

**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.



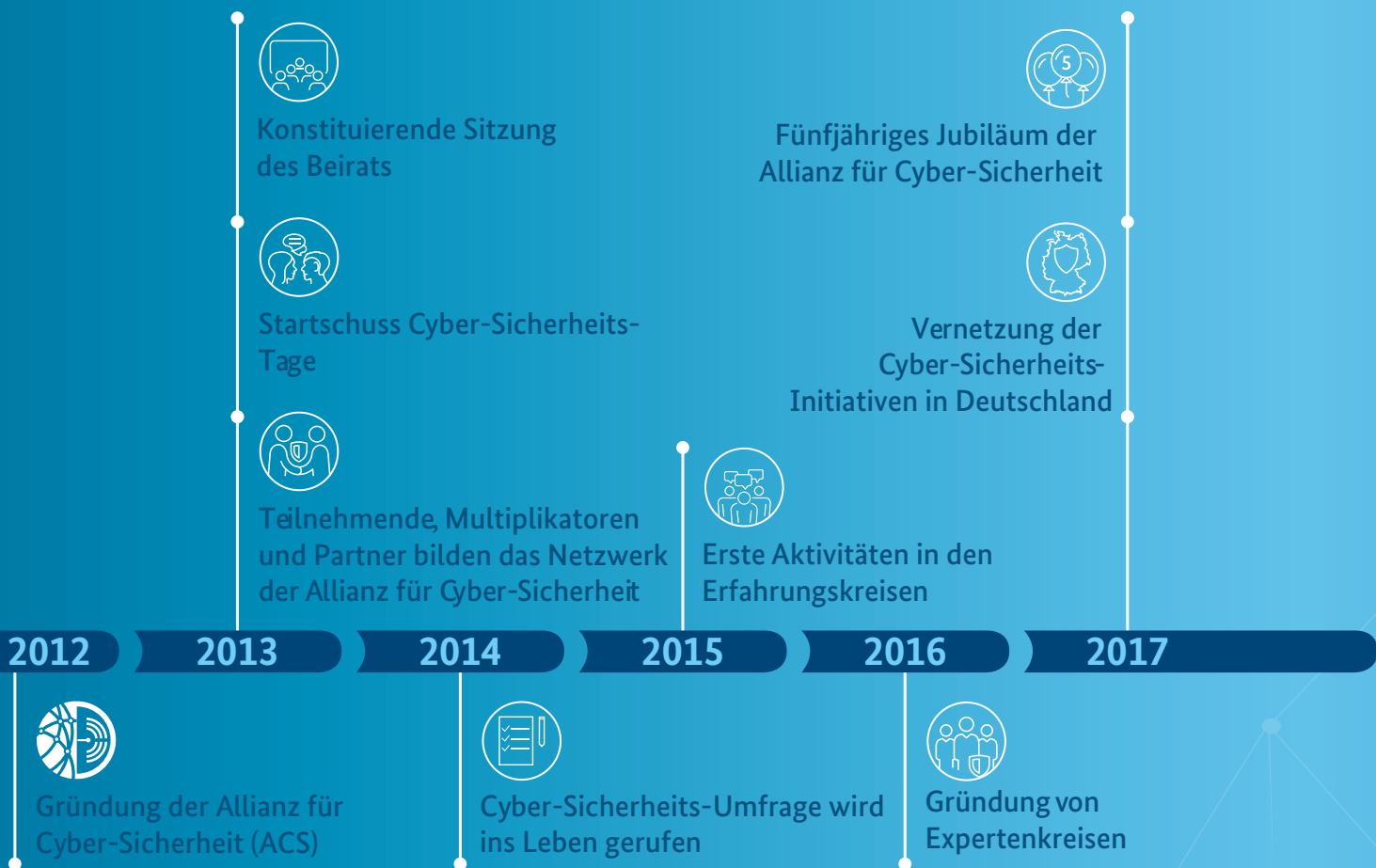
Als Nächstes wurde die Idee der Multiplikatoren entwickelt. Institutionen wie z. B. Verbände, Kammern, Vereine, Initiativen und Netzwerke oder Medienpartner, die sich besonders engagieren möchten, können durch ihren öffentlichkeitswirksamen Einsatz für die ACS die Bedeutung von Cyber-Sicherheitsmaßnahmen 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-



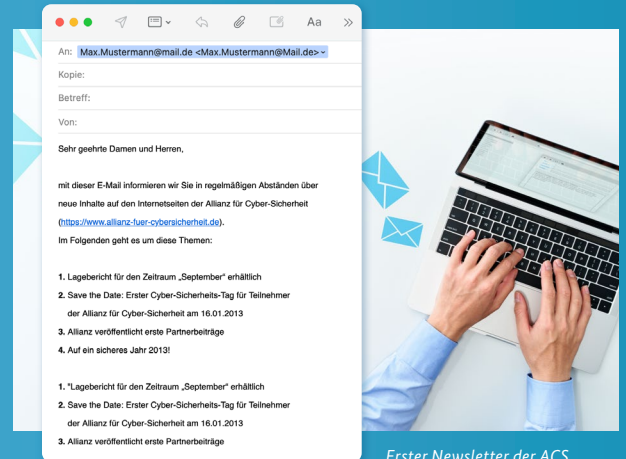
stellungen zur Erhöhung des Cyber-Sicherheitsniveaus bei. Speziell für den Infopool wurde das kompakte Format der Cyber-Sicherheits-Empfehlungen (CS-Empfehlungen) entwickelt.

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?**

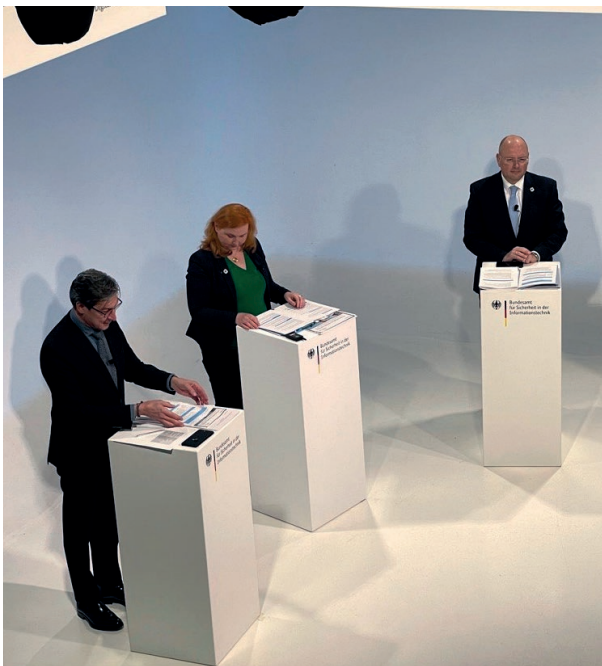
Eine der großen offenen Fragen zu Beginn war: Wie erreichen wir unsere zukünftigen Zielgruppen? Es gibt in Deutschland mehrere Millionen Unternehmen und viele andere Organisationen. Nur ein Prozent dieser Akteure an die ACS zu binden, wäre ein zu ambitioniertes Ziel gewesen. Glücklicherweise waren wir 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

Herzgebirge: 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>

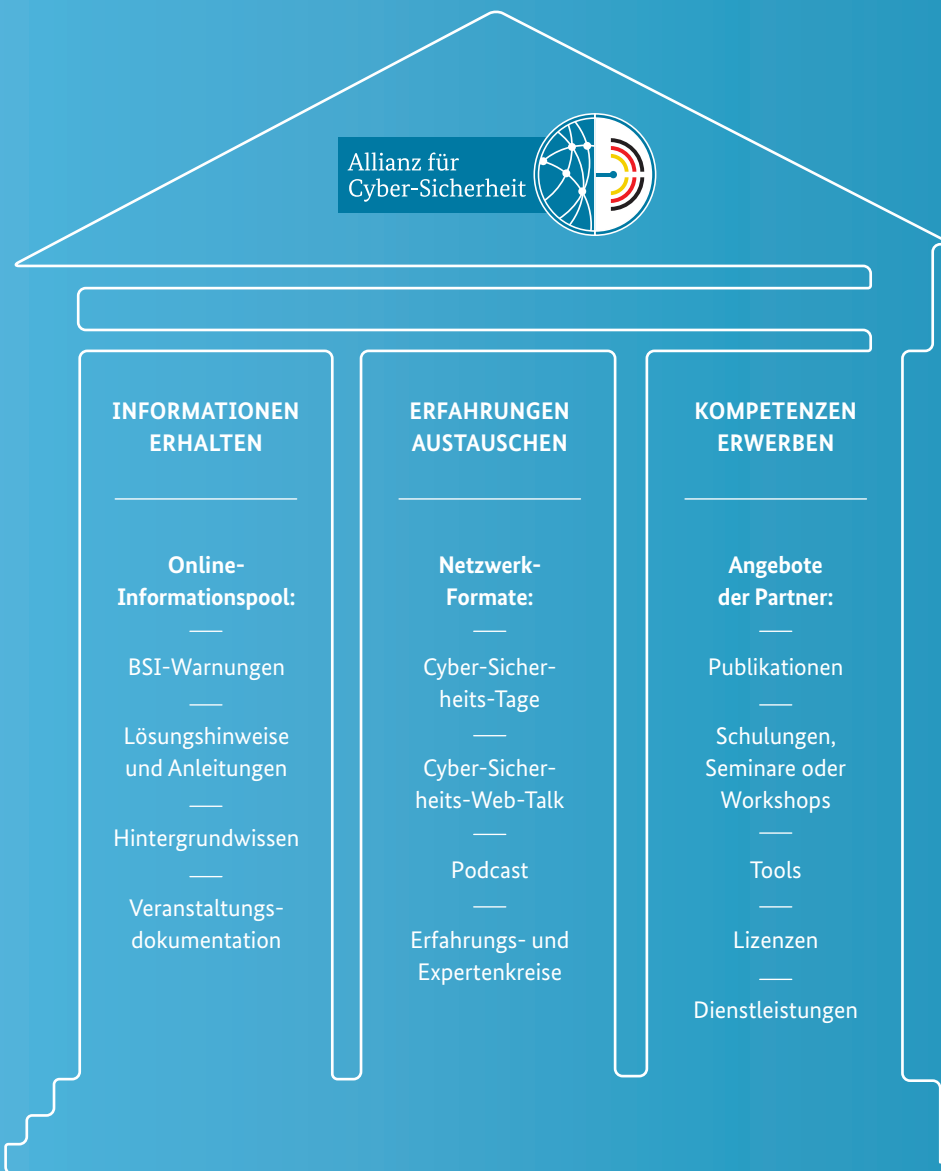
Zum zehnjährigen Jubiläum hat die ACS ihr Leitbild formuliert:

*„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. ■



**Bei dieser Datei handelt es sich um einen Auszug aus dem BSI-Magazin 2022/01, das am 23. Juni 2022 veröffentlicht worden ist. Das ganze BSI-Magazin sowie das vollständige Impressum können Sie hier lesen:**

**[https://www.bsi.bund.de/DE/Service-Navi/Publikationen/BSI-Magazine/bsi-magazine\\_node.html](https://www.bsi.bund.de/DE/Service-Navi/Publikationen/BSI-Magazine/bsi-magazine_node.html)**