganisationen nunmehr als interaktives Onlinetool zur Verfügung steht.

## **Welche Cyber-Sicherheitsthemen finden Sie aktuell für die Wirtschaft besonders relevant?**

Die Bedrohungslage nimmt stetig zu, denn Cyber-Angriffe laufen mehr und mehr automatisiert ab. Es sind längst nicht mehr nur die großen Fische im Visier von Cyber-Kriminellen, sondern zunehmend auch kleinere Unternehmen, denen im Zweifel keine IT-Sicherheitsbeauftragten oder informationstechnischen Sicherheitskonzepte zur Verfügung stehen und die damit schneller zur Zielscheibe werden. Das verunsichert viele kleinere



und mittlere Unternehmen und macht Cyber-Sicherheit zu einem der größten Hemmnisse, wenn es darum geht, Digitalisierungsmaßnahmen im eigenen Unternehmen umzusetzen.

Insbesondere im Handwerk geht es meines Erachtens vorrangig darum, Hemmnisse und Berührungspunkte gegenüber dem Thema abzubauen und Handwerksbetriebe bei der Umsetzung von Cyber-Sicherheitsmaßnahmen nicht allein zu lassen, sondern sie dabei zu unterstützen! Getreu dem Motto: Digitalisierung meines Unternehmens, aber sicher!

Daher sind niedrigschwellige Angebote und praxisnahe Lösungen, wie beispielsweise der Routenplaner Cyber-Sicherheit, die Notfallkarte der ACS oder verschiedene Checklisten, auch künftig wichtige Instrumente, um die Cyber-Sicherheit im Handwerk zu erhöhen, und somit auch für unsere Arbeit relevant.

#### **Welcher Zukunftsthemen soll sich die ACS annehmen?**

Wichtige Zukunftsthemen wie Künstliche Intelligenz, Robotik, Drohnen, Smarthome oder Internet of Things bewegen die Wirtschaft und werden ihre Zukunft formen. Auch das Handwerk wird sich zunehmend mit diesen Technologien auseinandersetzen müssen, wenn es auch künftig wettbewerbsfähig bleiben möchte.

Wenn also digitale Technologien, eingebettet in cyber-physische Systeme, zunehmend Einzug in die Wirtschaft finden, müssen die Unternehmen das Thema Cyber-Sicherheit von der ersten Minute mitdenken (Stichwort: Security by Design). Dafür benötigen gerade kleine Unternehmen die Unterstützung der ACS, die mit konkreten Angeboten, Sicherheitskonzepten und einem starken Netzwerk eine praxisnahe Begleitung der Unternehmen bei der Erhöhung ihres Schutzgrads gewährleisten kann.

#### **Wagen wir einen Blick in die Zukunft: Wie sieht die ACS bei ihrem 20-jährigen Bestehen aus?**

Die Allianz wird weitere Mitglieder willkommen heißen und so über ein noch stärkeres und größeres Netzwerk verfügen, dem sich zahlreiche Unternehmen und Multiplikatoren angeschlossen haben, um gemeinsam Angebote für eine cyber-sichere Zukunft der deutschen Wirtschaft zu entwickeln.

#### **Was möchten Sie der ACS noch mit auf den Weg geben?**

Wir wünschen der ACS auch für die Zukunft das Allerbeste und freuen uns über das erfolgreiche Fortbestehen und eine Intensivierung unserer Zusammenarbeit. Und wir wünschen uns, dass auf die bisher entwickelten Angebote wie den Routenplaner und die Cyber-Sicherheits-Tage für das Handwerk noch viele weitere gemeinsame und erfolgreiche Projekte folgen. ■

# „Packen wir es an, gemeinsam!“

**Interview mit Sebastian Artz, Bitkom e.V., Fachbeirat ACS**



Als Bereichsleiter für Cyber- und Informationssicherheit verantwortet **Sebastian Artz** die inhaltliche Arbeit des Bitkom rund um den Schutz und die Absicherung Kritischer Infrastrukturen, 5G- und Cloud-Sicherheit, Sicherheitstechnologien, ISMS, Verschlüsselung, Wirtschafts- und Geheimschutz, digitale Souveränität sowie die Cyber-Sicherheitsarchitektur.

**Die Arbeit der Allianz für Cyber-Sicherheit (ACS) wird durch einen Beirat begleitet. Wie ist der Beirat zusammengesetzt und was ist seine Funktion?**

Der Beirat bündelt die Perspektiven von erfahrenen Expertinnen und Experten aus unterschiedlichen Branchen. Damit dient der Beirat als wichtiges Gremium, um die Unternehmenswirklichkeit in der gesamtwirtschaftlichen Breite in den Aktivitäten und Angeboten der ACS berücksichtigt zu wissen. Gleichzeitig fungiert der Beirat als Takt- und Impulsgeber, immer mit dem klaren Ziel vor Augen, wirksame Unterstützungsangebote bereitzustellen und der gesamten Wirtschaft Orientierung beim Thema Cyber-Sicherheit zu geben.

**Sie sind als Mitglied des Fachbeirats Teil der ACS. Was macht der Fachbeirat?**

Als Fachbeirat sind wir quasi das Spiegelbild des Beirats auf Fachebene. Ausgerichtet an den vom Beirat vorgegebenen Leitplanken planen wir gemeinsam unsere Veranstaltungen und übernehmen die fachliche Ausgestaltung. Unser Ziel ist es, den Beirat bestmöglich zu unterstützen und die verschiedenen Vorhaben voranzubringen.

**Welches Projekt, das Sie bisher mit der ACS umgesetzt haben, war Ihr „Lieblingsprojekt“?**

Für mich ist es vor allem die Summe aus den vielen unterschiedlichen Formaten, die die ACS auszeichnet. Egal ob Fachvorträge, thematische Eventtage, neue Podcast-Folgen oder aktuelle Infos zur Bedrohungslage im Cyber-Raum, für alle ist etwas Neues und Wissenswertes dabei. Persönlich hat es mir beispielsweise viel Freude gemacht, gemeinsam mit unserer ACS am Safer Internet Day ein Schwerpunktformat zur Rolle und Relevanz des Verhaltens von Privatpersonen und Mitarbeitenden im Cyber-Raum zu veranstalten.

**Welche Cyber-Sicherheitsthemen finden Sie aktuell für die Wirtschaft besonders relevant?**

Das bestimmende Thema ist die Gefahr von Ransomware-Angriffen. Im Endeffekt ist es aber unerheblich, ob die Kriminellen per Phishing, Supply-Chain-Angriff oder über 0- oder N-Day-Schwachstellen, fehlkonfigurierte Cloud-Umgebungen, Schatten-IT oder Innentäterinnen und Innentäter zum Ziel kommen. Die kriminelle Energie findet ihren Weg. Deshalb ist es entscheidend, dass sich die Unternehmen bestmöglich auf den Ernstfall vorbereiten, indem sie sich proaktiv und präventiv mit dem Thema Cyber-Sicherheit auseinandersetzen. Und genau hier setzen wir als ACS an.

**Welcher Zukunftsthemen sollte sich die ACS annehmen?**

Cyber-Sicherheit ist keine einmalige Aufgabe oder ein zu erreichender Zustand, sondern ein kontinuierlicher Prozess. Deshalb müssen wir uns darauf konzentrieren, praxisnahe Angebote immer auf der Höhe der Zeit für unser Netzwerk bereitzustellen. Unsere Aufgabe ist es, das Cyber-Sicherheitsniveau in der Breite zu steigern. Auf dieses übergeordnete Ziel müssen all unsere Aktivitäten einzahlen.

**Wagen wir einen Blick in die Zukunft: Wie sieht die ACS bei ihrem 20-jährigen Bestehen aus?**

Stand heute verfügen wir bereits über das größte Cyber-Sicherheitsnetzwerk Europas und bilden gemeinsam eine enorm wichtige und pulsierende Plattform, nicht nur für den Wissensaustausch, sondern auch ganz konkret für die Unterstützung von kleinen und mittleren Unternehmen zur Verbesserung ihrer digitalen Abwehrkräfte. In den nächsten zehn Jahren wird unsere Allianz weiterwachsen und noch stärker werden. Denn in Anbetracht der sich verschärfenden Bedrohungslage im Cyber-Raum ist die wichtigste Geste nicht der erhobene Zeigefinger, sondern die ausgestreckte Hand.

**Was möchten Sie der ACS noch mit auf den Weg geben?**

Ich könnte mir gut vorstellen, den Aufbau einer ganzheitlichen Sicherheitskultur in Unternehmen verstärkt auf die Agenda zu heben. Praxisnahe Hilfestellungen und Erfolgsgeschichten könnten einen echten Mehrwert für den Kreis der Teilnehmenden der ACS leisten. So oder so liegt noch viel Arbeit vor uns. Packen wir es an, gemeinsam! ■

# Das Cyber-Sicherheitsnetzwerk

## Gemeinsam IT-Sicherheitsvorfälle lösen

von Angelika Jaschob, Referat Kooperation mit Herstellern und Dienstleistern

Das Cyber-Sicherheitsnetzwerk bietet gerade für kleine und mittlere Unternehmen eine wertvolle Unterstützung nach einem IT-Sicherheitsvorfall an. Zusätzlich bieten regionale Foren einen geschützten Raum an, um die Reaktion auf IT-Sicherheitsvorfälle zu trainieren. Mit dem Trainingskoffer werden hierfür erste Trainingseinheiten bereitgestellt.



Broschüre des CSN mit Hilfestellungen für KMU und Bürgerinnen und Bürger

### Das Cyber-Sicherheitsnetzwerk als reaktive Ergänzung der ACS

Im Berichtszeitraum des BSI-Lageberichts 2021 übermittelte das BSI 14,8 Millionen Meldungen zu Infektionen durch Schadprogramme an deutsche Netzbetreiber. Das sind mehr als doppelt so viele wie im Jahr davor.

### Aber ein IT-Sicherheitsvorfall ist kein Tagesgeschäft

Jedes Unternehmen kann sich durch präventive Maßnahmen auf einen IT-Sicherheitsvorfall vorbereiten, die Allianz für Cyber-Sicherheit (ACS) bietet hier ein umfangreiches Portfolio an Maßnahmen. Mit über 6.000 Mitgliedern ist die ACS als Public-private-Partnership (PPP) eine starke Initiative für Unternehmen.

Aber wie gut ist das eigene Unternehmen tatsächlich auf einen IT-Sicherheitsvorfall vorbereitet? Der Selbsttest des Cyber-Sicherheitsnetzwerks (CSN) ermöglicht es gerade kleinen Unternehmen, auf diese Frage eine erste Einschätzung des eigenen Sicherheitsniveaus zu bekommen.

Wenn das eigene Unternehmen trotz guter Sicherheitsmaßnahmen Opfer eines IT-Sicherheitsvorfalls wird, können Helfer des CSN bei der Vorfall-Bearbeitung unterstützen. Das CSN ist ein freiwilliger Zusammenschluss von qualifizierten Helfern, die sich bereit erklären, ihre individuelle Expertise und ihr individuelles Know-how zur Behebung von IT-Sicherheitsvorfällen zur Verfügung zu stellen. So soll das CSN das Angebot der Allianz für Cyber-Sicherheit zukünftig im Bereich „Reaktion“ ergänzen, derzeit befindet es sich noch in der Pilotphase.



## Die Digitale Rettungskette des Cyber-Sicherheitsnetzwerks bietet Unterstützung

Je nach IT-Sicherheitsvorfall stellt sich die Frage: Wer kann wie helfen? Die Broschüre zur Digitalen Rettungskette soll hier Anwendung finden, um nach einem IT-Sicherheitsvorfall an der richtigen Stelle bzw. am richtigen Glied der Kette einzusteigen oder aktiv an das nächste Glied in der Kette zu eskalieren. Dabei erstreckt sich die Digitale Rettungskette von der Unterstützung durch Checklisten über eine telefonische Unterstützung durch Helfer des Cyber-Sicherheitsnetzwerks bis hin zu einem Team von Vorfall-Experten, welches vor Ort tätig werden kann. Mit dem Konzept einer Digitalen Rettungskette arbeiten qualifizierte Helfer aufeinander abgestimmt.

Ein Qualifizierungsprogramm stellt die einheitliche Qualität der Vorfallbearbeitung durch qualifizierte Helfer sicher. Dabei gibt das Cyber-Sicherheitsnetzwerk den Rahmen vor, so dass bei der Vorfallbehandlung ein strukturiertes und nachvollziehbares Vorgehen angewandt wird und die Betroffenen qualifizierte Unterstützung erhalten. Die Webseiten des Cyber-Sicherheitsnetzwerks bieten eine schnelle Übersicht über diese qualifizierten regionalen Helfer.

## Regionale Foren

„Ich könnte ruhiger schlafen, wenn ich einen IT-Sicherheitsvorfall schon einmal üben und außerdem einschätzen könnte, wie meine Mitarbeiter und ich in so einer Stresssituation reagieren würden“, sagte so ein Geschäftsführer eines mittelständischen Unternehmens.

Mit den regionalen Foren bietet das CSN sowohl Unternehmen als auch Helfern die Möglichkeit, in einer gesicherten Umgebung die Bewältigung eines Vorfalls zu trainieren.

Mit dem Trainingskoffer stellt das CSN eine kostenfreie Übungs- bzw. Spielesammlung zur Verfügung.

Der Trainingskoffer ist quasi ein einfaches spielerisches Training für die Vorfallbearbeitung „out of the box“. Er ist so gestaltet, dass die Trainingseinheiten leicht selber erstellt und schnell eingesetzt werden können.

Regionale Foren sind ca. zweistündige Erfahrungsaustauschformate, welche als Frühstücksrunde, Business-Lunch oder als Stammtisch am Abend stattfinden können, und werden in der Regel von erfahrenen Vorfall-Experten organisiert und geleitet. Die regionalen Foren können



regelmäßig sowohl physisch als auch virtuell an einem bestimmten Ort stattfinden. Mit diesem Format können sich insbesondere teilnehmende Unternehmen sowie Digitale Ersthelfer ihre Kompetenz bei der Vorfallbearbeitung im CSN ausbauen und so ihre Kompetenz erweitern.

### Der Trainingskoffer

Der Trainingskoffer enthält unterschiedliche Trainingsformen, neben Brettspielen und Rollenspielen wird auch ein Trainingszirkel mit unterschiedlichen Lernstationen bereitgestellt.

Die Lernstationen bestehen aus kleinen Spielen, sog. Mini-games, die auf einfachen und populären Spielprinzipien basieren. Thematisch decken die Lernstationen vor allem die Themen der Digitalen Rettungskette und die Vorfallbearbeitung eines Digitalen Ersthelfers ab.

Der Trainingszirkel beinhaltet neben einem Warm-up zum Kennenlernen

- » ein Zuordnungsspiel zum Thema IT-Störung vs. IT-Sicherheitsvorfall
- » ein Dominospiel zum Thema Digitale Rettungskette
- » ein Quiz zum Thema Vorfallbearbeitung durch den Digitalen Ersthelfer
- » ein Memospiel zum Thema Vor-Ort-Unterstützung

Wenn bei der Nutzung als Lernstation mehrere Teams teilnehmen, werden Punkte vergeben und ggf. ein Preis ausgelobt, um die Motivation zu steigern und das Zusammenarbeiten im Team zu fördern.



Übungen mit Hilfe von Lernstationen bilden Gesprächsthemen in den regionalen Foren ab und bringen das eher unbeliebte Sicherheits-Thema nach dem Prinzip „Take Security“ in den Austausch. Sie dienen als Teaser, um Themen und Erfahrungen aufzugreifen und zu diskutieren.

Alle Lernstationen können auch online durchgeführt werden und die Trainingseinheiten können auch einzeln, z. B. in Schulungen oder Vorlesungen, integriert werden.



### Ausblick Rollenspiele

Im Trainingskoffer werden neben den freien Trainingseinheiten auch noch unterschiedliche Rollenspiele angeboten.

Hier geht es vor allem darum, dass die Teilnehmer die Vorfallbehandlung in konkreten Situationen trainieren. Jeder Teilnehmer erhält eine Rollenkarte, beispielsweise als Helfer des CSN oder in der Funktion des betroffenen Unternehmens (z. B. Geschäftsführer). Der Forenleiter fungiert als Rollenspielleiter, der den Vorfall kennt und zusätzliche Geschehnisse oder auch Hilfestellungen in das Rollenspiel einbringen kann.

Mit den Rollenspielen bietet das CSN eine gute Möglichkeit, die Vorfallbearbeitung in einer sicheren Umgebung vorab zu trainieren, insbesondere bietet sich für die Teilnehmenden die Möglichkeit des Perspektivwechsels.

Der Trainingskoffer ist modular aufgebaut und kann sowohl durch Forenleiter als auch durch Trainer oder andere Teilnehmer kontinuierlich um weitere Rollenspiele ergänzt werden. Für Themen wie „Ransomware“ oder „Social Engineering“ werden Rollenspiele bereitgestellt. ■





# Vielfalt schafft Mehrwert beim BSI

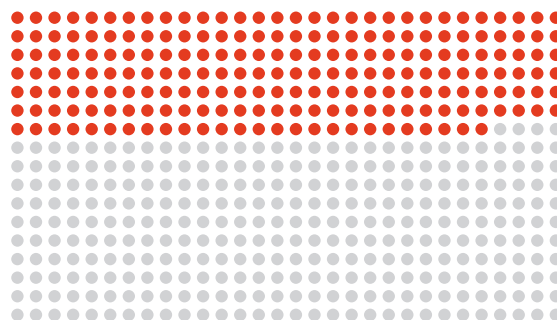
**Diversität in allen Dimensionen leben**

*von Bettina Jäkel-Schmidt, Referat Personalentwicklung*

Im öffentlichen Dienst und in den Unternehmen finden die Themen Vielfalt und Chancengerechtigkeit eine immer größere Beachtung. Während viele Organisationen bereits seit vielen Jahren an einer interkulturellen Öffnung arbeiten, wächst nun auch die Entwicklung von Diversitätskompetenzen. Auch das BSI steht als Wachstumsbehörde im dynamischen Feld der Informationssicherheit gemeinsam mit allen Beschäftigten vor der schönen Herausforderung, Diversität in all ihren Dimensionen mit noch mehr Leben zu füllen. Dabei sollen gezielte und kontinuierliche Maßnahmen im Diversity-Management unter dem Motto #VIELFALTLEBEN eine zukunftsfähige Arbeitskultur unterstützen.



**40 Prozent** der neuen Beschäftigten im BSI sind **Frauen**. Damit steigt der Gesamtanteil von **28,3 Prozent** auf **32,9 Prozent**.



Zuwachs Beschäftigte 2018 bis 2021

**A**uch das BSI arbeitet mit den Zielen des Bundesgleichstellungsgesetzes (BGleig). Alle vier Jahre werden in einem Gleichstellungsplan Ziele und Maßnahmen festgelegt. Unabhängig davon, dass das BSI an das Gesetz gebunden ist, soll der Anteil von Frauen insgesamt erhöht werden. Insbesondere geht es darum, Absolventinnen und Professionals aus MINT-Berufen zu gewinnen. Auch wenn sich gegenwärtig immer mehr junge Frauen für ein Technologie-Studium entscheiden, ist der Bedarf an Frauen mit IT-bezogenen Berufen auf dem Arbeitsmarkt aktuell immer noch sehr hoch. Das BSI entwickelt die Ansprache von Frauen im Personalmarketing kontinuierlich weiter und sieht sich damit auf einem erfolgreichen Weg. Auch strukturell bewegt sich einiges. Zwar lässt sich der Wandel zu vielfältigeren Teams in allen Bereichen nicht von heute auf morgen umsetzen, aber er kommt doch kontinuierlich voran.

Deshalb ist es auch wichtig, dass die bei uns tätigen Frauen im IT-Bereich sichtbare Role-Models sind und in ihrer Karriereentwicklung spezifisch unterstützt werden. Dazu gibt es ein ganzes Bündel an Maßnahmen.

„Diversitätskompetenz ist die Fähigkeit, wertschätzend, anerkennend und vorurteilsfrei mit gesellschaftlicher Vielfalt umzugehen und diese zu gestalten. Hierzu sind die Fähigkeiten zur Selbstreflexion und zum Perspektivwechsel sowie Ambiguitätstoleranz notwendig.“

Aus der Diversitätsstrategie für die Bundesverwaltung, 2021

Beispiel: Sensibilität erzeugen durch Poster zu Führungsleitsätzen



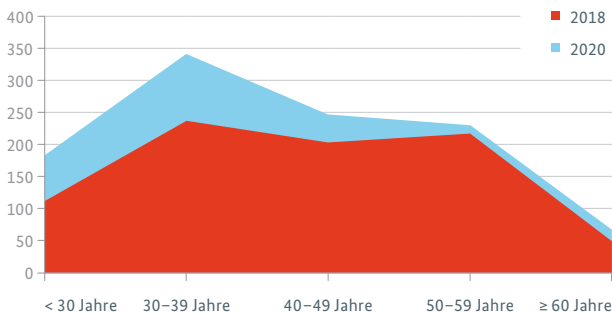
**Dimension: Rollenbilder**

Eine vielfältigere Gesellschaft verändert auch tradierte Rollenbilder. Auch Männer werden im Kontext der Diversität vor spezifische Herausforderungen gestellt: Neue Rollenanforderungen in Partnerschaft und Care-Arbeit werden im BSI sichtbar. Elternzeiten von Vätern werden selbstverständlicher und auch immer länger. Eine besonders erfreuliche Entwicklung: Etwa die Hälfte aller Mitarbeitenden, die in Teilzeit arbeiten, sind Männer.

Es geht nur gemeinsam: Die Einsicht, dass wir mehr Frauen – besonders in Führungspositionen – brauchen, ist nicht nur eine von außen vorgegebene Zielgröße, sondern auch eine überfällige gesellschaftliche Notwendigkeit, die außerdem dabei unterstützen kann, dem Fachkräftemangel zu begegnen. Gemischte Teams sind zudem kreativer und erfolgreicher. Denn vielfältige Teams fördern vielfältige Perspektiven, die einen Mehrwert schaffen. Das erleben wir im BSI jeden Tag.



Mitarbeitende im BSI nach Altersgruppen



**Dimension: Alter**

Das BSI hat eine relativ ausgeglichene Altersstruktur unter seinen Beschäftigten. Im Vergleich zu anderen Behörden, die nicht oder nicht so schnell wachsen, ist das Demografie-Problem der bevorstehenden Altersabgänge der Generation „Babyboomer“ in den kommenden Jahren noch gering. Der Altersdurchschnitt aller Mitarbeitenden im BSI lag Mitte 2020 mit 41,3 Jahren leicht unter dem Durchschnitt der Erwerbsbevölkerung insgesamt. Tendenz: Das BSI wird immer jünger. ■



**Diversity-Highlights im BSI**

- Information, Learnings und Austausch durch das Programm von Employers for Equality und interne 90-Minuten-Diversity-Impulse
- Entwicklung von gendersensiblen Stellenanzeigen, Anforderungsprofilen und Veranstaltungsplanungen
- Gründung women@bsi mit Vernetzungsformaten zu frauenspezifischen Themen
- „PLAY DIVERSITY“ im Einarbeitungsprogramm von Auszubildenden und dualen Studierenden
- Unterzeichnung und Beteiligung „CHARTA DER VIELFALT“, beispielsweise 10. DEUTSCHER DIVERSITY-TAG: Panel „Diversity weiterdenken“
- „JEDE JECK IS ANDERS“ im Karneval, „MEIN EHRENAMT“ zum Tag des Ehrenamts

# Gemeinsam stark – gelebte Vielfalt im BSI

## Interview mit BSI-Präsident Arne Schönbohm

**Auf der Karriereseite des BSI heißt es: Das BSI wird „immer bunter“. Was genau ist damit gemeint?**

Informationssicherheit betrifft heute alle Menschen; egal, ob privat oder beruflich. Um unsere Aufgaben dabei heterogen abbilden zu können, sind viele Sichtweisen, gepaart mit Fachwissen, notwendig. Das BSI-Team ist darum in Bezug auf Vielfaltskriterien wie Alter, Geschlecht oder Interkulturalität inzwischen sehr divers. Durch die unterschiedlichen Hintergründe und Persönlichkeiten bringt unsere Belegschaft verschiedene Perspektiven und unterschiedliche Herangehensweisen in die tägliche Arbeit ein. So wird aus vielen Einflüssen ein ganzheitliches Denken und Agieren und wir können voneinander lernen. Vielfalt macht uns zukunftsfähig.

**Es ist bereits umfassend erforscht, dass diverse Teams bzw. Organisationen erfolgreicher sind. Welche Beispiele gibt es dazu im BSI?**

Unsere Mitarbeitenden nehmen Vielfalt als Stärke wahr. Sie motiviert und prägt unsere Organisationskultur. Im BSI merken wir aber insbesondere: Vielfältige Perspektiven und Ideen bringen gute Synergien, mehr Innovation und bessere Entscheidungsgrundlagen. Ein Beispiel: Unsere neuen Mitarbeitenden aus der Wirtschaft mit ihren spezifischen Berufserfahrungen sorgen für frischen Wind. Gepaart mit der BSI-Erfahrung unserer Langjährigen und verschiedenen Persönlichkeiten, macht dieser Mix den Mehrwert aus. Aber Diversity-Management heißt bei uns auch Steuerung: auf eine diverse Besetzung bei Panels hinwirken, Beurteilungen und Auswahlprozesse sensibel umsetzen. Und wir haben die klare Erwartungshaltung an Führungskräfte, dass sie gleichermaßen wertschätzend mit allen Mitarbeitenden wie auch dem Teamerfolg umgehen. Wir bauen unsere Maßnahmen hier kontinuierlich weiter aus.

**Im letzten Jahr ist das BSI der Charta der Vielfalt beigetreten. Was versprechen Sie sich davon?**

Hier sind wir in guter Gesellschaft mit anderen Behörden und namhaften Unternehmen. Diese Selbstverpflichtung hilft uns dabei, Ziele zu formulieren, und ermöglicht uns, im BSI abgestimmt planvoll vorzugehen. Wir profitieren außerdem von Best-Practice-Beispielen und einem regelmäßigen und gewinnbringenden Austausch. Zudem ist es mir wichtig, nach außen und nach innen eine klare Haltung zu zeigen.

**Was tut die BSI-Leitung, damit Diversity kein Lippenbekenntnis ist?**

Letztlich geht es bei allem, was wir tun, darum, die Vielfaltsbrille aufzusetzen und zu schauen, was wir damit noch besser machen können. Damit sind wir alle auch Lernende. Ich schließe mich dabei nicht aus.

Als Leitung sind wir zudem Vorbild und wollen zugleich ermöglichen: Wir bekennen uns zu einem diskriminierungsfreien und chancengerechten Arbeitsumfeld und erwarten das auch von allen Führungskräften in der täglichen Arbeit mit ihren Teams. Der regelmäßige Dialog und die Sensibilisierung unterstützen hierbei. ■



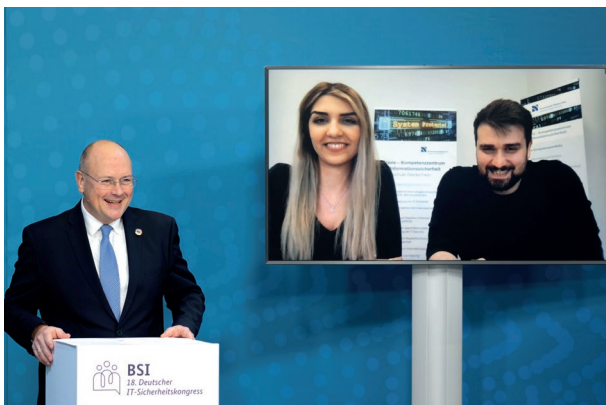
→  
Ralf Wintergerst, Hans Peter Wollseifer, Milen Volkmar, Thomas Rosteck und Arne Schönbohm (v. l. n. r.) diskutierten mit der Moderatorin Claudia Veen in der Podiumsdiskussion das Thema „Cyber-Sicherheit ist Chefinnen- und Chefsache!“



# Impulse für die sichere Digitalisierung Deutschlands

## Der 18. Deutsche IT-Sicherheitskongress

Zwei Tage im Zeichen der Cyber-Sicherheit: Mit mehr als 8.000 angemeldeten Teilnehmerinnen und Teilnehmern war der 18. Deutsche IT-Sicherheitskongress des BSI auch im Jahr 2022 die größte deutsche Veranstaltung zum Thema Cyber-Sicherheit.



Das digitale Veranstaltungsformat des Kongresses bot den Teilnehmenden eine Plattform für den digitalen Austausch zu aktuellen Themen der Cyber-Sicherheit. Auf der digitalen Veranstaltungsplattform wurden am 1. und 2. Februar 2022 auf zwei Bühnen 28 Fachvorträge präsentiert und in drei verschiedenen Podiumsdiskussionen die Themen „Cyber-Sicherheit ist Chefinnen- und Chefsache!“ sowie der „Digitale Verbraucherschutz“ erörtert. Thematische Schwerpunkte in den zahlreichen Fachvorträgen und Diskussionen waren unter anderem sichere 5G-Netze, der Schutz Kritischer Infrastrukturen wie der Energieversorgung, Quantenkryptografie sowie die sichere Digitalisierung

Das Preisträger-Duo des „Best Student Awards“ 2022: Asiye Öztürk und Erfan Koza vom Clavis-Institut für Informationssicherheit der Hochschule Niederrhein

von Staat und Verwaltung. Das Vortragsprogramm wurde durch eine begleitende virtuelle Ausstellung ergänzt. Sie ermöglichte allen Teilnehmenden, mit 21 externen Ausstellern sowie mit BSI-Mitarbeiterinnen und -Mitarbeitern an zwei BSI-Ständen direkt in Kontakt zu treten.

Hochkarätige Sprecherinnen und Sprecher aus Politik, Behörden, Unternehmen, Verbänden und Wissenschaft machten den Kongress zum zentralen Forum für Zusammenarbeit im Bereich Cyber-Security. In seiner Eröffnungsrede verdeutlichte BSI-Präsident Arne Schönbohm, dass Informationssicherheit eine Gemeinschaftsaufgabe ist und das enorme Interesse an dem Kongress zeige, dass das Thema in der Gesellschaft angekommen sei. Diskutiert wurde unter anderem darüber, wie Cyber-Sicherheit zur Cheffinnen- und Chefsache wird – wie es auch im Titel des Kongresses hieß. Denn angesichts der wachsenden Bedeutung der Digitalisierung und der angespannten Bedrohungslage ist das Thema Cyber-Sicherheit als eine strategische Aufgabe zu verstehen. Diesen Aspekt haben sowohl Bundesinnenministerin Nancy Faeser als auch der niedersächsische Minister für Inneres und Sport Boris Pistorius und Iris Plöger von der BDI-Hauptgeschäftsführung während der Eröffnung des ersten Kongresstages unterstrichen. In ihrer Rede betonte Bundesinnenministerin Nancy Faeser die zentrale Bedeutung der Informationssicherheit für die Funktionsfähigkeit von Staat, Wirtschaft und Gesellschaft: „IT-Sicherheit ist elementarer Bestandteil der inneren Sicherheit.“ Sie kündigte an, das BSI zu einer „Zentralstelle im Bund-Länder-Verhältnis ausbauen“ zu wollen und so die föderale Zusammenarbeit zu verbessern.

### Verbraucherinnen und Verbraucher im Blick: BSI übergibt erstes IT-Sicherheitskennzeichen

Im Rahmen des Kongresses übergab das BSI das erste IT-Sicherheitskennzeichen: Der Anbieter mail.de erhielt insgesamt vier IT-Sicherheitskennzeichen für vier verschiedene E-Mail-Dienste. Das BSI stellt mit dem IT-Sicherheitskennzeichen, mit dem sich Sicherheitseigenschaften von IT-Produkten leichter beurteilen lassen, Verbraucherinnen und Verbrauchern eine Orientierung zur Verfügung (siehe Artikel auf S. 44). Das Kennzeichen schafft somit mehr Transparenz am Markt und bietet Nutzerinnen und Nutzern die Möglichkeit, vor dem Kauf von IT-Produkten eine informierte und bewusster Kaufentscheidung zu

*Mit dem Impuls aus dem BSI „Damit morgen nicht das Licht ausgeht: Cyber-Sicherheit statt Blackout“ eröffnete Christine Hofer einen der zahlreichen Themenblöcke*



treffen. Das IT-Sicherheitskennzeichen ist damit ein wichtiger Meilenstein für das Engagement des BSI und eine sichere Digitalisierung.

### Zwei Nachwuchskräfte erhalten Förderpreis für Arbeiten zum Schutz von Energienetzen

Mit dem „Best Student Award“ zeichnet das BSI im Kontext des Deutschen IT-Sicherheitskongresses traditionell junge Talente aus, die mit besonderen Ideen und Leistungen zur Verbesserung der Informationssicherheit in Deutschland beitragen. Die beiden Doktoranden Asiye Öztürk und Erfan Koza vom Clavis-Institut für Informationssicherheit der Hochschule Niederrhein wurden im Rahmen des IT-Sicherheitskongresses für ihre Arbeit zum Schutz von Energienetzen ausgezeichnet. Das Preisträger-Duo des „Best Student Awards“ 2022 fokussierte sich damit auf die Betreiber solcher Kritischen Infrastrukturen, auf die durch das IT-Sicherheitsgesetz 2.0 neue Aufgaben zukommen.



*Boris Pistorius, Minister für Inneres und Sport des Landes Niedersachsen, unterstreicht in seiner Rede die vertrauensvolle und enge Zusammenarbeit zwischen dem BSI und dem Land Niedersachsen*

Aufgrund der positiven Resonanz und um auch künftig möglichst vielen Teilnehmerinnen und Teilnehmern eine Plattform für den Austausch zu aktuellen Themen der Cyber-Sicherheit zu bieten, wird der Kongress fortan jährlich und weiterhin digital stattfinden.

Einen Rückblick auf den diesjährigen Kongress bietet sowohl die BSI-Internetseite als auch der Tagungsband zum 18. Deutschen IT-Sicherheitskongress, der im SecuMedia Verlag erschienen ist und eine umfassende Kongressdokumentation aller Vorträge beinhaltet. ■

#### Weitere Informationen:



<https://www.bsi.bund.de/IT-Sicherheitskongress>

# Der Beirat Digitaler Verbraucherschutz

**Externe Impulse stärken den digitalen Verbraucherschutz im BSI**

von Dr. Katharina Witterhold, Referat Grundsatzfragen des Digitalen Verbraucherschutzes und Kooperationen

Seit Juni 2021 unterstützt der Beirat Digitaler Verbraucherschutz das BSI dabei, zielgruppenorientierte und praxistaugliche Maßnahmen zu entwickeln, die die Cyber-Sicherheit im digitalen Alltag von Verbraucherinnen und Verbrauchern erhöhen. Das Gremium, bestehend aus zehn Expertinnen und Experten, stärkt die Verbraucherperspektive durch die aktive Beteiligung der Zivilgesellschaft, der Verbraucherwissenschaften, der Informatik und der Wirtschaft in den Prozessen des BSI.



## Die Herausforderung

Schon seit vielen Jahren erarbeitet das BSI praxistaugliche Mindeststandards und Handlungsempfehlungen für die öffentliche Verwaltung, für Wirtschaftsunternehmen sowie Forschungseinrichtungen und ermöglicht so den sicheren Einsatz von Informations- und Kommunikationstechnik. Mit dem IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) sind die Verbraucherinnen und Verbraucher mehr in den Fokus gerückt. Das BSI hat frühzeitig erkannt, dass sich ein IT-Sicherheitssystem an den Fähigkeiten und Bedürfnissen seiner Nutzerinnen und Nutzer orientieren muss. Die Einschätzung dieser Fähigkeiten ist angesichts dieser heterogenen Zielgruppe keine leichte Aufgabe. Hinzu kommt, dass auch Erreichbarkeit und Problembewusstsein sich anders gestalten als beispielsweise bei Akteurinnen und Akteuren der öffentlichen Verwaltung.

Verbraucherinnen und Verbraucher sind in ihrem Privatbereich nicht eingebunden in Strukturen, die ihnen konkrete Vorgaben bzgl. der Verwendung von Produkten machen oder sie bei deren sicherer Nutzung anleiten. Auch ist es abhängig vom individuellen Interesse und Risikobewusstsein, ob sie sich beispielsweise für einen Newsletter anmelden, der sie über aktuelle Bedrohungen informiert. Entsprechend gilt es, bei den Verbraucherinnen und Verbrauchern für IT-Sicherheit zu werben sowie für die Einsicht in die Notwendigkeit, sich mit dieser langfristig zu befassen. Dies alles vollzieht sich vor einem dynamischen Hintergrund. Besonders der Markt für digitale Konsumgüter ist sehr dynamisch und erfordert ein kontinuierliches Monitoring von bestehenden sowie neuen Instrumenten und ihrer Entwicklung.



### Die Aufgabe

Der Beirat Digitaler Verbraucherschutz unterstützt das BSI darin, passgenaue Angebote für die unterschiedlichen Zielgruppen innerhalb der Verbraucherschaft zu entwickeln. Übergeordnete Ziele sind dabei, die Beurteilungsfähigkeit und die Problemlösungskompetenz der Verbraucherinnen und Verbraucher zu stärken. Ein wichtiger Bestandteil dieser Strategie ist der Ausbau des bestehenden Informationsangebots des BSI für Privatanwenderinnen und -anwender, welches bereits lange vor dem IT-SiG 2.0 etabliert wurde und damit frühzeitig auf die Notwendigkeit reagiert hat, auch Privatpersonen als unverzicht-

baren Bestandteil einer resilienten Cyber-Gesellschaft zu adressieren. Die Beiratsmitglieder bringen durch ihre Expertise in den Bereichen Verbraucherinformation und -recht, Cyber-Sicherheitsberatung sowie digitale Marktplätze und Bildung die dafür notwendige Perspektivenvielfalt mit. Doch nicht nur die Beratung zu Handlungsempfehlungen für Verbraucherinnen und Verbraucher sind Teil der Beiratsarbeit. Auch das IT-Sicherheitskennzeichen und die Auswahl zukünftiger Produktkategorien sowie Einschätzungen zu kommenden Trends auf dem Verbrauchermarkt sollen vom Beirat adressiert werden.

### Das Team

**Prof. Dr. Martina Sasse (Sprecherin)**

*Ruhr-Universität Bochum*

**Dr. Dennis Romberg (stellvertretender Sprecher)**

*Verbraucherzentrale Bundesverband*

**Philipp Ehmann**

*eco – Verband der Internetwirtschaft e.V.*

**Prof. Dr. Hannes Federrath**

*Gesellschaft für Informatik e.V. (GI)*

**Dr. Sven Herpig**

*Stiftung Neue Verantwortung e. V. (SNV)*

**Linus Neumann, Vertr.: Frank Rieger**

*Chaos Computer Club e.V. (CCC)*

**Prof. Dr. Martin Schmidt-Kessel**

*Universität Bayreuth*

**Rebekka Weiß**

*Bitkom e.V.*

**Helga Zander-Hayat, Vertr.: Dr. Ayten Öksüz**

*Verbraucherzentrale NRW e.V.*

**Jörg Zymnossek\***

*Stiftung Warentest*

### Der Ausblick

Das vielfältige Aufgabenspektrum des Beirats Digitaler Verbraucherschutz legt die Fokussierung auf ausgewählte Themenbereiche nahe. Aus diesem Grund widmet sich der Beirat in jedem Jahr zielgerichtet der Bearbeitung eines Themas. Für das erste Jahr wählte der Beirat das Thema „Passwortsicherheit, 2-Faktor-Authentisierung und Phishing – Evaluation der Gefährdungslage und Bewertung der Handlungsempfehlungen des BSI“ aus.

Ausgangspunkt hierfür ist die Beobachtung, dass die Absicherung der Onlinekonten für Verbraucherinnen und Verbraucher zwar von höchster Relevanz ist, die praktische Umsetzung mitunter aber schwerfällt. Daher ist es das Ziel des Beirats, eine Handreichung für das BSI zu erarbeiten, auf deren Basis es zukünftig Verbraucherinnen und Verbraucher anwenderorientiert und nutzerfreundlich beraten kann. ■

\*Bis 25. April 2022.

# Ein digitaler Dialog in Zeiten der Pandemie

## „Dialog für Cyber-Sicherheit“ – der Blick über den (digitalen) Tellerrand

von Nora Kluger, Referat Cyber-Sicherheit für Gesellschaft und Bürger, und Dr. Angelika Praus, Referat Strategien und neue Ansätze der Informationssicherheit

Mit der „Denkwerkstatt Sichere Informationsgesellschaft“ startete im Februar 2021 der erste Jahreszyklus des BSI-Projekts „Dialog für Cyber-Sicherheit“. Dabei wird im Rahmen eines Pilotprozesses ein Partizipations- und Multistakeholder-Modell umgesetzt, das in dem Vorgängerprojekt „Institutionalisierung des gesellschaftlichen Dialogs“ (BSI-Magazin 2/2020) von den Dialogteilnehmerinnen und -teilnehmern selbst entwickelt wurde.

Mit dem „Dialog für Cyber-Sicherheit“ soll der Dialog des BSI mit Vertreterinnen und Vertretern der organisierten Zivilgesellschaft sowie der Bereiche Wirtschaft, Wissenschaft, Staat, Kultur und Medien („Multistakeholder“) weiter ausgebaut und verstetigt werden.

Mit diesem Projekt, das vom nexus Institut und dem iRights.Lab im Auftrag des BSI umgesetzt wird, möchte sich das BSI im Sinne eines Open-Government-Ansatzes

öffnen, Vertrauen aufbauen, die bidirektionale Kommunikation ausbauen, Partizipation ermöglichen und eine Plattform für einen dauerhaften Dialog zur Cyber-Sicherheit mit allen gesellschaftlichen Gruppen schaffen.

### Ein Dialog für alle Gruppen

Im Rahmen der Denkwerkstatt 2021 wählten die Teilnehmerinnen und Teilnehmer ein fünfköpfiges Dialogkomitee aus fünf Stakeholder-Gruppen, das den Dialog-



„Ich bin überzeugt, dass Technik dem Menschen dienen muss, nicht umgekehrt. Mensch und Umwelt sollten bei der Digitalisierung im Vordergrund stehen. Ich möchte deshalb eine Kursänderung von einer technikzentrierten und effizienzgetriebenen Digitalisierung hin zu einer nachhaltigen menschenzentrierten Digitalisierung bewirken. Hierfür ist eine kontinuierliche diskriminierungsfreie Partizipation der zivilgesellschaftlichen Akteurinnen und Akteure auf allen Ebenen unerlässlich. Ich freue mich sehr, dass ich als Vertreter der Zivilgesellschaft im Dialogkomitee des Projektes ‚Dialog für Cyber-Sicherheit‘ des BSI die Möglichkeit habe, zwischen allen Stakeholder-Gruppen als Intermediär zu fungieren.“

- Mirko de Paoli, Vorstandsvorsitzender Bundesverband Smart City e.V.,  
Vertreter der organisierten Zivilgesellschaft im Dialogkomitee des „Dialogs für Cyber-Sicherheit“





„Die Technologie macht rasante (Quanten-)Sprünge. Durch den Dialog zwischen unterschiedlichen Akteurinnen und Akteuren schaffen wir einen gemeinsamen Blick und ein gemeinsames Verständnis auch für die gewünschte Andersartigkeit, die es in der heutigen Welt mehr denn je braucht. Wir stehen vor großen Herausforderungen, die wir nicht allein, sondern nur gemeinsam mit den unterschiedlichen Perspektiven lösen können. Im Mittelpunkt unseres Wirkens steht immer das Gemeinwohl aller – Mensch, Tier und Natur. Das Dialogprojekt ist ein erkenntnisreiches Format, gewinnbringend für alle Beteiligten und unsere Gesellschaft, für die Lösungen erarbeitet werden.“

- Jörg Schüler, Geschäftsführer und Gründer Digitale Helden gGmbH, Vertreter des Sektors „Medien und Kultur“ im Dialogkomitee des „Dialogs für Cyber-Sicherheit“

prozess für zwei Jahre begleitet und eine Schnittstelle zwischen BSI, Auftragnehmern und den fünf Stakeholder-Gruppen bildet.

Ein inhaltlicher Schwerpunkt der Denkwerkstatt war die Vorstellung und Auswahl von fünf spannenden Themen aus dem Bereich Cyber-Sicherheit durch die Dialogpartnerinnen und -partner, zu denen in den folgenden Monaten in kleineren Arbeitsgruppen, sogenannten Workstreams, diskutiert und gearbeitet wurde:

- digitale Katastrophenhelfer
- digitales Mindesthaltbarkeitsdatum
- Dos and Don'ts für nachhaltig sichere Produkte
- Evaluation von Awareness-Maßnahmen
- Cyber-Sicherheit an Schulen

#### Herausforderungen im digitalen Raum

Aufgrund der Pandemie fanden die Workstreams im ersten Projektzyklus digital statt, was mit einigen technischen,

organisatorischen, rechtlichen und kommunikativen Herausforderungen verbunden war. Und nachdem auch der zwischenmenschliche Kontakt und das persönliche Kennenlernen der Beteiligten pandemiebedingt wegfielen, gestalteten sich die Kommunikation und der Vertrauensaufbau auf Distanz schwieriger als im physischen Raum.

Trotz dieser Hürden und dank des Engagements der zum großen Teil ehrenamtlichen Stakeholderinnen und Stakeholder konnten in diesem ersten Projektzyklus wertvolle Ergebnisse erarbeitet und viele Erfahrungen gesammelt werden, die in den weiteren Pilotprozess einfließen.

Mit der Vorstellung der Workstream-Ergebnisse des Vorjahres endete im Mai 2022 der erste Projektzyklus des Dialogs. Der zweite beginnt mit der „Denkwerkstatt Sichere Informationsgesellschaft“ im zweiten Halbjahr 2022, die voraussichtlich in Präsenz stattfinden wird. Alle Beteiligten hoffen, sich bald persönlich kennenzulernen und auch analog zusammenarbeiten zu können. ■

**Dialog für  
Cyber-Sicherheit**



#### Weitere Informationen:



Mehr zum Dialog, zu den Themen der Workstreams und zur Möglichkeit der Mitwirkung  
<https://www.dialog-cybersicherheit.de>

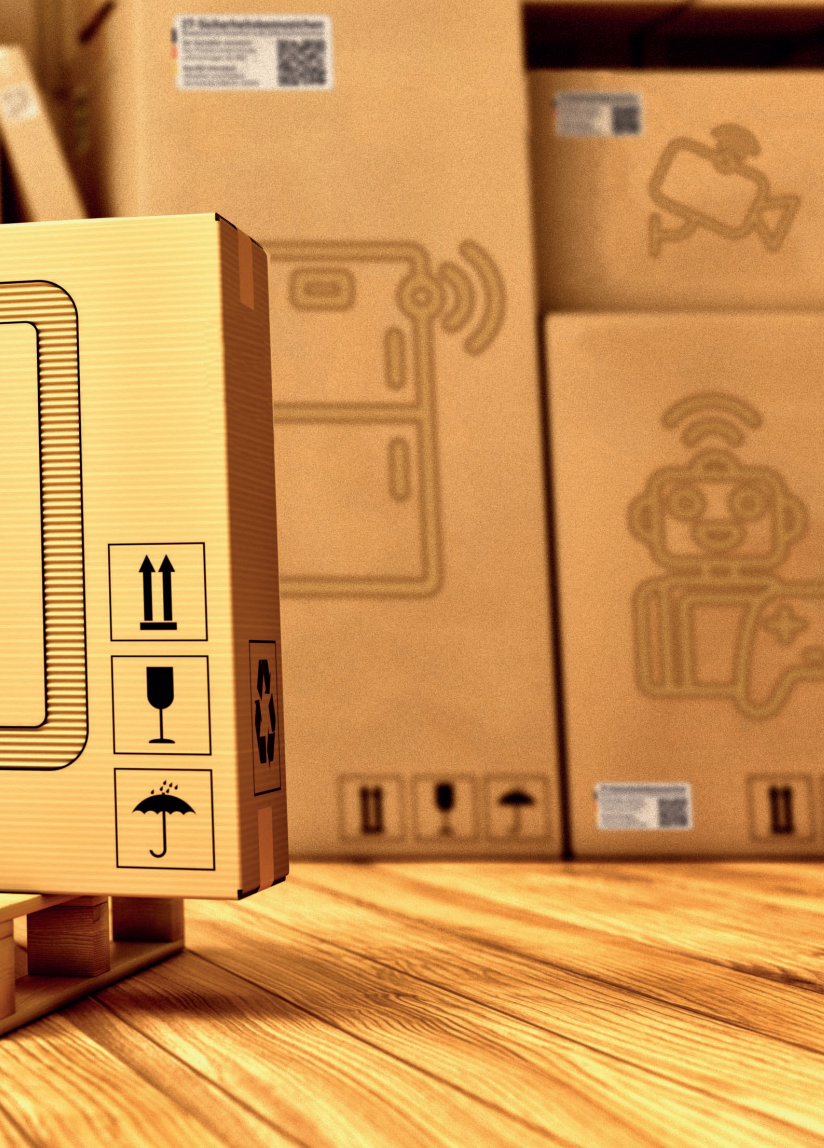


# Einführung des IT-Sicherheitskennzeichens

Ein Kennzeichen für mehr Transparenz und Informationssicherheit auf dem deutschen Verbrauchermarkt

*von Quan Ha The, Referat Erteilung von IT-Sicherheitskennzeichen, und Robert Hoyer, Referat Grundsatzfragen des Digitalen Verbraucherschutzes und Kooperationen*

Die Digitalisierung des Alltags bringt neben Annehmlichkeiten auch Sicherheitsrisiken mit sich. Gleichzeitig wird es für Verbraucherinnen und Verbraucher immer schwieriger, die wesentlichen IT-Sicherheitseigenschaften von digitalen Geräten und Anwendungen zu beurteilen. Das IT-Sicherheitskennzeichen bietet eine Lösung für dieses Problem und schafft mehr Transparenz auf dem digitalen Verbrauchermarkt.



Produktkategorien möglich. Um das IT-Sicherheitskennzeichen zu erhalten, verpflichtet sich der Hersteller bzw. Dienstanbieter freiwillig, durch das BSI erarbeitete oder anerkannte Branchenstandards für die jeweiligen Produktkategorien einzuhalten. Diese Sicherheitsstandards können sich je nach Produktkategorie unterscheiden. So gilt beispielsweise die Technische Richtlinie BSI TR-03148 für die Produktkategorie „Breitbandrouter“ oder die BSI TR-03108 für die Produktkategorie „E-Mail-Dienste“.

#### Das IT-Sicherheitskennzeichen

- ... schafft Transparenz für Verbraucherinnen und Verbraucher, da es wichtige Fakten zu den Sicherheitseigenschaften von vernetzten Produkten und Diensten aktuell, verständlich sowie neutral zusammenfasst und auf bekannte Sicherheitslücken hinweist;
- ... hilft, die Sicherheitseigenschaften von IT-Produkten leichter zu beurteilen und eine informierte Kaufentscheidung zu treffen;
- ... steigert das Sicherheitsniveau von IT-Produkten, da Hersteller und Dienstanbieter einen Anreiz erhalten, Sicherheitsstandards bereits in der Entwicklungsphase mitzudenken (Security by Design) und die Geräte bei Auslieferung mit einer entsprechenden Standardkonfiguration zu versehen (Security by Default).

#### Das IT-Sicherheitskennzeichen als Pfeiler des Digitalen Verbraucherschutzes im BSI

Um Verbraucherinnen und Verbrauchern mehr Informationen zur Sicherheit von Consumer-IT zur Verfügung zu stellen, wurde das IT-Sicherheitskennzeichen am 8. Dezember 2021 eingeführt. Seitdem ist eine Beantragung des Kennzeichens möglich.

Mit der Eröffnung des Antragsverfahrens und der Vergabe der ersten IT-Sicherheitskennzeichen ist es dem BSI innerhalb weniger Monate gelungen, eine besonders wichtige Aufgabe aus dem IT-Sicherheitsgesetz 2.0 zu erfüllen und die Transparenz von IT-Sicherheit auf dem Verbrauchermarkt aktiv zu gestalten.

Das IT-Sicherheitskennzeichen erhöht das Bewusstsein der Verbraucherinnen und Verbraucher für die Sicherheitseigenschaften von Geräten und digitalen Diensten. IT-Sicherheit wird damit als entscheidendes Kaufargument stärker am Verbrauchermarkt platziert. Das Kennzeichen ist somit ein neues, zentrales Element des Digitalen Verbraucherschutzes in Deutschland.

Eine Beantragung des IT-Sicherheitskennzeichens ist innerhalb der vom BSI definierten und veröffentlichten

#### IT-Sicherheitskennzeichen

Bundesamt für Sicherheit in der Informationstechnik

**Der Hersteller versichert:**  
Das Produkt entspricht den Anforderungen des BSI.

**Das BSI informiert:**  
Aktuelles zum Produkt  
[bsi.bund.de/IT-SIK](https://bsi.bund.de/IT-SIK)



*Beispielhaftes IT-Sicherheitskennzeichen mit QR-Code und BSI-Link, die zur allgemeinen Informationsseite zum IT-Sicherheitskennzeichen führen*

#### Dynamische Sicherheitsinformationen: Mehrwert für Verbraucherinnen und Verbraucher

Hat ein Produkt das IT-Sicherheitskennzeichen erhalten, ist der jeweilige Hersteller oder Dienstanbieter verpflichtet, das Etikett des IT-Sicherheitskennzeichens auf dem Gerät, der Verpackung oder der Herstellerwebsite zu platzieren. Das Etikett enthält einen Kurzlink und einen QR-Code. Verbraucherinnen und Verbraucher gelangen darüber auf die Produktinformationsseite des BSI und erhalten dort relevante Informationen zu den Sicherheitseigenschaften des jeweiligen Produktes, die der Hersteller zugesichert hat. Zudem sind auf der Website aktuelle,

leicht abrufbare Sicherheitsinformationen zu finden, wie beispielsweise Hinweise zu Schwachstellen, die dem BSI bekannt sind, oder zu verfügbaren Updates für Produkte, die mit dem Kennzeichen versehen sind. Das Besondere hierbei: Die Informationen sind dynamisch und werden vom BSI nach Erkenntnislage und über die gesamte Laufzeit des IT-Sicherheitskennzeichens – in der Regel zwei Jahre – aktualisiert.

### Marktaufsicht für aktiven Verbraucherschutz

Im Rahmen der Antragsbearbeitung wird zunächst geprüft, ob die Konformität mit den vom BSI festgelegten Sicherheitsanforderungen plausibel und nachvollziehbar zugesichert wurde. Eine technische Prüfung durch das BSI, wie etwa bei einer Zertifizierung, erfolgt im Rahmen der Erteilung des IT-Sicherheitskennzeichens nicht. Während der Laufzeit des IT-Sicherheitskennzeichens kann die nachgelagerte Marktaufsicht eine solche Prüfung anlasslos (stichprobenartig) oder anlassbezogen, etwa bei Bekanntwerden einer Sicherheitslücke, durchführen. Die Erkenntnisse aus der Marktaufsicht fließen in die dynamischen Sicherheitsinformationen auf der Produktinformationsseite des BSI ein. Zum verstärkten Schutz der Verbraucherinnen und Verbraucher kann das BSI, insbesondere bei Verstößen gegen Sicherheitsstandards, die Freigabe des IT-Sicherheitskennzeichens widerrufen. Wird das IT-Sicherheitskennzeichen ohne Freigabe durch das BSI verwendet, stellt dies eine Ordnungswidrigkeit dar und kann mit einer Geldbuße von bis zu 500.000 Euro geahndet werden.

### Ein erfolgreicher Start

Bereits kurz nach der Einführung des IT-Sicherheitskennzeichens am 8. Dezember 2021 sind beim BSI die ersten Anträge für die Produktkategorien „Breitbandrouter“ und „E-Mail-Dienste“ eingegangen. Durch das effizient gestaltete Erteilungsverfahren konnte BSI-Präsident Arne Schönbohm die ersten vier IT-Sicherheitskennzeichen schon am 1. Februar 2022 im Rahmen des 18. Deutschen



BSI-Präsident Arne Schönbohm und Fabian Bock, Geschäftsführer der mail.de GmbH, bei der Übergabe des ersten IT-Sicherheitskennzeichens



IT-Sicherheitskongresses übergeben. Gekennzeichnet wurden vier E-Mail-Dienste des Anbieters mail.de. Weitere Anträge liegen bereits vor und befinden sich in der Bearbeitung.

Mit der Erteilung der ersten IT-Sicherheitskennzeichen tritt auch der Mechanismus der BSI-Marktaufsicht erstmals in Kraft.

### Eine konstruktive Zusammenarbeit und ständiger Dialog

Um diesen Erfolg zu ermöglichen, haben Mitarbeiterinnen und Mitarbeiter aus verschiedenen Abteilungen des BSI ihre Kompetenzen und ihr Know-how gebündelt. Ob zunächst innerhalb einer Projektgruppe zur Konzeption des IT-Sicherheitskennzeichens oder im Rahmen der operativen Umsetzung und Einführung unter der Federführung des zuständigen Referats: Das IT-Sicherheitskennzeichen ist ein Thema mit vielen Schnittstellen im BSI und der Erfolg eine Leistung, zu der viele beigetragen haben.

Das BSI stellt damit Verbraucherinnen und Verbrauchern ein praktisches Werkzeug für den digitalen Alltag zur Verfügung, mit dem sich Sicherheitseigenschaften von IT-Produkten leichter beurteilen lassen.

Auf seiner Website stellt das BSI vielfältige Informationen für interessierte Antragsteller sowie Verbraucherinnen und Verbraucher zur Verfügung. Neben grundsätzlichen Erläuterungen zu Aufbau, Funktionsweise und Ablauf des Antragsverfahrens befinden sich dort umfangreiche FAQs und die zugehörigen Produktinformationsseiten der



ersten erteilten IT-Sicherheitskennzeichen. Im Laufe des Jahres soll das Informationsangebot zum IT-Sicherheitskennzeichen durch zielgruppenorientierte Maßnahmen wie Videos und Informationskampagnen weiter erhöht werden.

Um das Bewusstsein für die Bedeutung transparenter Sicherheitseigenschaften von Verbraucher-IT zu erhöhen, befindet sich das BSI zusätzlich im kontinuierlichen Austausch und Dialog mit Stakeholdern, dazu gehören beispielsweise Wirtschafts- und Verbraucherschutzverbände.

#### Weiterentwicklung des IT-Sicherheitskennzeichens

Die nächsten Produktkategorien für das IT-Sicherheitskennzeichen stammen aus dem Bereich des Internet of Things (IoT) und basieren auf dem europäischen IoT-Basisstandard ETSI EN 303 645. In diesem Bereich wird das BSI im Laufe des Jahres immer mehr Produktkategorien für das IT-Sicherheitskennzeichen veröffentlichen. Damit möchte das BSI die Transparenz von IT-Sicherheitseigenschaften in einem für Verbraucherinnen und Verbraucher besonders wichtigen Marktsegment erhöhen.

Auch wenn es derzeit noch kein einheitliches und verpflichtendes IT-Sicherheitskennzeichen auf EU-Ebene gibt, sieht das BSI das nationale IT-Sicherheitskennzeichen als mögliche Blaupause und ersten Schritt in diese Richtung. Durch die angestrebte Verwendung von europäischen Normen, wie beispielsweise dem IoT-Basisstandard ETSI EN 303 645, bemüht sich das BSI bereits jetzt um einen Gleichlauf mit europäischen Standards.

Neben neuen Produktkategorien entwickelt das BSI auch die Prozesse und Verfahren für die Erteilung des IT-Sicherheitskennzeichens weiter. Zur Erklärung des Verfahrens gegenüber Antragstellern wurde dazu eine Verfahrensbeschreibung auf der Website des BSI veröffentlicht. Weiterhin befindet sich ein Projekt zur Digitalisierung des Antragsverfahrens auf dem OZG-Portal des Bundes in Umsetzung, wodurch auf absehbare Zeit eine Antragstellung für das IT-Sicherheitskennzeichen vollständig online möglich sein wird. ■

#### Weitere Informationen:



Informationswebsite zum IT-SiK:  
<https://www.bsi.bund.de/IT-SiK>



Verzeichnis erteilter IT-Sicherheitskennzeichen:  
[https://www.bsi.bund.de/SiteGlobals/Forms/IT-Sicherheitskennzeichen/IT-Sicherheitskennzeichen\\_Formular.html](https://www.bsi.bund.de/SiteGlobals/Forms/IT-Sicherheitskennzeichen/IT-Sicherheitskennzeichen_Formular.html)



Beispielseite für die Produktinformationsseite:  
<http://www.bsi.bund.de/it-sik/beispiel>



Antragstellung IT-Sicherheitskennzeichen:  
<http://www.bsi.bund.de/it-sik/antrag>



# Eingestuft und gut geschützt

## Ganzheitlicher Digitalisierungsansatz zur Verarbeitung von Verschlusssachen

*von Marianne Ziesmer und Hans-Willi Fell, Referat Produkte und Systeme für Verschlusssachen, und Silke Heiligenschmidt, Referat VS-IT-Infrastruktur*

Schutzbedürftige Informationen müssen sicher verarbeitet und kommuniziert werden können. Gerade der Schutz von Verschlusssachen (VS) ist für die Bundesverwaltung besonders wichtig und bildet die Grundlage für ein souveränes und resilientes staatliches Handeln. Daher sind geeignete VS-IT-Produkte für die sichere und vorschriftenkonforme Handhabung von Verschlusssachen eine wichtige Voraussetzung für das Gelingen der Digitalisierung im Hochsicherheitsbereich.



Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet die Informationssicherheit zum Schutz von VS durch die Bereitstellung eines breiten Produktportfolios an VS-IT-Produkten für Bund, Länder und die geheimschutzbetreute Wirtschaft. Allein die Verfügbarkeit geeigneter VS-IT führt jedoch nicht automatisch zu einer digitalen Transformation in der Verwaltung. Anwenderinnen und Anwender in den Verwaltungen, Behördenleitungen sowie IT-Beauftragte sind gefragt, die Digitalisierung in effizienter, nutzerfreundlicher und vor allem sicherer Form zu gestalten. Es geht dabei nicht nur darum, VS-IT-Produkte zu platzieren, sondern sie auch in die alltäglichen Arbeitsprozesse zu integrieren, um so ihren Mehrwert in der Verwaltung voll auszuschöpfen.

Das BSI unterstützt diesen Prozess, indem es die Anforderungen zwischen Anwendern, Herstellern und BSI harmonisiert. Benutzerfreundlichkeit, Betriebbarkeit und Skalierbarkeit von VS-IT sind daher neben den klassischen Zielen der Informationssicherheit (Vertraulichkeit, Verfügbarkeit und Integrität) unabdingbar für eine moderne VS-IT. Durch die enge Kooperation mit der Bundesverwaltung und den Herstellern können die Anforderungen der Anwenderinnen und Anwender direkt in die Produktentwicklung einfließen, um eine sichere und gleichzeitig bedarfsgerechte Ausgestaltung von VS-IT zu ermöglichen.

#### Die Anforderungen immer im Blick

Eine Verschlusssache ist eine im öffentlichen Interesse geheimhaltungsbedürftige Information. In der Bundesrepublik Deutschland regelt die Verschlusssachenanweisung (VSA) den Umgang mit VS. Sie definiert unter anderem die Geheimhaltungsgrade, die entsprechend der Schutzbedürftigkeit anzuwenden sind: VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD), VS-VERTRAULICH, GEHEIM und STRENG GEHEIM.

Grundsätzlich steigen die Anforderungen an die Schutzwirkung der IT-Produkte, je höher der Geheimhaltungsgrad der VS ist. So sind z. B. ab dem Geheimhaltungsgrad VS-VERTRAULICH besondere Anforderungen an den Abstrahlenschutz von IT-Hardware zu stellen.

Um zu gewährleisten, dass die hohen Anforderungen an die VS-IT auch eingehalten werden, dürfen laut VSA nur solche IT-Produkte für die Verarbeitung von VS eingesetzt werden, die vom BSI evaluiert und zugelassen worden sind. Einschätzungen zu kommenden Trends auf dem Verbrauchermarkt sollen vom Beirat adressiert werden.



SINA Communicator H



R&S®ELCRODAT 7-FN

#### IT-Produkte im Bereich der höher eingestuften VS

Die Coronapandemie hat den Bedarf an GEHEIM-fähigen Produkten für die Bereiche Audio, Video und Dokumentenaustausch noch einmal deutlich verstärkt und die Entwicklungsprojekte in diesen Bereichen zusätzlich beschleunigt. Das BSI ist dabei entwicklungsbegleitend eng eingebunden und führt im Rahmen der Zulassungsverfahren entsprechende Evaluierungen durch.

Im Bereich der GEHEIM-tauglichen Sprach- und Videotelefonie findet beispielsweise derzeit eine umfangreiche Modernisierung der Bestandssysteme von ISDN zu IP-basierter Telefonie statt. Durch die Neuentwicklungen der Produkte „Communicator H“ der Firma secunet und „ED7-FN“ von Rohde & Schwarz werden zukünftig einfache Bedienbarkeit, Interoperabilität über ein gemeinsames Netzwerkprotokoll sowie der Einsatz Quantencomputer-resistenter Kryptografie sichergestellt.

Neben der sicheren Sprache und Videotelefonie stellt der GEHEIM-fähige Datenaustausch einen weiteren Schwerpunkt unter den VS-IT-Produkten dar. Mit SINA Workflow (SWF) steht ein Verschlusssachen-Vorgangsbearbeitungssystem bereit, das eine umfassende digitale IT-Unterstützung bei der Bearbeitung von VS-Daten bietet. SWF ist eine VSA-konforme, zugelassene und revisionssichere Lösung, um einen VS-Vorgang von der Bearbeitung über die Registrierung bis hin zur Verteilung von VS-Daten digital zu realisieren.

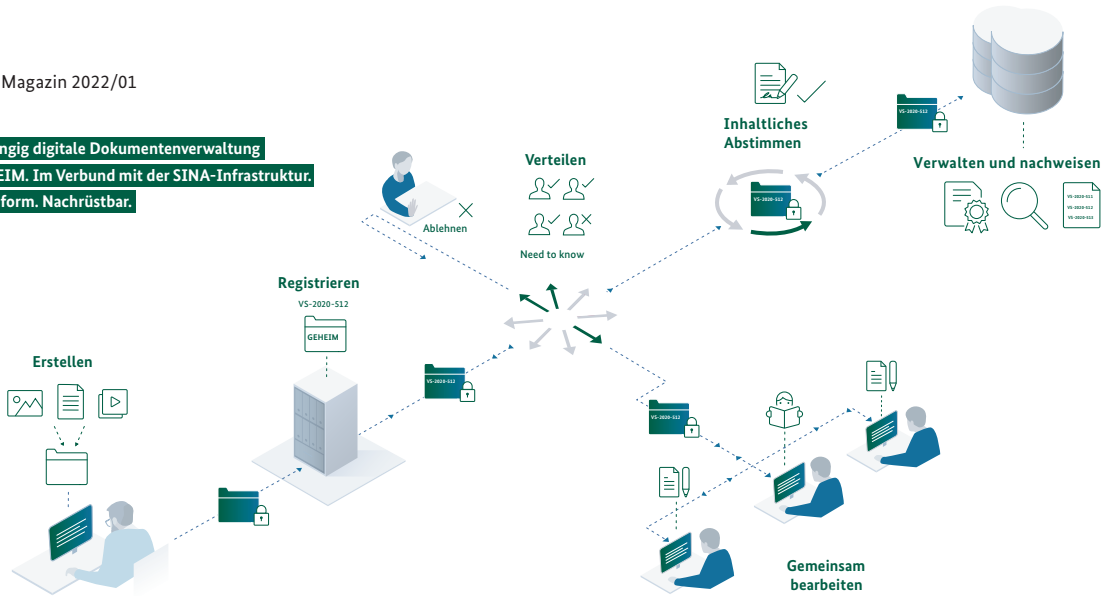
SINA Workflow ist Teil einer zugelassenen Produktlandschaft der Firma secunet, deren Produkte sich funktional ergänzen und im Zusammenspiel mit der SINA-H-Architektur als Produktserie für die Verarbeitung, Speicherung und Übertragung von Verschlusssachen bis einschließlich GEHEIM die Vertraulichkeit, Integrität und Verfügbarkeit eingestufte Daten gewährleisten.

Aktuell sollen während einer Erprobung von SWF im BSI die betrieblichen und die funktionalen Aspekte eingehender beurteilt werden. Dabei ist nach einem halben Jahr Probetrieb ab Mitte 2022 ein fließender Übergang in den Wirkbetrieb geplant. Die Erfahrungen und Erkenntnisse aus der Pilotierungsphase werden in die Produktbegleitung und Weiterentwicklung zugelassener VS-IT-Produkte des BSI für die Bundesverwaltung einfließen.

#### Ressortübergreifend sicher kommunizieren

Informationsaustausch höherer VS-Grade findet nicht nur innerhalb eines Referats, einer Abteilung oder einer Behörde statt. Hochsicher, schnell, zuverlässig und nutzerfreundlich sollte sich eine GEHEIM-fähige Kommunikation auch zwischen Ministerien und Behörden gestalten und so effiziente Regierungsarbeit gewährleisten. Hier soll die Digitalisierung ebenfalls Hürden in der ressortübergreifenden Kommunika-

Durchgängig digitale Dokumentenverwaltung  
bis GEHEIM. Im Verbund mit der SINA-Infrastruktur.  
VSA-konform. Nachrüstbar.



tion von hoch eingestuftem Verschlusssachen abbauen und Prozesse grundlegend vereinfachen.

Um dieses Vorhaben zu bündeln, wurde die Bundesmaßnahme Ressortübergreifende VS-Kommunikation (R-VSK) beim Auswärtigen Amt ins Leben gerufen. Dabei soll ein mit den Ressorts der Bundesverwaltung abgestimmtes Vorgehen die Sicherheit und Nutzerfreundlichkeit fördern und zugleich Synergien beim Einsatz von VS-IT-Produkten schaffen. Dazu wurden verschiedene Ziele definiert. Zum einen fokussiert die Bundesmaßnahme darauf, die sichere Sprach- und Videokommunikation zu verbessern. Dies geschieht in enger Kooperation mit den Herstellern geeigneter VS-IT-Produkte. Zum anderen steht der ressortübergreifende, digitale Austausch von VS über Netzwerkinfrastrukturen im Mittelpunkt.

Im Jahres-Release 2022 der Bundesmaßnahme soll das oben beschriebene VS-Vorgangsbearbeitungssystem SWF integriert werden und die bereits vorhandenen Fähigkeiten zur Sprach- und Videokommunikation ergänzen. Die Behörden werden im Rahmen der Maßnahme R-VSK mit zentral administrierten VS-IT-Produkten ausgestattet. Das BSI berät die Bundesmaßnahme durch seine Expertise in den Bereichen VS-IT-Produkte, Geheimschutz sowie Sicherheit in Rechenzentren der Bundesverwaltung.

Mit der Bundesmaßnahme R-VSK verfolgt das Auswärtige Amt eine Dual-Vendor Strategie, sodass die Einhaltung von Standards in den Bereichen Sprach-, Video- und Datenkommunikation für die Realisierung besonders wichtig ist. Eine große Herausforderung ist dabei die Interoperabilität zwischen Produkten verschiedener Hersteller sowie den bereits bestehenden Lösungen und Strukturen einzelner Akteure. Im Rahmen einer ressortübergreifenden Arbeitsgruppe mit Vertreterinnen und Vertretern verschiedener Stakeholder wird hierzu intensiv der Dialog gesucht, um Interessen zu vereinen und einen ganzheitlichen, infrastrukturellen Ansatz zu ermöglichen.

Ebenso rücken Technologien wie beispielsweise Cloudumgebungen in den Fokus der VS-verarbeitenden IT-Produkte. Mittel- und langfristig wird es darum gehen, wie verschiedene Systeme vermehrt ineinandergreifen können, ohne Sicherheitsrisiken zu eröffnen und trotzdem die Potenziale innovativer technischer Lösungen voll auszuschöpfen.

**Fazit und Ausblick**

Als ganzheitlicher Digitalisierungsansatz bietet das Vorhaben R-VSK zum einen die Chance, Kommunikation im Geheimhaltungsgrad GEHEIM neu zu denken und die Vorteile der Digitalisierung auch in diesem Bereich zu nutzen. Zum anderen stellt es die Akteure aber vor die Herausforderung, etablierte Prozesse zu digitalisieren und Rahmenbedingungen, darunter die Ressorthoheit über VS, nicht zu verletzen. Mit der geplanten Anbindung weiterer Behörden wird die Möglichkeit, ressortübergreifend digitalisiert Daten auszutauschen, zu telefonieren und Videokonferenzen durchzuführen, kontinuierlich ausgebaut. Dies ist mit einem erheblichen Abbau der Kommunikationshürden zwischen den Behörden und der Minimierung des Zeit- und Arbeitsaufwandes verbunden.

Im nächsten Schritt werden im Jahres-Release 2022 der R-VSK die pilotierten und evaluierten Lösungen in den Wirkbetrieb überführt. Dazu sollen in enger Abstimmung zwischen dem Auswärtigen Amt und dem Bundesministerium des Innern und für Heimat die ressortübergreifende zentrale Infrastruktur für die VS-Verarbeitung hocheingestufteter Daten ausgebaut sowie auch eine behördeneigene SWF-Instanz für das Bundeskanzleramt realisiert werden.

Der Ausbau der VS-Dienste, die Erweiterung der angeschlossenen Ressorts und Behörden, die Harmonisierung mit bestehenden sowie neuen Infrastrukturen sind maßgeblich von den Fähigkeiten der VS-IT-Produkte abhängig. Das BSI wird initiativ in diesen Handlungsfeldern tätig werden, um die nachgefragte Produktpalette für den VS-Bereich bereitstellen zu können. Hierzu werden weitere Erprobungen im Rahmen von Proofs of Concept angestoßen, um den Einsatz von VS-IT-Produkten im BSI weiterzu-entwickeln und Implikationen für zukünftige Produkteinführungen in anderen Behörden zu erhalten.

Die Verfügbarkeit einer breiten Palette von interoperablen, nutzer- und betreiberfreundlichen VS-IT-Systemen von möglichst mehreren Herstellern ist entscheidend, damit die Bundesverwaltung auch in Zukunft auf einen ausreichend gefüllten Produktkatalog einschlägiger VS-IT-Systeme zugreifen kann. ■



# Gemeinsam stark für Cyber-Sicherheit

Wir als die Cyber-Sicherheitsbehörde des Bundes stehen gemeinsam für den gesetzlichen Auftrag: eine sichere Informationstechnik für die voranschreitende Digitalisierung. Eine große und verantwortungsvolle Mission, der wir uns als Team BSI verschrieben haben. Denn bei uns zählt vor allem eines: Teamgeist.

Mit Leidenschaft und Begeisterung leistet jede und jeder Einzelne einen wichtigen Beitrag für die gute Sache: dass die Menschen der digitalen Welt vertrauen können. Angesichts dieser großen Aufgabe soll unser Team weiter stetig wachsen.



Deshalb suchen wir:



## engagierte Fach- und Führungskräfte,

deren Herz auf der digitalen Seite schlägt.

Du bist ein Teamplayer? Du bist Einsteigerin/Einsteiger, Young Professional oder Expertin/Experte im Bereich der IT-Sicherheit? Du interessierst dich für technische Themen und möchtest für die gute Sache eintreten? Dann komm ins Team BSI. Hier bieten wir dir spannende Aufgaben, Gestaltungsmöglichkeiten und ein abwechslungsreiches Arbeitsumfeld.



Teamgeist



Gesellschaftlicher  
Mehrwert



Themen- und  
Aufgabenvielfalt



Gestaltungs-  
spielraum



Weiter-  
entwicklung



Bunte Teams und  
Chancengleichheit



Flexible  
Arbeitsgestaltung



Sicherheit



# Instanz für die Sicherheit biometrischer Verfahren

**Neues Biometrie-Evaluations-Zentrum in Sankt Augustin eröffnet**

*von Ralph Breithaupt, Referat Bewertungsverfahren für eID-Technologien in der Digitalisierung*

Im November 2021 haben der Präsident der Hochschule Bonn-Rhein-Sieg (H-BRS), Prof. Hartmut Ihne, und BSI-Präsident Arne Schönbohm das Biometrie-Evaluations-Zentrum (BEZ) auf dem Campus der Hochschule in Sankt Augustin bei Bonn eröffnet.



Mit ihrer einfachen Bedienbarkeit und ihrer Zuverlässigkeit haben sich biometrische Verfahren, bei denen körperliche Merkmale wie Gesicht, Fingerabdruck, Retina oder Iris für eine eindeutige Verifikation genutzt werden, einen festen Platz unter den IT-Sicherheitssystemen zur Authentisierung von Nutzerinnen und Nutzern verschafft. Anders als PIN, Passwort oder Sicherheitstoken können biometrische Merkmale nicht vergessen oder verloren werden. Durch die Einführung von Gesicht- und Fingerabdruck-Biometrie in Reisepass und Personalausweis konnte die Identitätsverifikation für hoheitliche Anwendungen etwa bei der Grenzkontrolle automatisiert, damit gleichzeitig verbessert und beschleunigt werden. Aus modernen Reiseprozessen und anderen hoheitlichen Anwendungen ist die Biometrie nicht mehr wegzudenken.

Den größten Erfolg hat die Biometrie allerdings im Consumer-Bereich: Mit dem Aufstieg des Smartphones zum zentralen Alltagswerkzeug für alle haben sich hier biometrische Verfahren aufgrund ihrer Benutzerfreundlichkeit und breiten Akzeptanz zur zentralen Authentisierungstechnik entwickelt. Die fortschreitende Digitalisierung und Automatisierung in Staat und Gesellschaft erhöhen ihre Bedeutung weiter, so dass sie auch beim Onlinebanking

und in E-Government-Anwendungen für die Authentisierung genutzt werden können.

### **Biometrische Verfahren müssen sicher sein**

Biometrische Systeme sind einfach anzuwenden, schwierig hingegen ist die Prüfung ihrer realen Sicherheit. Diese wird von der biometrischen Erkennungsgenauigkeit (Performanz), der Resistenz gegen Überwindungsangriffe (Überwindungssicherheit, z. B. mit Fälschungen) und auch von der korrekten Bedienung durch die Nutzerinnen und Nutzer (Usability) bestimmt und lässt sich in der Regel nur mit einem sehr großen Aufwand ermitteln.

- Die biometrische Performanz kann ausschließlich mit umfangreichen, praxisnahen Funktionstests mit möglichst vielen unterschiedlichen Testpersonen abgeschätzt werden.
- Die Überwindungssicherheit biometrischer Systeme muss mit möglichst vielen Angriffsvarianten von erfahrenen Evaluatorinnen und Evaluatoren geprüft werden (Schwachstellenanalyse), um belastbare Erkenntnisse zu gewinnen.
- Usability-Aspekte lassen sich ebenfalls nur mit zahlreichen Testpersonen und mit ausgefeilten Prüfkonzepnten untersuchen.

Aufgrund der hohen technischen Komplexität biometrischer Systeme können solche Untersuchungsergebnisse kaum von einem System auf ein anderes übertragen oder simuliert werden und müssen mit jeder signifikanten Änderung an Soft- und Hardware stets neu und unter möglichst praxisnahen Umgebungsbedingungen ermittelt werden.

### **BEZ treibt Biometrieforschung voran**

Das Ziel des Biometrie-Evaluations-Zentrums (BEZ) ist es, genau diese Evaluationen von Performanz, Überwindungssicherheit und Usability durchzuführen. Im November 2021 konnten sich, zusammen mit zahlreichen Medienvertretern, der Präsident der Hochschule Bonn-Rhein-Sieg (H-BRS), Prof. Hartmut Ihne, und der Präsident des BSI, Arne Schönbohm, davon überzeugen, wie im BEZ die Sicherheit biometrischer Verfahren für hoheitliche und kommerzielle Anwendungen evaluiert und praxisorientiert weiterentwickelt wird.

Der Aufbau und gemeinsame Betrieb des BEZ ist das Ergebnis der vor mehr als 13 Jahren begonnenen Kooperation zwischen der H-BRS und dem BSI auf dem Gebiet der Biometrie. In dieser Zeit sind zahlreiche gemeinsam betreute Abschlussarbeiten und Kooperationen in Forschungs- und Entwicklungsprojekten entstanden, die ebenfalls zu einer engen und vertrauensvollen Zusammenarbeit zwischen der Cyber-Sicherheitsbehörde des Bundes und der angesehenen Forschungsinstitution geführt haben.

Aus der Sicht des BSI ist das Evaluations-Zentrum in seiner jetzigen Form genau die richtige Antwort auf die besonderen Herausforderungen, die durch den vielseitigen Einsatz biometrischer Verfahren mit wachsenden Sicherheitsanforderungen entstanden sind.

### Evaluation im kontinuierlichen Dauerbetrieb

Das BEZ ist das erste deutsche dedizierte Kompetenzzentrum für Biometrie-Evaluation. Dort wird, neben den üblichen sporadischen Massentests mit möglichst vielen Testpersonen, ein kontinuierlicher Dauertestbetrieb mit relativ wenigen Testpersonen (zwischen 100 und 150) umgesetzt, der dafür mit vielen Wiederholungen über

neue Sicherheitstechnologien entwickelt sowie Hersteller, Forscherinnen und Forscher, Prüflabore und Consumer kompetent beraten.

Die H-BRS bildet in der Zusammenarbeit die Schnittstelle zu angewandter Forschung und Entwicklung und zum wissenschaftlichen Netzwerk in der Biometrie. Für die angewandte Forschung der Hochschule bietet die Zusammenarbeit mit dem BSI die Gelegenheit für einzigartige Einblicke in die Anforderungen der Praxis, für eine hocheffiziente Entwicklungsbegleitung und zu direkten Vergleichen mit den besten Systemen aus hoheitlichen Anwendungen.



*Evaluation der BSI-Schleuse aus dem Forschungsprojekt Facetrust zur Entwicklung neuer Sicherheitstechnologien*

mehrere Jahre besonders tiefgehende Analysen ermöglicht. Mit diesem Dauertestkonzept können biometrische Systeme sehr viel zeitnaher untersucht, Entwicklungsergebnisse stets mit dem Stand der Technik abgeglichen und dabei die natürliche Variation der Testpersonen über die Zeit in den Analysen berücksichtigt werden.

Die geografische Lage des BEZ auf dem Campus der Hochschule Bonn-Rhein-Sieg in Sankt Augustin bei Bonn bietet für diese Analysen potenziell Zugang zu bis zu 9.000 Studierenden sowie rund 1.000 Mitarbeitenden. Die Nähe zu einem großen Einkaufszentrum sowie zu Schulen und Altenheimen erleichtert zudem die Anwerbung von weiteren Testpersonen.

Für das BSI ergibt sich durch die Kooperation mit dem BEZ die Möglichkeit, Fragestellungen aus der hoheitlichen Praxis kurzfristig zu bearbeiten und regelmäßige Marktanalysen zu betreiben. Auf Basis dieser Erkenntnisse werden Prüfmethode für Sicherheitszertifizierungen und

Dabei hat das BSI die Aufgabe übernommen, für einen besonders umfassenden Datenschutz im BEZ zu sorgen. Ein speziell dafür entwickeltes Sicherheits- und Datenverarbeitungskonzept gewährleistet ein hohes Maß an Datensicherheit für die personenbezogenen Daten der Testpersonen (nach EU-DSGVO) und Vertraulichkeit der sensiblen Analyseergebnisse gegenüber Herstellern sowie für hoheitliche und kommerzielle Partner von BSI und H-BRS.

Strategisches Ziel ist es, das BEZ als herstellerunabhängige Instanz für Anwenderinnen und Anwender, für Entscheiderinnen und Entscheider, Hersteller, Forschungsinstitute und Zertifizierungsstellen zu etablieren. Das Evaluations-Zentrum ist dabei ein wichtiges Beispiel für strategische Allianzen des BSI, um die fortschreitende Digitalisierung sicher und nachhaltig zu gestalten. ■

# Die Neupositionierung des IT-Grundschatzes in der Bundesverwaltung

## Das BSI stärkt die Informationssicherheit in der Bundesverwaltung

Interview mit Konstantin Beck und Claudia Gola, Referat Informationssicherheitsberatung am Standort Sachsen

Die Anzahl und die Komplexität der Angriffe im Cyber-Raum steigen. Besonders im Fokus stehen Behörden, die immer häufiger zu Zielen von Attacken werden. Umso wichtiger ist es, den Reifegrad der Informationssicherheitsmanagementsysteme (ISMS) der Bundesverwaltung weiter zu erhöhen. Das Projekt „Neupositionierung des IT-Grundschatzes für die Bundesverwaltung“ will den IT-Grundschatz in der Fläche stärken und die Umsetzung für die Anwenderinnen und Anwender vereinfachen. Wir haben mit dem Projektleiter Konstantin Beck und der stellvertretenden Projektleiterin Claudia Gola über das Projekt gesprochen.

### Vor welchem Hintergrund ist das Projekt entstanden?

**Konstantin Beck:** Informationssicherheit ist wie eine Kette: Sie ist nur so stark wie ihr schwächstes Glied. Mit steigendem Grad der Digitalisierung in der Bundesverwaltung steigen auch die Anforderungen an die Informationssicherheit. Die Systeme werden komplexer und sind stärker miteinander vernetzt. Zudem können gegenseitige Abhängigkeiten untereinander bestehen. Das führt zu einer akuterer Bedrohung der Systeme in der Bundesverwaltung. Es ist unsere Aufgabe, dafür zu sorgen, dass die einzelnen Glieder der Kette sicher halten.

Vor diesem Hintergrund wurde im Umsetzungsplan Bund für alle Ressorts und Bundesbehörden der IT-Grundschatz als verbindlicher Standard festgelegt. In jährlichen Sachstandsberichten wird der Reifegrad der ISMS der Behörden abgefragt. So konnten Potenziale identifiziert werden, den Reifegrad der Behörden weiter zu erhöhen und den IT-Grundschatz in der Breite zu stärken.

### Auf wessen Initiative ist das Projekt entstanden?

**Claudia Gola:** Die Initiative für das Projekt ging aus einem Austausch zwischen dem Bundesinnenministerium (BMI) und dem BSI hervor. Wir haben vereinbart, Lösungen für eine stärkere Umsetzung des IT-Grundschatzes gemeinsam zu erarbeiten.

**Welche Ansatzpunkte für eine weitere Stärkung des IT-Grundschatzes sehen Sie und welche Ziele haben Sie sich im Projekt gesetzt?**

**Konstantin Beck:** Zur Ermittlung der konkreten Bedarfe haben wir uns dazu entschieden, zuerst in Kooperation mit dem BMI eine Online-Umfrage unter den Informationssicherheitsbeauftragten (ISBs) der Bundesverwaltung durchzuführen. Sie konnten so ihre Sichtweise darlegen. Aus den Antworten haben wir drei Handlungsfelder abgeleitet:





1. Wir wollen die Anwendung des IT-Grundschutzes in der Bundesverwaltung vereinfachen.
2. Wir erhöhen die Zahl der in der Bundesverwaltung vorhandenen Zertifizierungen nach ISO 27001 auf Basis des IT-Grundschutzes.
3. Wir suchen nach Möglichkeiten, die Toolunterstützung für ISMS zukünftig zu verbessern.

#### *Welche Erkenntnisse nehmen Sie aus der Umfrage noch mit?*

**Claudia Gola:** Die Umfrage hat uns geholfen, die Projektaktivitäten gezielt auf die Bedürfnisse unserer Kunden in der Bundesverwaltung auszurichten.

Die Details können Sie im Ergebnisbericht nachlesen, den wir den ISBs in der AG Informationssicherheit vorgestellt und auch zur Verfügung gestellt haben.

Insgesamt haben wir festgestellt, dass die Ansatzpunkte sehr komplex und multikausal sind. Dabei spielen notwendige Sensibilisierungen eine wichtige Rolle, aber auch Ressourcenmangel, Umfang und Komplexität des Themas sowie Hemmnisse bei der Beschaffung. Diese Vielzahl ist nicht durch einen der beteiligten Akteure allein lösbar.

Das BSI kann hier vor allem Beratung anbieten. Die bestehenden Angebote sollen zugänglicher gemacht werden und weitere Angebote hinzukommen.

Ein für uns sehr erfreuliches Ergebnis waren die vielen positiven Reaktionen der Teilnehmer auf die Umfrage und die Initiative des BSI durch das Projekt.

#### *Was haben Sie sich nun aufgrund der Ergebnisse der Umfrage vorgenommen?*

**Konstantin Beck:** Wir haben einen Arbeitsplan mit Arbeitspaketen zu vier verschiedenen Themenfeldern definiert:

- Im Bereich „Produkte und Services für die Bundesverwaltung“ verbessern wir die Übersicht und Verfügbarkeit der Werkzeuge für die praktische Arbeit und fördern die Vernetzung der ISBs.
- Ziel bei der Umsetzung des IT-Grundschutzes in der Bundesverwaltung ist es, Einstieg und Umsetzung durch gezielte Angebote für die Bundesverwaltung zu vereinfachen.
- Für Zertifizierungen in der Bundesverwaltung werden wir Angebote entwickeln, um mehr Bundesbehörden dazu zu bewegen, eine Zertifizierung anzustreben.
- Das Arbeitspaket „ISMS/IT-Grundschutztools in der Bundesverwaltung“ schließlich befasst sich mit den Möglichkeiten der Umsetzung einer einfacher verfügbaren, anforderungsgerechteren und benutzerfreundlicheren IT-Lösung für die Bundesverwaltung.



# „Informationssicherheit ist wie eine Kette: Sie ist nur so stark wie ihr schwächstes Glied. Mit steigendem Grad der Digitalisierung in der Bundesverwaltung steigen auch die Anforderungen an die Informationssicherheit.“

- Konstantin Beck, Referat Informationssicherheitsberatung am Standort Sachsen

Mir ist es wichtig zu sagen, dass das Projekt nur ein erster Aufschlag ist und auch nach Projektende weiter an den Ursachen gearbeitet werden soll und auch muss. Dafür gibt es beispielsweise die BSI-interne „Task-Force Basis-Absicherung“, die Anforderungen des IT-Grundschutz-Kompendiums für die Basis-Absicherung mit dem Ziel prüft, den Einstieg in den IT-Grundschutz noch „schlanker“ zu gestalten.

**Mit wem arbeiten Sie im Projekt zusammen, um diese ambitionierten Ziele zu erreichen?**

**Claudia Gola:** Das kann nicht ein Referat oder eine Abteilung des BSI allein bewerkstelligen. Deshalb ist uns die Zusammenarbeit besonders wichtig.

Im Projekt arbeiten sieben Referate abteilungsübergreifend zusammen, darunter Beratungsreferate, die Referate für IT-Grundschutz und Zertifizierungen sowie für IT-Sicherheitssysteme und -Produkte und die Referate für Sicherheits- und Servicemanagement.

Die Kooperation funktioniert auch behördenübergreifend. So unterstützt uns z. B. das zuständige Fachreferat im BMI mit der entsprechenden ministeriellen Fachexpertise. Diese kurzen Kommunikationswege ermöglichen es uns, agil und flexibel auf Änderungen zu reagieren. Dazu kommen natürlich auch unsere Kunden, die ISBs der Bundesverwaltung, die wir über Workshops und andere Formate im Projekt beteiligen. ■

## Weitere Informationen:



Ergebnisbericht zur Umfrage in der Bundesverwaltung:  
[https://www.bsi.bund.de/DE/Intern/Sicherheitsberatung/Bund/Publikationen/NIT-GSB/NIT-GSB\\_node.html](https://www.bsi.bund.de/DE/Intern/Sicherheitsberatung/Bund/Publikationen/NIT-GSB/NIT-GSB_node.html)



E-Mail:  
referat-bl13@bsi.bund.de

# Workshop-Reihe: Prüfung von KI-Systemen

**Internationale Expertise zur Regulierung von  
Digitalisierungsanwendungen**

*von Dr. Arndt von Twickel und Dr. Christian Berghoff, Referat Bewertungsverfahren  
für eID-Technologien in der Digitalisierung*



Der Einsatz von Künstlicher Intelligenz (KI) in der Digitalisierung bietet einerseits enorme Chancen, z. B. im Kontext autonomer Fahrzeuge, birgt aber andererseits neue Risiken, die sich bisher nur unzureichend absichern lassen. Um regelmäßig den aktuellen Stand der Forschung, deren praktische Umsetzung und offene Fragen zu erörtern, führt das BSI gemeinsam mit dem TÜV-Verband und dem Fraunhofer Heinrich-Hertz-Institut (HHI) eine jährliche Workshop-Reihe durch. An diesem Austausch beteiligen sich hochrangige internationale Expertinnen und Experten. Die Workshop-Reihe wird in diesem Jahr zum dritten Mal stattfinden.

In den letzten Jahren ist die Leistungsfähigkeit von Systemen auf Basis Künstlicher Intelligenz (KI) stark gestiegen, weshalb sie in immer mehr Anwendungsbereichen zum Einsatz kommen. Hierzu zählen auch sicherheitskritische Anwendungen wie z. B. die Biometrie oder das automatisierte Fahren, in denen Fehlfunktionen gravierende Auswirkungen haben können. KI-Systeme weisen jedoch trotz ihrer enormen Leistungssteigerungen auch verschiedene Risiken auf, die angemessen berücksichtigt werden müssen. Hierzu zählt die oft mangelnde Robustheit gegenüber Veränderungen in den verarbeiteten Eingabedaten, die z. B. beim automatisierten Fahren in Abhängigkeit von der Tageszeit und dem Wetter auftreten. Eine weitere Herausforderung besteht in der Anfälligkeit der KI-Systeme für qualitativ neuartige Angriffe, mit denen Angreifer gezielt unerwünschte Entscheidungen hervorrufen können. Um solche Risiken beim Einsatz von KI-Systemen in der Praxis zu minimieren, sind die passenden Methoden entscheidend. Eine gemeinsame Arbeitsgruppe von BSI und TÜV-Verband entwickelt daher seit Mitte 2019 Anforderungen an KI-Systeme im Mobilitätsbereich.

## **Gemeinsame Workshop-Reihe**

Da viele der hiermit verbundenen Fragen noch Gegenstand der aktuellen Forschungsaktivitäten sind, wurde 2020 mit dem Fraunhofer HHI aus Berlin als weiterem Partner eine gemeinsame Workshop-Reihe ins Leben gerufen. Ziel ist es, einerseits einen bestmöglichen Überblick über den aktuellen Stand der Forschung, der Entwicklung und der praktischen Umsetzung zu erhalten und andererseits ein internationales Netzwerk von Expertinnen und Experten aufzubauen.

## **Workshop 2020 „Auditing AI-Systems: From Basics to Applications“**

Der erste Workshop wurde im Oktober 2020 hybrid durchgeführt: mit 20 Personen in Präsenz in Berlin sowie per Videostream mit über 100 Teilnehmenden. Schwerpunkt hierbei waren die Aufarbeitung von wissenschaftlichen Grundlagen und eine Diskussion zur praktischen Anwendbarkeit. Hierfür konnten hochrangige Referentinnen und Referenten gewonnen werden, u. a. vom MIT und von der ETH Zürich. Es wurden verschiedene Angriffe auf KI-Verfahren sowie mögliche Verteidigungsstrategien



Dirk Schlesinger, Leiter des TÜV AI lab und Chief Digital Officer der TÜV SÜD AG

diskutiert. Die Ergebnisse des Workshops flossen in ein gemeinsames Whitepaper ein. Hierbei kristallisierten sich folgende Kernaussagen heraus: 1. KI-Systeme müssen im Anwendungskontext betrachtet und Zielkonflikte hinreichend berücksichtigt werden; 2. der komplexe Lebenszyklus von KI-Systemen erfordert eine Prüfung und Absicherung auf mehreren Ebenen, von der Planung und Datengewinnung bis zum Update im Betrieb; 3. eine verbesserte Prüfbarkeit und Absicherung lässt sich neben technischen Fortschritten ggf. auch durch eine anwendungsbezogene gezielte Beschränkung der Randbedingungen, z. B. der Wetterbedingungen, erreichen.

#### Workshop 2021 „Auditing AI-Systems: From Principles to Practice“

Der zweite Workshop wurde im Oktober 2021 erneut hybrid mit 20 Personen vor Ort und über 100 Teilnehmenden im Livestream ausgerichtet. Die Umsetzung erster Absicherungs- und Prüfansätze in praktischen Projekten ermöglichte es, den Fokus stärker auf den Austausch von Erfahrungen bei der Umsetzung zu legen. Insbesondere wurden hierzu Projekte aus den Bereichen Mobilität, Gesundheit und Biometrie betrachtet. Die Ergebnisse wurden im Kontext des im April 2021 von der EU-Kommission veröffentlichten Verordnungsentwurfs zur KI diskutiert, u. a. mit einer Vertreterin der EU-Kommission und Vertretern aus Industrie und Forschung. Die KI-Verordnung der EU wird besonders Hochrisiko-KI-Systemen, z. B. im Mobilitätsbereich, weitreichende Anforderungen auferlegen. Vor der geplanten Operationalisierung der KI-Verordnung innerhalb der kommenden zwei bis drei Jahre sind allerdings noch wesentliche technische Fragen zu klären, um angemessen detaillierte Anforderungen

zu formulieren und hinreichend genaue Prüfverfahren zu entwickeln. Auf Basis der Ergebnisse aus dem Workshop wurde in einem Whitepaper eine Bestandsaufnahme zur Prüfbarkeit von KI-Systemen vorgenommen.

#### Ausblick

Durch die Workshop-Reihe „Prüfung von KI-Systemen“ leistet das BSI gemeinsam mit seinen Partnern und internationalen Expertinnen und Experten einen wichtigen Beitrag, um den Einsatz von KI-Systemen in Zukunft überprüfbar sicher zu gestalten. Der nächste Workshop ist für November 2022 geplant. Entsprechende Informationen und ein Anmeldelink werden rechtzeitig auf der BSI-Webseite zur Verfügung gestellt. ■

#### Weitere Informationen:



Whitepaper „Towards Auditable AI Systems“ (2022)  
[https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Towards\\_Auditable\\_AI\\_Systems\\_2022.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Towards_Auditable_AI_Systems_2022.pdf)



Whitepaper „Towards Auditable AI Systems“ (2021)  
[https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Towards\\_Auditable\\_AI\\_Systems.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Towards_Auditable_AI_Systems.pdf)



EU-Verordnungsentwurf  
<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

# NESAS als 5G-Zertifizierungsverfahren

## Sicherheit für den Mobilfunkstandard der nächsten Generation

von Thomas Rahimi und Stefan Gottschalk, Referat Zertifizierung von Netzwerkkomponenten und Beschleunigte Sicherheitszertifizierung, und Dr. Helge Kreuzmann, Referat Anerkennung und Zertifizierung von Stellen und Personen

Durch neue Anwendungsfälle und einen erweiterten Funktionsumfang in der 5. Generation des Mobilfunkstandards (5G) spielt die IT-Sicherheit moderner Mobilfunknetze eine immer wichtigere Rolle. Die in 5G angestrebte Verlagerung einzelner Netzfunktionen von Hardware hin zu softwarebasierten und virtualisierten Funktionen mit immer kürzeren Release-Zyklen führt zu neuen Sicherheitsanforderungen. Das Network Equipment Security Assurance Scheme (NESAS) soll diese Anforderungen bedienen und eine gemeinsame Basis schaffen, um das IT-Sicherheitsniveau branchenweit zu erhöhen.

**N**ESAS ist ein von der Groupe Speciale Mobile Association (GSMA) und dem 3rd Generation Partnership Project (3GPP) unter Mitwirkung global operierender Mobilfunkhersteller, Netzbetreiber und Anbieter entwickeltes Rahmenwerk zur Überprüfung, Gewährleistung und Verbesserung der IT-Sicherheit in der Mobilfunkbranche.

### Vom Bewertungs- zum Zertifizierungsschema

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat das GSMA-NESAS-Bewertungsschema zu einem nationalen Zertifizierungsschema weiterentwickelt, damit Hersteller ein IT-Sicherheitszertifikat für 5G-Mobilfunkausrüstung erlangen können. Das NESAS Cybersecurity Certification Scheme – German Implementation (NESAS CCS-GI) ermöglicht es Herstellern, die Einhaltung von geforderten Sicherheitseigenschaften durch ein deutsches IT-Sicherheitszertifikat nachzuweisen. Dafür wurden die für die Zertifizierung und zur Einhaltung nationaler gesetzlicher Vorgaben notwendigen Prozessschritte ergänzt und angepasst.

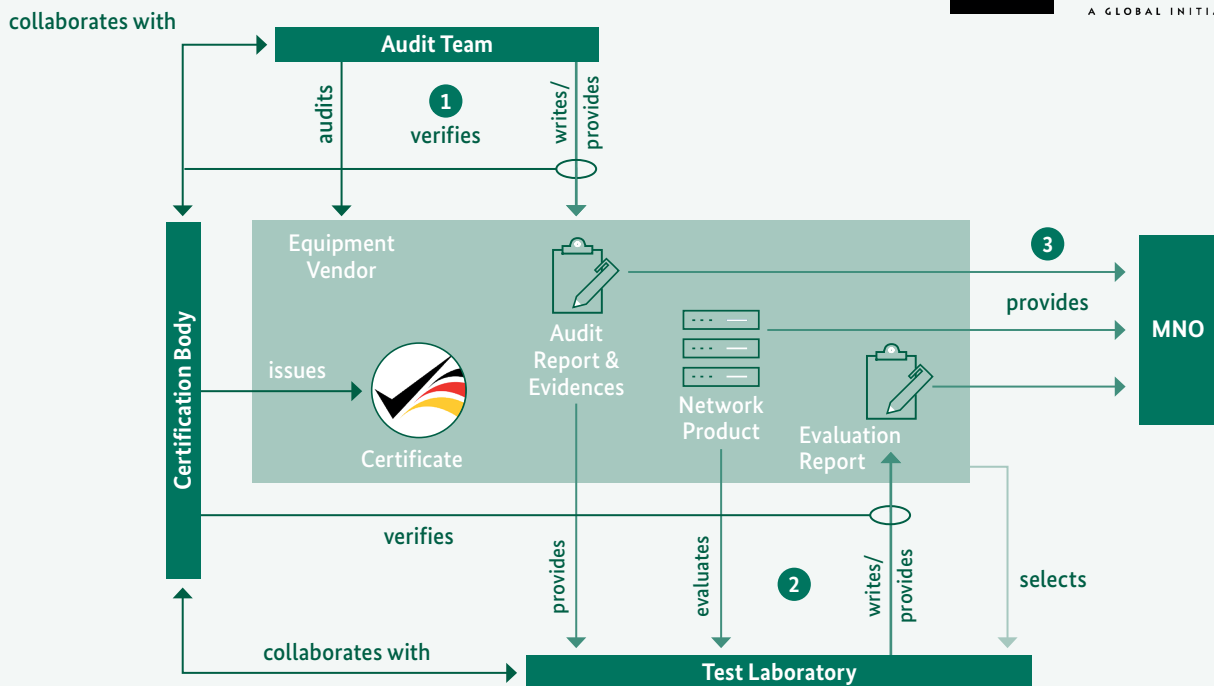
Möchte ein Antragssteller ein NESAS-CCS-GI-Produktzertifizierungsverfahren durchlaufen, muss er eine Prüf-

stelle mit der Produktevaluierung beauftragen und kann anschließend einen Zertifizierungsantrag stellen. Die Zertifizierungsstelle überprüft, ob sich das Produkt für eine Zertifizierung eignet, und beginnt im positiven Fall das Zertifizierungsverfahren. Das NESAS-Schema betrachtet nicht ausschließlich die Sicherheitsleistung des Netzwerkproduktes, sondern überprüft auch die Einhaltung von Sicherheitsanforderungen an die Produktentwicklungs- und Lebenszyklusprozesse. Dieses Vorgehen soll dazu beitragen, Sicherheitsprinzipien von Beginn an auch prozessual zu verankern und Updates zu ermöglichen. Die Bewertung untergliedert sich daher in die zwei aufeinander aufbauenden Teilbereiche Prozessaudit und Produktevaluation.

### Der Einsatz von externen Schemadokumenten

NESAS CCS-GI ist auf der Basis des GSMA-NESAS-Bewertungsschemas entstanden und nutzt zugleich die SCAS-Tests des 3GPP. Bei der Erstellung wurde darauf geachtet, eine möglichst hohe Kompatibilität mit dem Bewertungsschema der GSMA zu wahren. Um zukünftige Anpassungen der GSMA-Dokumente zu berücksichtigen, werden in den Schemadokumenten von NESAS CCS-GI die Dokumente der GSMA und die SCAS-Tests des

## specifies NESAS (methodology and requirements) FS.xx



## TSG SA3 specifies SCAS (security requirements, test cases) TS33.xxx

Abbildung 1: Die Abbildung stellt das Zusammenwirken der Partner, die am Zertifizierungsprozess beteiligt sind, dar. Weiterhin werden die Organisationen, welche die zur Anwendung kommenden Schemadokumente, Methoden und Sicherheitsanforderungen erstellen, gezeigt

3GPP referenziert. Aktualisierungen der externen Dokumente werden durch das BSI beobachtet und einem Bewertungsprozess unterzogen, bevor sie zu einem bestimmten Zeitpunkt in NESAS CCS-GI übernommen werden. Das Eingangsdatum eines Zertifizierungsantrages bestimmt die angewendeten Versionen der externen, referenzierten Dokumente.

Zusätzliche Anforderungen an Methoden sowie Präzisierungen und Ergänzungen von Sicherheitsanforderungen werden in Anwendungshinweisen zum Schema (AIS) dokumentiert. Durch eine Beteiligung in Standardisierungsgruppen der GSMA und des 3GPP werden diese Anpassungen für nachfolgende Versionen der externen Dokumente vorgeschlagen. Auf diesem Weg lässt sich auch der Bedarf an zusätzlichen Prüfkriterien für Mobilfunkausrüstung in die etablierten Gremien einbringen, für die es eventuell noch keine Prüfkriterien gibt.

Die aufeinander aufbauenden Prüfschritte sowie die Wiederverwendung von Auditergebnissen für Produkte, die nach denselben Prozessen entwickelt wurden, tragen dazu bei, kürzer werdende Release-Zyklen bei der

Bewertung der IT-Sicherheitsleistung eines Produktes für 5G-Mobilfunkausrüstung zu berücksichtigen. Durch die Adaption eines etablierten Bewertungsschemas und die Mitwirkung in diversen Gremien lassen sich die nationalen Bedarfe an zertifizierter Mobilfunkausrüstung genauso berücksichtigen wie die Ansprüche international agierender Hersteller bezüglich der Einsatzfähigkeit von Hard- und Software. ■



Abbildung 2: Das Signet für das nationale Zertifizierungsverfahren NESAS CCS-GI ist auf der Zertifizierungsurkunde sowie im Zertifizierungsbutton auf zertifizierten Produkten abgebildet

## Weitere Informationen:



[https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-NESAS/NESAS-CCS-GI\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-NESAS/NESAS-CCS-GI_node.html)

# Die vernetzte Stadt

## Informationssicherheit für Smart Cities

von Kilian Mitterweger, Referat Cyber-Sicherheit in Smart Home und Smart Cities

Die Begriffe „Smart City“ und „Smart Region“ werden mit der Vorstellung verbunden, Informations- und Kommunikationstechnologien (IKT) zu nutzen, um Teilhabe und Lebensqualität in urbanen und ländlichen Räumen zu erhöhen und sie ökonomisch, ökologisch und sozial nachhaltiger zu gestalten. Die Informationssicherheit als das Kernthema des BSI spielt für den Erfolg zugehöriger Digitalisierungsprojekte eine entscheidende Rolle.

**I**m Rahmen des Transformationsprozesses, der mit der Umsetzung von „Smart City“-Konzepten einhergeht, werden bestehende und neue Informationsquellen digital erschlossen und vernetzt. Das können klassische Geoinformationen oder Verwaltungsdaten, aber auch Sensordaten aus dem Verkehrssektor, der Wasser- und Energieversorgung, dem Abfall- und Wertstoffmanagement oder dem Umweltmonitoring sein.

Die Vernetzung von Informationen verschiedener Akteure steht im Zentrum einer „Smart City“-Vision. Sie ermöglicht

sektorenübergreifende Anwendungsfälle, die in Ihrer Vielfalt bislang nicht vollständig untersucht und praktisch erprobt sind. So gilt beispielsweise die Koppelung verschiedener Bereiche der Energieversorgung (wie Strom und Wärme) und der Mobilität unter Nutzung von sensordatenbasierten Prognosen und digitalisierten Märkten als ein Schlüssel zu einer wirtschaftlichen, klimaneutralen und stabilen Energieversorgung. In der Vernetzung liegt zugleich die konzeptionell größte Herausforderung, die bei weitem nicht nur technische Fragestellungen betrifft. So werden beispielsweise auch Fragen bezüglich einer innovations-



freundlichen und sozialverträglichen Monetarisierung von (Teil-)Diensten, der Daten-Governance und dahinterliegender rechtlicher und organisatorischer Rahmenbedingungen aufgeworfen.

#### Herausforderung Informationssicherheit

Mit der Vielzahl an Möglichkeiten entstehen neue Herausforderungen in Bezug auf die Informationssicherheit, deren Stärkung eine Kernaufgabe des BSI ist. Dabei stehen die Integrität der verarbeiteten Informationen und der informationsverarbeitenden Systeme, die Verfügbarkeit dieser Informationen und digitaler Prozesse sowie, insbesondere im Kontext personenbezogener Daten, deren Vertraulichkeit im Zentrum. Das Bedrohungspotenzial für die Integrität und Verfügbarkeit steigt mit dem Grad der Vernetzung, das Ausmaß möglicher Schäden durch Cyber-Sicherheitsrisiken mit dem Digitalisierungsgrad. Die Notwendigkeit, ein angemessenes Cyber-Sicherheitsniveau zu etablieren, wird deutlich sichtbar. Zudem erfordert beispielsweise die Digitalisierung von Verwaltungsdienstleitungen im Rahmen des Onlinezugangsgesetzes, insbesondere zur Umsetzung des „Once-only-Prinzips“, besondere Maßnahmen zum Schutz der Vertraulichkeit von relevanten Daten.

#### Das BSI gestaltet Informationssicherheit in der Digitalisierung

Um die Informationssicherheit in „Smart Cities“ und „Smart Regions“ zu gestalten, hat das BSI neben sektorspezifischen Richtlinien, wie beispielsweise der BSI TR-03164 für intelligente Transportsysteme, und Richtlinien für regulierte Sektoren, wie die BSI TR-03109-1 für die Kommunikationseinheit eines intelligenten Messsystems, auch Handlungsempfehlungen zur Informationssicherheit für kommunale IoT-Infrastrukturen veröffentlicht. Letztere unterstützen Entscheidungstragende und operativ Verantwortliche für kommunale IoT-Projekte von ersten Experimenten bis hin zum Betrieb und zur späteren

Außerbetriebnahme von IoT-Infrastrukturen bei der Bereitstellung nachhaltig sicherer Lösungen. Darüber hinaus werden weiterführende Informationen für tiefergehende Betrachtungen referenziert. Der Fokus liegt hierbei auf den organisatorischen Rahmenbedingungen als Voraussetzung für den Aufbau technisch sicherer Systeme. Daneben ist für die Informationssicherheit jedoch auch die Verfügbarkeit von (nachweislich) sicheren IT-Komponenten auch abseits der bezüglich Informationssicherheit regulierten Sektoren entscheidend. Um die dafür notwendigen Anforderungen zu identifizieren, bedarf es technisch tiefergehender Analysen.

#### IoT-Netze und Datenplattformen als technische Grundlage

IoT-Infrastrukturen lassen sich in IoT-Netze und in Datenplattformen aufteilen. Während IoT-Netze wie LoRaWAN eine (teils sektorspezifische) Infrastruktur zur Kommunikation und zum Management verteilter IoT-Geräte bereitstellen, sind Datenplattformen die zentrale Komponente für einen einheitlichen Datenzugang insbesondere für sektorübergreifende Anwendungsfälle. Für IoT-Netze besteht die Aufgabe darin, die Informationssicherheit trotz vieler, teilweise physisch zugänglicher IoT-Geräte sicherzustellen. Im Kontext von Datenplattformen stehen dabei die Informationssicherheitsaspekte des Cloud-Computings und der Verfügbarkeit von integrierten Daten im Vordergrund.

#### Ausblick

All diese Überlegungen stehen im Zentrum aktueller Planungen zur Erstellung von Sicherheitsstandards in den genannten Bereichen. Zusammen mit geeigneten Prüfkriterien entsteht so die Grundlage für nachweisbar sichere Komponenten zum Aufbau und Betrieb kommunaler IoT-Infrastrukturen. Neben den erwähnten Handlungsempfehlungen, den bereits etablierten Sicherheitsstandards wie dem IT-Grundschutz-Kompendium und dem Angebot der Sicherheitszertifizierung für Managementsysteme und IT-Produkte entstehen auf diese Weise weitere Bausteine für informationstechnisch sichere, smarte Städte und Regionen. ■

#### Weitere Informationen:



[https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03164/TR-03164\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03164/TR-03164_node.html)



[https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/TechnRichtlinie/TR\\_03109-1\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Smart-Meter-Gateway/TechnRichtlinie/TR_03109-1_node.html)



[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartCity/Handlungsempfehlungen\\_Smart\\_City.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartCity/Handlungsempfehlungen_Smart_City.pdf)



# Cyber-Sicherheit in der öffentlichen Verwaltung

**Boris Pistorius, Minister für Inneres und Sport in Niedersachsen, und BSI-Präsident Arne Schönbohm über Herausforderungen und erfolgreiche Synergien**

*Öffentliche Verwaltungen, Krankenhäuser oder Energieversorger – all diese Kritischen Infrastrukturen wurden schon Opfer von schweren Cyber-Angriffen. Wie groß ist die Gefahr, dass in Niedersachsen aufgrund eines solchen Angriffs einmal alle Menschen tagelang im Dunkeln sitzen, keinen Strom haben oder sogar Kraftwerke implodieren? Und was tun Sie dagegen?*



**Boris Pistorius:** Eine 100-prozentige Sicherheit gibt es nicht, dafür sind die Bedrohungen zu komplex und die technischen Veränderungen zu schnell. Wesentliche Faktoren bei der Abwehr solcher Angriffe sind etwa die Größe der Netzwerkstrukturen, die technische Ausstattung oder auch der praktische Umgang mit Cyber-Sicherheit der angegriffenen Organisation und auch, wie gut die Mitarbeiterinnen und Mitarbeiter für den Fall eines Cyber-Angriffs geschult werden. Die öffentliche Verwaltung schützen wir bei uns dadurch, dass wir möglichst optimale technische Voraussetzungen bei Hard- und Software schaffen und moderne, dem Stand der Technik entsprechende Systeme einsetzen, die von Profis betreut werden. Im Niedersächsischen Computer Emergency Response Team (N-CERT) sind echte Spezialisten für die Abwehr von Cyber-Angriffen auf Behörden beschäftigt, die mit ihrer Expertise, mit Rat und Tat die IT-Betriebe unterstützen. Unternehmen und Betreiber Kritischer Infrastrukturen wie Energieversorger beraten wir außerdem mit der Zentralen Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes und dem Wirtschaftsschutz des Verfassungsschutzes.

*Wie können Verbraucherinnen und Verbraucher ihre Identitäten, Daten und die eigenen Netzwerke und Angriffspunkte im Haushalt, wie den Router, vernetzte Fernseher oder Sprachsteuerungssysteme wie Echo-Boxen, schützen?*

**Pistorius:** Die Wahrheit ist doch, dass digitale Produkte im Privaten häufig leichtfertig verwendet werden. Kleine Kinder wachsen inzwischen mit Alexa, Siri und so weiter auf, sie kommunizieren mit der KI, das ist Technik, die Spaß macht, das Leben einfacher macht und in der Anschaffung inzwischen ziemlich günstig ist. Um den Menschen dabei zu helfen, zu erkennen, wo sie vorsichtig sein müssen, gibt es

den Ratgeber Internetkriminalität des Landeskriminalamtes – und viele ähnliche Angebote, etwa auch auf der Homepage des LKA und des BSI. Hier kann man sich über aktuelle digitale Trends, Gefahren und die Prävention informieren.

Ein wichtiger Schritt ist außerdem, dass es für alle Verbraucherinnen und Verbraucher jetzt ein verlässliches IT-Sicherheitskennzeichen gibt, mit dem Sicherheitseigenschaften von IT-Produkten leichter beurteilt werden können. Bei einem Auto oder Kühlschrank gibt es das bereits seit Jahrzehnten. Ich hoffe sehr, dass im Bereich netzfähiger Geräte diese Kennzeichnung zum Standard wird und damit zu deutlich mehr Transparenz im Verbrauchermarkt beiträgt.

*Sind meine persönlichen Daten in Finanzämtern, Bürgerämtern usw. sicher?*

**Pistorius:** Wir sind als öffentliche Hand dazu verpflichtet, sorgsam mit diesen Daten umzugehen. Dies gilt analog und digital. Der Bereich ist mir sehr wichtig, denn hier geht es um das Vertrauen, das die Menschen in uns als ihre Verwaltung setzen. Wir tun dafür seit Jahren sehr viel, um dem gerecht zu werden. Insbesondere das Gesetz über digitale Verwaltung und Informationssicherheit von 2019 ist ein echter Meilenstein für die Sicherheit der digitalen Verwaltung in Niedersachsen. Auch die Datenschutzgrundverordnung verlangt klare technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten durch die Behörden. Ein Großteil der Daten liegt in den Bürgerämtern und Kommunalverwaltungen, mit denen wir intensiv zusammenarbeiten und die wir beraten.

## Kurzvita Boris Pistorius

Boris Pistorius (Jahrgang 1960) ist seit Februar 2013 Niedersächsischer Minister für Inneres und Sport. Seit November 2017 ist er Mitglied des Niedersächsischen Landtages, seit Oktober 2017 Mitglied im parlamentarischen Kontrollausschuss für Europol. Pistorius ist zudem seit Juni 2017 Sprecher der SPD-geführten Innenressorts der Länder.



*Öffentliche Verwaltungen, Krankenhäuser oder Energieversorger – all diese kritischen Infrastrukturen wurden schon Opfer von schweren Cyber-Angriffen. Wie groß ist die Gefahr, dass in Deutschland aufgrund eines solchen Angriffs einmal alle Menschen tagelang im Dunkeln sitzen, keinen Strom haben oder sogar Kraftwerke implodieren? Und was tun Sie dagegen?*



**Arne Schönbohm:** Da möchte ich unbedingt beruhigen. Gerade weil all diese von Ihnen genannten Einrichtungen sogenannte KRITIS-Bereiche sind. Das bedeutet, sie unterliegen ab einer bestimmten Größe der Gesetzgebung und damit der Regulierung der als kritisch definierten Infrastruktur. Damit müssen sie uns als BSI z. B. regelmäßig nachweisen, dass sie ihre IT-Infrastruktur nach dem Stand der Technik absichern.

Im Mittelpunkt der meisten Cyber-Angriffe stehen Unternehmen. Cyber-Kriminelle sind meist Erpresser, die finanzielle Interessen haben. Sie legen ganze Unternehmen und Einrichtungen lahm und erpressen diese dann, u. a. auch mit entwendeten Daten. Ein paar Zahlen: Allein zwischen Mai 2020 und Mai 2021 wurden 144 Millionen neue Schadprogramm-Varianten registriert. Das sind 22 Prozent mehr als im Jahr zuvor. Der höchste jemals gemessene durchschnittliche Tageszusatz lag bei 553.000 neuen Schadprogramm-Varianten. Rund 44.000 E-Mails mit Schadprogrammen wurden von uns in deutschen Regierungsnetzen pro Monat abgefangen, bevor sie die Postfächer der Empfänger erreichten. Von diesen Methoden sind immer wieder auch Kommunen oder Krankenhäuser betroffen, die eben nicht unter die genannten gesetzlichen Regelungen fallen. Bislang haben wir es geschafft, unsere Kritischen Infrastrukturen gut zu schützen. Mit präventiven Maßnahmen oder schneller Krisenreaktion. Aber die Angreifer entwickeln sich immer weiter, daher dürfen wir alle keine Sekunde in dem Bemühen nachlassen, das IT-Sicherheitsniveau weiter zu erhöhen. Und deswegen ist die enge Zusammenarbeit auch auf Bund-Länder-Ebene so wichtig.

*Wie können Verbraucherinnen und Verbraucher ihre Identitäten, Daten und die eigenen Netzwerke und Angriffspunkte im Haushalt, wie den Router, vernetzte Fernseher oder Sprachsteuerungssysteme wie Echo-Boxen, schützen?*

**Schönbohm:** Mit gesundem Menschenverstand und tatsächlich etwas Disziplin. Das will ich erklären. Es ist wie immer im Leben. Wir alle wissen, Sport ist gesund, aber die Couch ist bequemer. Disziplin bedeutet hier: Informieren Sie sich, z. B. über unseren BSI-Podcast, auf Instagram oder auf unseren gut verständlichen und sehr praxisorientierten Verbraucherseiten auf unserer Website. Sichern Sie Ihren Heimrouter einmal mit unserer

Anleitung ab, denn das Standardpasswort auf der Rückseite des Geräts ist alles andere als sicher. Bei E-Mails von der Bank ohne Anlass kann ein einfacher Tipp helfen: Schauen Sie auf die E-Mail-Adresse des Absenders. Ganz schnell zeigt sich da, dass die Sparkasse nicht in Buxtehude sitzt, sondern sehr weit außerhalb Deutschlands.

*Sind meine persönlichen Daten in Finanzämtern, Bürgerämtern usw. sicher?*

**Schönbohm:** Sowohl Finanzämter als auch Bürgerämter sind kommunale Einrichtungen, das bedeutet, dass sie nicht unter unsere Zuständigkeit für den Bund fallen. Allerdings haben wir sehr fähige Einheiten bei uns im Haus, die speziell Kommunen und Länder beraten. Gemeinsam mit den kommunalen Spitzenverbänden wurde auch ein eigenes IT-Grundsicherheitsprofil für Kommunen entwickelt, ein Leitfaden, mit dem Schritt für Schritt die nötigen Absicherungsmaßnahmen umgesetzt werden können. Das allerdings müssen die Kommunen dann auch selbst tun.

Leider müssen wir feststellen, dass es immer wieder auch Angriffe auf kommunale Einrichtungen gibt. Wir nehmen bei diesem Thema aber auch eine deutlich gestiegene Aufmerksamkeit für die Gefahren wahr, sowohl bei den Städten und Landkreisen als auch bei ihren Verbandsvertretungen und der Politik insgesamt. Das freut mich sehr und als BSI werden wir auch in Zukunft unsere Beratung und Unterstützung anbieten. ■

### Kooperationsvereinbarungen für intensive Bund-Länder-Zusammenarbeit

Niedersachsen ist das erste Bundesland, mit dem das BSI im November 2021 eine Verwaltungsvereinbarung abgeschlossen hat. Ziel der intensiven Kooperation ist es, die Cyber- und Informationssicherheit in einem Bundesland zu stärken und die enge Zusammenarbeit auszubauen. In der Vereinbarung mit dem Land Niedersachsen sind 17 Kooperationsfelder festgelegt. Dazu gehören Penetrationstests, forensische Analysen, gemeinsame Veranstaltungen und Hospitationen.

BSI-Ansprechpartnerinnen und -Ansprechpartner an den unterschiedlichen Standorten tauschen sich im Rahmen einer Kooperationsvereinbarung noch intensiver mit den Ländern aus. Eine Kooperationsvereinbarung ist rechtlich verbindlich.

# Schwachstellen in Produkten und ihre Auswirkungen auf die Lieferkette

## Wie ein offener Standard für mehr Sicherheit sorgt

von Thomas Schmidt und Jens Cordt, Referat Industrielle Steuerungs- und Automatisierungssysteme

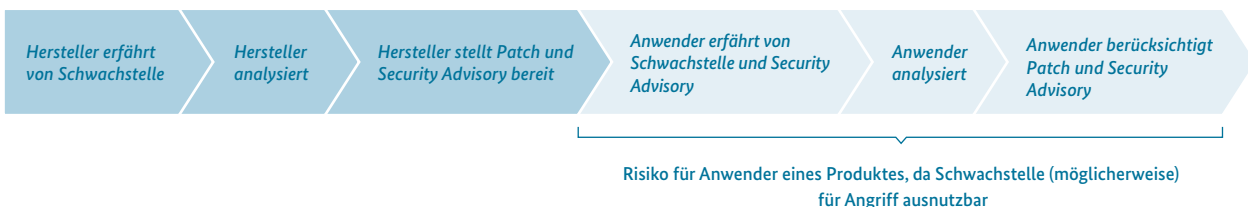
Die zeitnahe Installation von Sicherheitspatches oder Umsetzung mitigierender Maßnahmen sind eine Voraussetzung zur Absicherung von IT-Systemen und industriellen Steuerungsanlagen. Dennoch geschieht dies im Moment immer noch viel zu selten oder mit erheblicher Verzögerung. Abhilfe schaffen kann hier die Nutzung des internationalen Standards Common Security Advisory Framework (CSAF), an dem auch das BSI mitgearbeitet hat.

Die Behebung von Schwachstellen ist stets ein Wettlauf zwischen Unternehmen, die Soft- und Hardware entwickeln (Hersteller), sowie Unternehmen, die diese nutzen (Anwender/Kunden), und Angreifern (siehe Artikel auf S. 14). Es geht um Schnelligkeit und den sorgsam Umgang mit vorhandenen Ressourcen.

### Lebenszyklus einer Schwachstelle

Im einfachsten Fall erfährt ein Hersteller von einer Schwachstelle durch eigene Untersuchungen oder erhält eine Meldung im Rahmen einer koordinierten Schwachstellenveröffentlichung (Coordinated Vulnerability Disclosure, kurz: CVD). Eine ausführlichere Betrachtung findet sich in der Cyber-Sicherheitsempfehlung „Lebenszyklus einer Schwachstelle“. Der Hersteller analysiert

den Ausgangspunkt für die Maßnahmen bei den Kunden dar. Jeder Kunde muss entsprechende Gegenmaßnahmen umsetzen (z. B. den Patch installieren). Da sich die Einsatzbedingungen in jedem Unternehmen unterscheiden und auch Updates weitere Konsequenzen nach sich ziehen können, sind Auswirkungen und Hinweise des Herstellers zu beachten sowie die lokalen Gegebenheiten zu berücksichtigen. In der Zeit zwischen der Veröffentlichung des Security Advisories und der Implementierung der Gegenmaßnahmen steigt das Risiko, dass die Schwachstelle erfolgreich ausgenutzt wird. Denn auch Angreifer erfahren über das Security Advisory und das Update von der Schwachstelle und können ihrerseits damit beginnen, diese zu analysieren und auszunutzen. Daher ist schnelles Handeln notwendig.



die Schwachstelle und behebt diese in seinem Produkt. Anschließend stellt er seinen Kunden ein Security Advisory und einen Patch zur Verfügung. Das Security Advisory dient der Information über die betroffenen Produkte und Versionen sowie die Schwachstelle und zeigt entsprechende Schutzmaßnahmen auf. Dies stellt

### Theorie vs. Praxis

Dieser einfach erscheinende Prozess birgt in der Realität eine Vielzahl von Fallstricken. Einen wesentlichen Aspekt stellt die Lieferkette dar. In dem oben beschriebenen einfachsten Fall gibt es nur einen Hersteller und einen Kunden. Bei der Entwicklung von Software und

Produkten sind heute deutlich komplexere Abhängigkeiten gegeben. In diesen gibt es

- Hersteller von Softwarebibliotheken,
- Hersteller, die eine oder meist mehrere Softwarebibliotheken nutzen,
- Hersteller, die mehrere Anwendungen zu einem Produkt kombinieren und verkaufen, und
- Anwender, die eine Vielzahl unterschiedlicher Produkte betreiben.

Je weiter vorne in der Kette eine Schwachstelle auftritt, desto mehr Beteiligte müssen aktiv werden. Die jeweiligen Updates müssen, sofern die betroffenen Funktionen verwendet werden, eingepflegt, getestet und installiert werden. Alle Beteiligten müssen von der Schwachstelle erfahren, die Auswirkungen analysieren und entsprechend reagieren. Das größte Problem besteht dabei für den Betreiber eines Produktes am Ende der Lieferkette. Mindestens ab dem Zeitpunkt der Veröffentlichung von Informationen zur Schwachstelle steigt signifikant das

Die Suche und Analyse von neuen Advisories erfordert viel Zeit und Aufwand. Dies resultiert aus der Tatsache, dass die Advisories auf unterschiedlichsten Kanälen publiziert werden – von Twitter und RSS-Feeds über Mailinglisten bis hin zu öffentlichen Webseiten und geschlossenen Kundenportalen. Zusätzlich werden die Advisories noch in unterschiedlichsten Formaten bereitgestellt. Hier reicht das Spektrum von einfachem Text über HTML-Seiten bis zu PDF-Dokumenten. Auch die Sprache und Struktur der Dokumente unterscheidet sich von Hersteller zu Hersteller.

Diese Unterschiede in Verteilung, Format und Struktur machen eine automatisierte Auswertung fast unmöglich. Eine manuelle Bearbeitung bindet jedoch wertvolle Ressourcen, die eigentlich für andere Aufgaben gebraucht werden. Zudem stellt sich die Herausforderung, dass die Anzahl der Quellen mit der Anzahl an Zulieferern steigt. Dies führt dazu, dass die Advisories nicht oder nur mit Verzögerung ausgewertet werden. Beides verlängert jedoch die Phase, in der die Schwachstelle erfolgreich ausgenutzt werden kann.

#### Die Anzahl der Zwischenschritte ist fast beliebig erweiterbar.



Risiko, dass Angreifer diese ausnutzen. Je länger das Bearbeiten in der gesamten Lieferkette dauert, umso länger und größer wird das Risiko für den Betreiber. Daher gilt es, diesen Zeitraum möglichst klein zu halten, um Angriffe schnell zu verhindern.

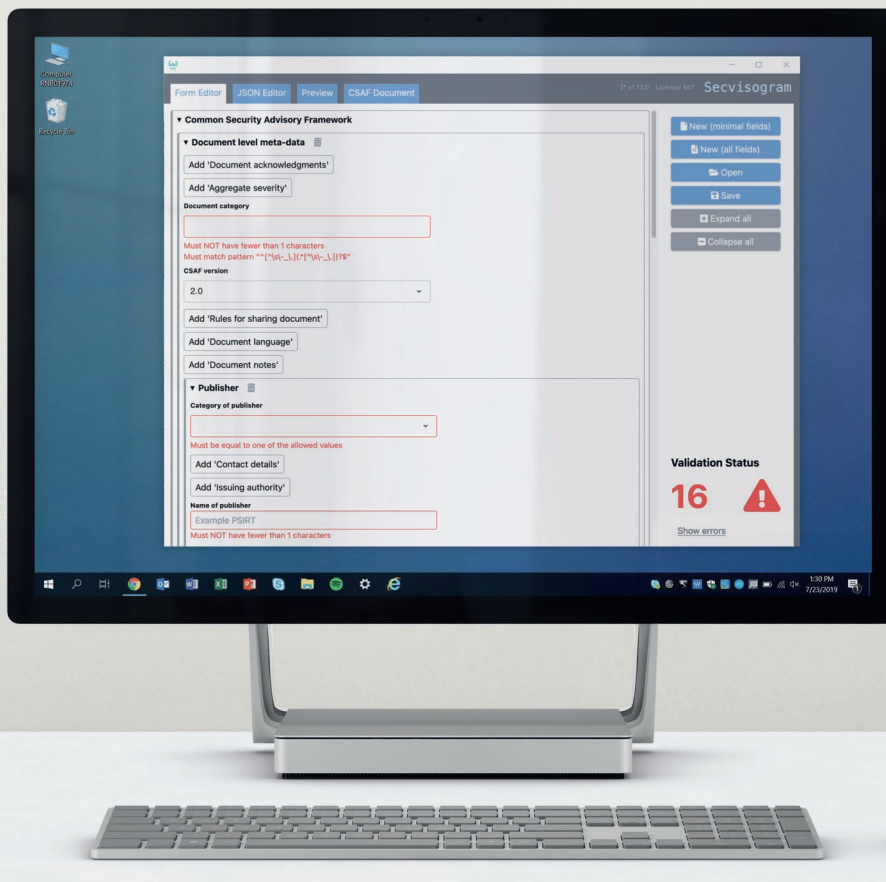
#### Verteilung und Bezug von Security Advisories

Ein wichtiger Aspekt dabei sind die bereits angesprochenen Security Advisories. Diese dienen der Information über eine Schwachstelle in einem konkreten Produkt und der betroffenen Version und geben Hinweise zur Mitigation. Momentan stellt dies jedoch eine Herausforderung für Hersteller und Anwender dar. Heim-anwenderinnen und -anwender, die vor allem Systeme mit automatischen Updates einsetzen, stehen nicht vor dieser Herausforderung. Anwender und Hersteller müssen jedoch die Auswirkungen der Änderungen analysieren.

Deshalb wurde international unter dem Dach der OASIS Open Foundation der offene Standard Common Security Advisory Framework (CSAF) entwickelt, an dem sich auch das BSI beteiligt hat. Es handelt sich um ein Framework, das neben dem JSON-basierten Format für Security Advisories auch deren Verteilung spezifiziert. Darüber hinaus werden weitere Anwendungsfälle über Profile spezifiziert. Umfangreiche formale Tests sorgen für ein angemessenes Maß an Qualität der CSAF-Dokumente.

#### Hersteller und Anwender – zwei Seiten einer Medaille

Der Standard hilft damit beiden Seiten – Anwendern und Herstellern. Letztere werden durch das Format bei der Erstellung von Security Advisories unterstützt. Es wird einfacher für Hersteller, entsprechende Informationen zusammenzustellen und für die Anwender bereitzustellen. Anwender haben den Vorteil, dass ein standardisierter



Mit Secvisogram stellt das BSI ein Werkzeug bereit, um maschinenverarbeitbare Security Advisories einfach und standardisiert zu erstellen. Die Ausgabe als menschenlesbares Dokument ist ebenfalls möglich

Kanal für den Zugriff auf die Security Advisories zur Verfügung steht.

Der größte Gewinn liegt jedoch in der maschinellen Verarbeitbarkeit. Um diesen Vorteil vollständig auszuspielen zu können, müssen Anwender wissen, welche Produkte sie einsetzen. Bei einem Betreiber einer industriellen Anlage wird diese Übersicht auch als Assetliste bezeichnet. Dies ist letztlich eine Inventarliste, in der das eingesetzte Produkt, dessen Hersteller, die Versionsnummer der Firm- oder Software und weitere wichtige Informationen festgehalten werden.

Auch Hersteller können ihrerseits von den CSAF-Meldungen profitieren. Der Hersteller führt eine Software Bill of Materials (SBOM). Dies ist eine Art digitaler Beipackzettel, in dem alle in einem Produkt eingesetzten Softwarebibliotheken mit Hersteller, Name und Version aufgelistet werden. Er beschreibt die Produkte und deren Bestandteile. Eine SBOM ist damit vergleichbar mit einer Assetliste für ein Produkt.

#### Weitere Informationen:



BSI-Veröffentlichung Lebenszyklus einer Schwachstelle:  
[https://www.allianz-fuer-cybersicherheit.de/Shared-Docs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS\\_027.html](https://www.allianz-fuer-cybersicherheit.de/Shared-Docs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_027.html)



Webseite des CSAF Technical Committee:  
[https://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=csaf](https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf)



CSAF-2.0-Spezifikation:  
<https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html>

Die SBOM und die Assetlisten liefern damit die Grundlage für einen Abgleich zwischen Security Advisories und vorhandenen Produkten, Anwendungen oder Software.

Wichtig ist dabei, dass ein Hersteller für seine eigenen Produkte – und vor allem für die veröffentlichten Versionen seiner eigenen Produkte – die entsprechende SBOM vorhält. Vielfach liegt diese für bestehende Produkte noch nicht vor. Bei neuen sollte sie bei der Entwicklung mit erzeugt und für kritische Komponenten nachträglich erstellt werden. Denn nur so kann der Hersteller bei neuen Schwachstellen nachvollziehen, welche Versionen seiner Produkte betroffen sind.

Darüber hinaus ermöglicht CSAF es, über den oben beschriebenen standardisierten Kanal auch Informationen zu verteilen, wenn ein Produkt von einer bestimmten Schwachstelle nicht betroffen ist. Dieses als Vulnerability Exploitability eXchange (VEX) bezeichnete Profil in CSAF unterstützt beispielsweise dabei, falsch positive Ergebnisse von Security-Scannern zu korrigieren oder bei einer Schwachstelle wie Log4Shell die Ergebnisse der Analysen bzgl. Nichtverwundbarkeit schneller mit Kunden zu teilen, anstatt dies über eine Support-Hotline oder E-Mails tun zu müssen.

Der Standard definiert zudem auch Anforderungen an und Funktionen für zugehörige Werkzeuge. Dadurch wird die Erstellung von Tools erleichtert.

#### Toolverfügbarkeit

Das BSI beteiligt sich nicht nur an der Fortentwicklung des Standards, sondern hat bereits das Open-Source-Projekt „Secvisogram“ auf GitHub veröffentlicht. Dies ermöglicht die Erstellung von Advisories über eine grafische Schnittstelle und wird bereits von einigen Herstellern eingesetzt. Durch die Veröffentlichung möchte das BSI Feedback zu Erfahrungen beim Einsatz sammeln und auch die Mitarbeit an der Entwicklung anregen. In einem Folgeprojekt, welches in diesem Frühjahr gestartet ist, wird

die Benutzerfreundlichkeit signifikant erhöht, indem ein Assistent zum Erstellen von Security Advisories angeboten wird. Darüber hinaus wird ein Backend entwickelt, das die Funktionalität eines CSAF-Content-Management-Systems bereitstellt und damit die Verwaltung und Aktualisierung der Security Advisories erheblich erleichtern soll.

Weitere Tools, wie beispielsweise ein Static-Site-Generator zur standardkonformen, automatisiert abrufbaren Bereitstellung von CSAF-Dokumenten und ein Konformitätstool, werden entwickelt. Auch ein Konverter von der Vorgängerversion CVRF CSAF 1.2 ins aktuelle Format ist in Arbeit.

#### Fazit

CSAF alleine löst das Problem der Behandlung von Schwachstellen nicht. Es stellt jedoch einen wichtigen Baustein dar, um aufgedeckte Schwachstellen zeitnah beheben zu können. Angesprochen wurde die Assetliste, also eine Liste mit allen eingesetzten Produkten sowie den zugehörigen Versionen von Hard- und Software. Im Bereich der klassischen IT sind die Varianten bei der eingesetzten Hardware ggf. noch sehr überschaubar. Gleiches gilt für die verwendete Software. Im Bereich der industriellen Steuerungssysteme, die in Produktions- und Automatisierungsanlagen sowie Kritischen Infrastruktur eingesetzt werden, ist dies aufgrund der Vielzahl unterschiedlicher Komponenten, Sensoren, Aktoren, Steuerungen und Bedienstationen deutlich aufwändiger. Die Automatisierung und Vereinheitlichung ist aufgrund dessen auch in diesem Bereich dringend notwendig. Daher empfiehlt das BSI, entsprechende Anforderungen für eine neue Beschaffung aufzunehmen und zu berücksichtigen. ■



Secvisogram – GitHub Repository:  
<https://github.com/secvisogram/secvisogram>



CSAF-2.0-Spezifikation – CSAF content management system: <https://docs.oasis-open.org/csaf/csaf/v2.0/csaf-v2.0.html#916-conformance-clause-6-csaf-content-management-system>



Tools zur Verteilung von CSAF-Dokumenten:  
[https://github.com/csaf-poc/csaf\\_distribution](https://github.com/csaf-poc/csaf_distribution)



CVRF-CSAF-Converter:  
<https://github.com/csaf-tools/CVRF-CSAF-Converter>



Secvisogram – Onlineversion:  
<https://secvisogram.github.io/>



BSI-Seite zu CSAF:  
<https://bsi.bund.de/CSAF>

# Cyber-Sicherheit in der Lieferkette der Automobilindustrie

Wie die Branche mit TISAX einen eigenen Standard für die Informationssicherheit gesetzt hat

von Andreas Ebert, Leiter Know-how- und Prototypenschutz bei der Volkswagen AG

Was geheim ist, muss geheim bleiben. Diesen Satz kennt jeder Mitarbeitende im Volkswagen-Konzern, wenn es um den Schutz von Unternehmensgeheimnissen und Prototypen geht. Gerade in der Entwicklung von neuen Fahrzeugen und bei innovativen Produkten spielt im Konzern die Geheimhaltung eine große Rolle. Aus diesem Grund schließt die Volkswagen AG mit ihren Partnern nicht nur Geheimhaltungsvereinbarungen ab, sondern trifft selbst Maßnahmen in ihrer IT-Infrastruktur zur Informationssicherheit. Gleichzeitig verlangt der Konzern von seinen Partnern ebenfalls die Implementierung solcher Maßnahmen.

Im Jahr 2016 hat sich die Volkswagen AG dafür entschieden, den VDA-ISA-Anforderungskatalog zur Informationssicherheit als Standard anzuwenden. Seitdem ist für alle Partner die Erfüllung des VDA-ISA die Grundlage der Zusammenarbeit. Partner des Konzerns müssen die Erfüllung des VDA-ISA durch eine TISAX-Prüfung nachweisen. Nur dann dürfen sie in den Projekten mit als vertraulich oder als geheim eingestuftes Projektinformationen umgehen. Damit wird ein einheitlich starkes Sicherheitsniveau über die Supply-Chain erreicht.

Wenngleich kein Standard und kein Nachweisverfahren der Welt verhindern kann, Opfer von Cyber-Angriffen zu werden, so lassen sich die Risiken doch erheblich senken. Die Statistiken innerhalb der Volkswagen AG zeigen, dass die Wahrscheinlichkeit eines erfolgreichen Cyber-Angriffes auf Unternehmen, die über Zertifizierungen nach TISAX verfügen, geringer ist und die Folgen sowie Auswirkungen von Cyber-Angriffen sich besser beherrschen lassen.



*Andreas Ebert leitet im Volkswagen-Konzern den Know-how- und Prototypenschutz.*

*Daneben ist er Auditor für Qualitätsmanagement, IT-Sicherheit sowie für Softwareentwicklungsprozesse, Leiter des Arbeitskreises Informationssicherheit und Wirtschaftsschutz im VDA, Mitglied des BDI-Vorstandes im Ausschuss für Sicherheit sowie des AK Cybersicherheit und Wirtschaftsschutz.*



## Hintergrund TISAX

von Lennart Oly, Geschäftsführer ENX Association

Die Automobilindustrie hat früh begonnen, einen risiko-basierten und prozessorientierten Ansatz für die Informationssicherheit in der Supply-Chain zu implementieren. Mit dem TISAX-Modell (Trusted Information Security Assessment Exchange) verfügt die Automobilindustrie über einen eigenen Standard für die Prüfung der Informationssicherheit.

Verschiedene „TISAX-Prüfziele“ und damit verbundene „TISAX-Labels“ gehen auf spezifische Risikoprofile unterschiedlicher Unternehmenstypen im automobilen Wertschöpfungsnetzwerk ein. Sie machen die Erfüllung entsprechender Anforderungen transparent. So sind etwa zusätzliche Maßnahmen nachzuweisen, wenn ein Partner mit Kundeninformationen mit sehr hohem Schutzbedarf oder mit Prototypen umgeht.

Die Steuerung, Kontrolle, Qualitätssicherung und Entwicklung von TISAX erfolgen durch die ENX Association als unabhängige Organisation der Automobilindustrie.

Der Prüfkatalog (ISA) und das Prüfmodell (TISAX) werden auf diese Weise von Automobilherstellern und Zulieferern gemeinsam entwickelt. Das soll eine breite Akzeptanz sicherstellen.

TISAX zählt derzeit mehr als 6.000 geprüfte Standorte in über 60 Ländern. Jährlich kommen derzeit ca. 1.000 geprüfte Standorte hinzu. Über 90 Prozent der einmal geprüften Unternehmen unterziehen sich nach Ablauf der dreijährigen Laufzeit erneut dem Prüfverfahren.

Seit dem Start wurden mehr als 25.000 Verbesserungen der Informations- und Cyber-Sicherheit festgehalten.

Alle Organisationen, die direkt oder indirekt mit der Automobilindustrie zusammenarbeiten, können Teil der „Trusted Community“ werden. Die Nutzung von TISAX steht darüber hinaus grundsätzlich allen Branchen offen.



*Lennart Oly ist im Vorstand des Kompetenznetzwerks Trusted Cloud e.V. unter Schirmherrschaft des Bundesministeriums für Wirtschaft und Klima.*

*Als Unternehmer und Geschäftsführer befasst er sich mit der vertrauenswürdigen Digitalisierung automobiler Wertschöpfung und ist seit fast 20 Jahren in der Verantwortung für die Geschäftsführung der ENX Association.*



Der Volkswagen-Konzern plant gerade die deutliche Ausweitung der Anwendung des VDA-ISA/TISAX. Dieses vor dem Hintergrund der deutlich wachsenden Gefahren durch Cyber-Angriffe, der wachsenden Abhängigkeiten in der Supply-Chain sowie der Anforderungen aus dem IT-Sicherheitsgesetz 2.0.

Daher laufen derzeit die Vorbereitungen durch den Konzerneinkauf und die Konzernsicherheit, TISAX mit dem Schutzziel Verfügbarkeit zukünftig auch von Lieferanten von Serienteilen zu verlangen. Die Lieferanten sind bereits in einer Vorabinformation über die geplanten Veränderungen im Zusammenhang mit TISAX informiert worden.

In der „TISAX-Community“ wird derzeit das TISAX-Modell um die entsprechend notwendigen Anpassungen ergänzt (TISAX-Level, Relevant Controls usw.) sowie um die formale Anpassung der TISAX-Dokumentation. ■

# Moderne Messenger – heute verschlüsselt, morgen interoperabel?

Zum Hintergrundpapier über die Funktionsweise moderner Messenger und zur Zusammenarbeit mit dem Bundeskartellamt

von Dr. Friederike Laus, Referat Prüfung von Kryptoverfahren, Jan Metzke, Referat Produkte und Systeme für Verschlusssachen (VS-IT), Dr. Stephan Arlt, Referat Sicherheit in Internetinfrastrukturen und -diensten, und Dr. Matthias Korn, Referat Grundsatzfragen des Digitalen Verbraucherschutzes und Kooperationen

Messenger sind aus dem digitalen Alltag vieler Verbraucherinnen und Verbraucher nicht mehr wegzudenken – ob mit Familie, Freundinnen und Freunden, im Bekanntenkreis, in der Nachbarschaft oder im Beruf. Viele verwenden einen oder gar mehrere der vielen am Markt verfügbaren Messenger. Sei es zum Chatten, um Bilder zu teilen, für Sprach- und Videonachrichten oder -anrufe oder andere Zwecke. Aus diesem Anlass hat das BSI im Kontext einer Zusammenarbeit mit dem Bundeskartellamt die grundlegenden Funktionsweisen und zentralen Sicherheitseigenschaften moderner Messenger in einer BSI-Publikation erläutert.

## Messenger in aller Munde

Die Digitalisierung sollte den Menschen in erster Linie nutzen. Dafür muss sie nicht nur anwendungsfreundlich, sondern insbesondere auch sicher sein. Aus diesem Grund setzt sich das BSI für die Entwicklung von sicheren und zeitgemäßen Verbraucherprodukten und -diensten ein.

Messenger sind zu einem Standardwerkzeug für die moderne Kommunikation geworden und werden zum Austausch persönlicher und vertraulicher Informationen genutzt. Deshalb ist es wichtig, dass sich Nutzerinnen und Nutzer stets auf die Sicherheit dieser Dienste verlassen können.



### Erste Ergebnisse der Zusammenarbeit von BSI und Bundeskartellamt

Das BSI hat unter dem Titel „Moderne Messenger – heute verschlüsselt, morgen interoperabel?“ ein technisches Hintergrundpapier zu Messengern erstellt. Das Papier zeigt die ersten Ergebnisse der Zusammenarbeit im Bereich des Digitalen Verbraucherschutzes mit dem Bundeskartellamt auf. Gemeinsam wollen beide Behörden dafür sorgen, dass die Digitalisierung in erster Linie Vorteile für Verbraucherinnen und Verbraucher mit sich bringt.

Aus Verbraucherschutzperspektive wirkt sich eine wachsende Marktkonzentration auf wenige große Messenger-Anbieter potenziell negativ auf Interessen der Anwenderinnen und Anwender aus, beispielsweise, wenn sich die Nutzung eines bestimmten Messengers de facto nicht vermeiden lässt. Auf EU-Ebene werden daher Messenger besonders großer Anbieter (sogenannter *Torwächter*) im Gesetz über digitale Märkte (DMA) adressiert. Europäischer Rat und Europäisches Parlament haben sich im März 2022 darauf geeinigt, solchen Torwächtern eine Verpflichtung zur Interoperabilität ihrer Messenger mit denen anderer Anbieter aufzuerlegen.

### Viele moderne Messenger bieten Ende-zu-Ende-Verschlüsselung

Zunächst stellt sich jedoch die Frage, wie verschiedene Messenger-Anbieter mit der Vertraulichkeit der Kommunikationsinhalte umgehen. Die meisten Messenger versenden Nachrichten heutzutage verschlüsselt; bei immer mehr Anbietern ist der verschlüsselte Nachrichtenversand inzwischen sogar die standardmäßige Voreinstellung, ohne dass Nutzerinnen und Nutzer sich damit auseinandersetzen müssen. Bei der angebotenen Art der Verschlüsselung gibt es jedoch große Unterschiede: Wie werden Inhalte verschlüsselt – mittels einer Ende-zu-Ende- oder lediglich einer Transportverschlüsselung? Welche Inhalte werden verschlüsselt – nur Textnachrichten oder auch Sprachnachrichten, Bilder und Dateien, Audio- oder Videotelefonate? Werden nur Einzel- oder auch Gruppenkonversationen verschlüsselt?

Das Double-Ratchet-Protokoll gilt aktuell als Stand der Technik im Bereich der Ende-zu-Ende-Verschlüsselung für Messenger. Unter einer Ende-zu-Ende-Verschlüsselung versteht man an dieser Stelle, dass die Kommunikationsinhalte vom Nachrichtensender über den Übertragungsweg hinweg bis hin zum Nachrichtempfänger verschlüsselt und damit für Dritte (inklusive des Messenger-Anbieters) nicht einsehbar sind. Das ursprünglich für einen Vorläufer des Messengers Signal entwickelte Protokoll kommt in mehreren populären Messengern zum Einsatz – jedoch in teils abgewandelter Form, da es nicht standardisiert ist.

### Ausblick: Interoperabilität zwischen Messengern?

Ein Nachteil in Sachen Nutzungsfreundlichkeit stellt die Tatsache dar, dass Nutzerinnen und Nutzer eines Messenger-Anbieters – anders als beispielsweise bei Telefon

und E-Mail – in der Regel nicht mit denen eines anderen Anbieters kommunizieren können. Mit anderen Worten: Die meisten Messenger sind untereinander nicht interoperabel.

Bei der Umsetzung der Interoperabilität zwischen unterschiedlichen Messengern sind aus regulatorischer, aber auch aus technischer Sicht noch einige Herausforderungen zu bewältigen, darunter insbesondere das Zusammenspiel der unterschiedlichen Kommunikationsprotokolle. Noch in diesem Jahr will die zuständige Arbeitsgruppe der Internet Engineering Task Force (IETF) den Standard Messaging Layer Security (MLS) verabschieden. Dieser Standard stellt eine technische Grundlage dar, auf deren Basis sich zukünftig eine sichere Ende-zu-Ende-Verschlüsselung von Nachrichten in größeren Gruppen und über Anbietergrenzen hinweg realisieren lässt. Vorbehaltlich der weiteren Entwicklungen rund um den MLS-Standard stellt daher zumindest die Ende-zu-Ende-Verschlüsselung künftig kein Hindernis mehr für eine Interoperabilität dar.

Jedoch ist mit MLS lediglich die Verschlüsselung der Nachrichteninhalte abgedeckt. Für eine praktische Interoperabilität sind weitere technische Funktionalitäten notwendig. Dies betrifft vor allem einen geeigneten Kanal zur Übertragung der verschlüsselten Nachrichten sowie Funktionen zum Auffinden, Identifizieren und Vermitteln von bzw. zwischen Nutzerinnen und Nutzern. Die Umsetzung dieser und weiterer Funktionalitäten ist noch nicht gänzlich absehbar, wird jedoch einen nicht unerheblichen Einfluss auf die sichere Gestaltung der Interoperabilität haben.

Zusammenfassend lässt sich festhalten, dass sich Interoperabilität und Ende-zu-Ende-Verschlüsselung, also erweiterte Nutzungsmöglichkeiten bei gleichzeitig hoher Sicherheit, nicht ausschließen. Das Thema bleibt also spannend, und die nächsten Monate werden zeigen, wie es in puncto Interoperabilität zwischen Messengern weitergeht. ■

#### Weitere Informationen:



Hintergrundpapier „Moderne Messenger – heute verschlüsselt, morgen interoperabel?“  
<https://www.bsi.bund.de/dok/messenger-211103>



Bundeskartellamt: Zwischenbericht zur Sektoruntersuchung Messenger- und Video-Dienste  
[https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung\\_MessengerVideoDienste\\_Zwischenbericht.html](https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_MessengerVideoDienste_Zwischenbericht.html)



Bundesnetzagentur: Diskussionspapier zur Interoperabilität zwischen Messengerdiensten  
<https://www.bnetza.de/online-kommunikation.html>

BSI Basis-Tipp

# Sichere Onlineshops erkennen

Was beim Einkaufen im Internet zu beachten ist

Onlineshopping ist für immer mehr Menschen eine bequeme Alternative zum stationären Handel. Mit nur wenigen Klicks lassen sich Produkte bestellen und bequem nach Hause liefern. Doch was sollten Verbraucherinnen und Verbraucher – im besten Fall schon vor dem Onlineeinkauf – tun, um sich vor finanziellen Verlusten und einer Menge Ärger zu schützen?

Das Onlineshopping immer beliebter wird und Onlinehändler sowie Auktionshäuser in den vergangenen Jahren die Einkaufsgewohnheiten vieler Menschen verändert haben, ist nicht verwunderlich. Die lästige Parkplatzsuche, begrenzte Öffnungszeiten und das Schleppen von schweren Einkaufstüten gehören beim Einkauf im Internet der Vergangenheit an.

Doch beim Onlineshopping lauern mitunter Gefahren. Neben klassischen Betrugsfällen – die Ware oder Dienstleistung wird trotz Bezahlung nicht geliefert – kommt es in vielen Fällen auch zum Abgreifen und zum Missbrauch von Kreditkarten- oder Kontodaten. Das geschieht durch schlecht gesicherte Onlineaccounts oder gefälschte Webseiten sowie durch schädliche Links und Dateianhänge, die in scheinbar seriösen E-Mails lauern.





### Fakeshops sind das größte Problem beim Onlineshopping

Immer wieder tauchen im Internet sogenannte Fake-shops auf, die aussehen wie echte Shops, hinter denen sich aber Kriminelle verbergen. Überraschend günstige oder eigentlich ausverkaufte sowie äußerst beliebte Produkte sind dabei gerne eingesetzte Lockmittel.

Trotz Zahlung – meist per Vorkasse – wird anschließend aber keine, beschädigte oder falsche Ware geliefert. Laut Digitalbarometer 2021 hat jedes zweite Opfer von Betrug beim Onlineshopping ein Produkt bezahlt, aber nicht erhalten. Das BSI empfiehlt deshalb, möglichst die Zahlungsoptionen „Auf Rechnung“ oder „Lastschrift“ auszuwählen und sich neben den angebotenen Zahlungsmethoden vor dem Kauf über den Onlineshop zu informieren: Sind die AGB einsehbar, gibt es eine seriöse Anbieterkennzeichnung, Datenschutzvereinbarungen und ein seriöses Impressum?

Optisch sind Fakeshops meist gar nicht so einfach von „echten“ Shops zu unterscheiden. Um keine böse Überraschung zu erleben, gibt es jedoch ein paar Kriterien, anhand derer ein sicherer Onlineshop zu erkennen ist. Aber Achtung: Nur eines der aufgeführten Merkmale reicht dafür noch nicht. Im besten Fall finden Sie auf der Website alle sieben Merkmale für einen sicheren Onlineshop.

### Was im Ernstfall zu tun ist

Trotz aller Vorsicht und Sicherheitsmaßnahmen kann es passieren, dass jemand in eine Betrugsfalle tappt.

Die SOS-Karte zum Onlineshopping hilft Betroffenen und zeigt weitere Schutzmaßnahmen gegen Kriminalität beim Onlineshopping. Sie kann unter der Adresse [bsi.bund.de/dok/954484](https://www.bsi.bund.de/dok/954484) kostenlos heruntergeladen werden.

### #einfachaBSIchern

Was Sie beim Einkauf im Geschäft niemals tun würden, ist auch beim Onlineshopping keine gute Idee. Ein kurzweiliger Denkanstoß dazu ist auf der Website [einfachabsichern.de](https://www.einfachabsichern.de) in Form von humorvollen Spots zu finden. ■

#### Weitere Informationen:



Die SOS-Karte – Schutz beim Onlineshopping:  
<https://www.bsi.bund.de/dok/954484>



<https://www.einfachabsichern.de>



Die Initiative D21 hat Qualitätskriterien für Onlinehändler definiert. Siegel, die diese Kriterien erfüllen, finden Sie unter:  
<https://www.initiatived21.de/arbeitsgruppen/guetesiegelboard>

# Sicher online shoppen – sieben Merkmale für einen sicheren Onlineshop

- 1. Eindeutiger Bestellbutton**

Der Bestellbutton ist mit „Zahlungspflichtig bestellen“ oder mit einer anderen eindeutigen Formulierung wie „Jetzt kaufen“ beschriftet und nicht etwa mit unklaren Begriffen wie „Anmelden“ oder „Abschließen“.
- 2. Vorhängeschloss in der Browserzeile**

Ein Vorhängeschloss sowie das „https://“ in der Adresszeile des Browsers stehen für eine sichere Verbindung. Zudem gibt es in der Adresse keine auffälligen Domain-Endungen wie „de.com“.
- 3. Vorhandene Kontaktmöglichkeiten**

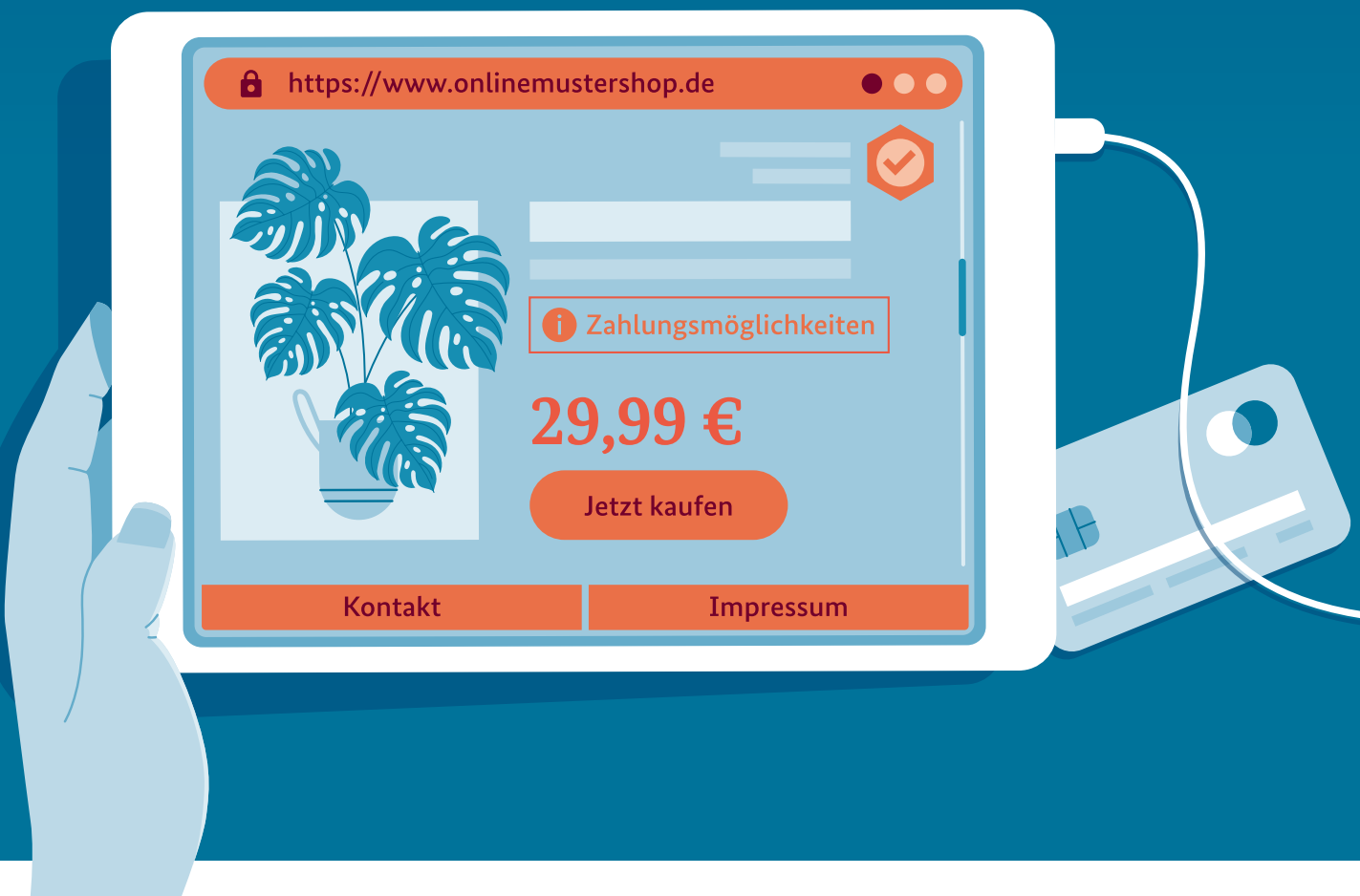
Telefonnummer und E-Mail-Adresse für die Kontaktaufnahme sind vorhanden und leicht auffindbar. Bei kostenpflichtigen (ausländischen) Telefonnummern, einem Postfach oder der Beschränkung auf ein Kontaktformular ist dagegen Skepsis geboten. Ein Anruf beim Anbieter oder Rezensionen des Shops auf anderen Portalen können als Kontrolle dienen.
- 4. Vollständiges Impressum**

Angaben zu Unternehmensname, Rechtsform, Namen der Vertretungsberechtigten, vollständige Anschrift und Kontaktmöglichkeiten sind enthalten.
- 5. Realistische und transparente Preise**

Der Preis des Produktes ist realistisch und mögliche Zusatzkosten sind transparent aufgeführt.
- 6. Gütesiegel**

Der Shop nutzt ein bekanntes Gütesiegel. Das Siegel enthält zudem eine Verlinkung zu weiteren Informationen zu Shop und Bestellprozess.
- 7. Mehrere Zahlungsmöglichkeiten**

Es gibt mehrere Zahlungsmöglichkeiten – beispielsweise Kauf auf Rechnung, per Kreditkarte oder über einen seriösen Online-Bezahldienst.



# Bestellen Sie Ihr BSI-Magazin!



Bundesamt  
für Sicherheit in der  
Informationstechnik

Bundesamt für Sicherheit in der  
Informationstechnik (BSI)  
Referat Öffentlichkeitsarbeit

Postfach 20 03 63  
53133 Bonn  
Telefon: +49 (0) 228 99 9582 0  
Telefax: 0228 99 9582-5455  
E-Mail: [bsi-magazin@bsi.bund.de](mailto: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 im Juni und im Dezember 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“ (2x im Jahr, Print)
- Die Lage der IT-Sicherheit in Deutschland (1x im Jahr, Print)

.....  
Name, Vorname

.....  
Organisation

.....  
Straße, Hausnr.

.....  
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 20 03 63, 53133 Bonn. Die von Ihnen angegebenen Daten werden ausschließlich für die Verwaltung des Versands bzw. die Übermittlung der Informationen verwendet, denen Sie oben zugestimmt haben. Sie können diese Einwilligung jederzeit widerrufen. Hierzu genügt eine E-Mail an [bsi-magazin@bsi.bund.de](mailto: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 beigegefügteten „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](mailto: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](mailto:bsi-magazin@bsi.bund.de).

## Datenschutzrechtliche Hinweise:

[https://www.bsi.bund.de/DE/Service/Datenschutz/datenschutz\\_node.html](https://www.bsi.bund.de/DE/Service/Datenschutz/datenschutz_node.html)

# 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:	Juni 2022
Texte und Redaktion:	Katrin Alberts, Sonia Golás, 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 Schneckelohe www.ak-druck-medien.de
Artikelnummer:	BSI-Mag22/715-1
Bildnachweise:	Titel: GettyImages © KTSDESIGN/SCIENCE PHOTO LIBRARY; S. 04, S. 08–11: © Hennig Schacht; S. 03, S. 06, S. 07, S. 14, S. 24, S. 25, S. 30–33, S. 35, S. 37, S. 38–39, S. 46, S. 54–55, S. 61, S. 65, S. 68, S. 70–71, S. 76–77: © BSI; S. 04, S. 34: AdobeStock © peopleimages.com, AdobeStock © pickup; S. 10: S. 12–13: AdobeStock © m.mphoto; S. 16: AdobeStock © alice_photo; S. 18–19: AdobeStock © greenbutterfly; S. 20–23: AdobeStock © OneLineStock.com, AdobeStock © riz; S. 23: AdobeStock © tadamichi; S. 26: AdobeStock © Vadim Pastuh; S. 29: AdobeStock © JustLife; S. 28: ZDH; S. 30: Bitkom e.V.; S. 36: AdobeStock © Stafeeva; S. 40: Quelle: privat/Caroline Schreer; S. 42: Mirko de Paoli; S. 43: Christian Klant; S. 44–45: AdobeStock © Cybrain; S. 46: Quelle: BSI/Weiler; S. 46–47: AdobeStock © elenabsi; S. 48: AdobeStock © deepagopi; S. 49: © Secunet und Rhode und Schwarz; S. 50: Secunet; S. 52–53: AdobeStock © metamorworks; S. 56: AdobeStock © olly; S. 58–59: © Fraunhofer HHI; S. 62–63: AdobeStock © tippapatt; S. 64: © MI; S. 70: VW; S. 71: ENX; S. 70–71: AdobeStock © HQUALITY; S. 72: AdobeStock © pickup; S. 74: AdobeStock © Panuwat D; S. 75: AdobeStock © JenkoAtaman

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>



