Public IT-Security Report

Cyber-Abwehr und -Verteidigung: eine gesamtstaatliche Anstrengung

ISSN 978-3-934401-75-4

Behörden Spiegel-Gruppe

Eine Plattform.
Alle Schutzdimensionen.
Beste Cyberprotection.

Der zuverlässige All-in-One Cyberschutz von Kaspersky deckt verschiedenste Schutzdimensionen ab:

- Verhaltensbasierte und mit KI unterstützte Bedrohungsabwehr
- Weltweit führende Threat Intelligence
- Managed Security Service 24/7
- Trainings für Cybersicherheitsbewusstsein
- Professioneller Service

Eine Gesamtlösung – für besten Cyberschutz

kas.pr/all-in-1

kaspersky **BRING ON THE FUTURE**

Copyright © 2023 AO Kaspersky Lab. All rights reserved.

Inhalt

4 Editorial
Reinhard Wolski

6 Sicherheit für den grenzenlosen Cyber-Raum
Andreas Könen, Bundesministerium des Innern und für Heimat (BMI)

8 Die Cyber-Dimension nationaler Sicherheit
Dr. Regine Grienberger, Auswärtiges Amt

10 Präventive Informationssicherheit
Generalmajor Jürgen Setzer, Bundeswehr

14 Das Nationale Cyber-Abwehrzentrum sichert behördenübergreifenden Informationsfluss
Roland Hartmann, BSI
Oberstleutnant Jan Pangerl, Bundeswehr

16 Die Nationale Sicherheitsstrategie braucht dringend Updates
Dr. Reinhard Brandl, MdB (CDU/CSU)

20 Die starren Strukturen aufbrechen und zusammenarbeiten
Alexander Handschuh, Deutscher Städte- und Gemeindebund

22 Die Nationale Sicherheitsstrategie Deutschlands – zwischen Anspruch und Wirklichkeit
Stephan Ursuleac, Bitkom e.V.

24 Zero Trust: die nächste Generation der Sicherheitsarchitektur
Andreas Ritschel und Hendrik Vagts, BWI GmbH

26 Wie lässt sich Cyber-Sicherheit üben?
Team Presse- und Informationszentrum, Kommando Cyber- und Informationsraum

30 Cyber-Sicherheit geht alle an – ressortübergreifende Zusammenarbeit im Kommando Cyber- und Informationsraum
Oberstleutnant Peter Leffler, Bundeswehr
Oberstleutnant Jan Pangerl, Bundeswehr

Impressum

Dieses Magazin wird von der Behörden Spiegel-Gruppe, ProPress Verlagsgesellschaft mbH Bonn/Berlin, verlegt.
Herausgeberin: Dr. Eva-Charlotte Proll
Redaktion: Reinhard Wolski, Benjamin Hilbricht
Verlagshaus Bonn: Friedrich-Ebert-Allee 57, 53113 Bonn, Telefon: +49 228 970 970
Verlagshaus Berlin: Kaskelstraße 41, 10317 Berlin, Telefon: +49 30 55 74 12 0
E-Mail: verlag@behoerdenspiegel.de
Layout und Herstellung: Spree Service- und Beratungsgesellschaft m.b.H.
Druck: msk marketingservice köln GmbH
Grafik Titelseite: BS/pinkeyes, stock.adobe.com

© 2023 Verlagsgesellschaft Bonn/Berlin

Editorial

Liebe Leserinnen und Leser,

Es. Geht. Nur. Gemeinsam.
Mit dieser neudeutschen Ausdrucksform begrüßen wir Sie in unserem Heft zur Public IT Security Conference 2023 des Behörden Spiegel. Welche Überlegungen hatten wir bei der Konzeption?

Die IT durchzieht das gesamte Leben, die gesamte Verwaltung, die Wirtschaft, die Verteidigung. Cyber-Sicherheit, Cyber-Abwehr und Cyber-Verteidigung müssen also aus vielen Blickwinkeln gedacht werden. Diesen Ansatz verfolgt der Behörden Spiegel mit seinem Kongress PITS und diesen Ansatz verfolgt die hier vorliegende Broschüre.

In der durch die Bundesregierung erlassenen Nationalen Sicherheitsstrategie steht: „Die Bundesregierung versteht Cybersicherheit als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft. Angesichts der Bedeutung des digitalen Raums ist Cybersicherheit ein essenzieller Teil von integrierter Sicherheit. Wir werden unsere Cybersicherheitsarchitektur weiterentwickeln, gezielt Technologien fördern und die Kooperation mit der Wirtschaft intensivieren. Wir werden zudem unsere Fähigkeiten zur Abwehr von Cyberangriffen stärken und unser Netzwerk der Cyber-Diplomatie ausbauen und nutzen, um die Sicherheit im Cyberraum zu erhöhen."

Auch hier liegt der Schwerpunkt auf „gemeinsam". Die Unterstützung einer deutschen Kommune bei der Wiederherstellung der digitalen Infrastruktur durch das Kommando Cyber- und Informationsraum ist ein sehr lobenswertes und zukunftsweisendes Beispiel für eine solche ressortübergreifende Zusammenarbeit.

International haben sich die Europäische Union und die NATO auf einen Bericht zur „Resilience of Critical Infrastructure" geeinigt. Dort ist zu lesen: „Some of the digital infrastructure used by governments and armed forces is also owned and operated by them. While fully a national competence, it is paramount to increase its resilience, too, in particular military and law enforcement digital infrastructure. Existing legislation and policies applying to the public sector could be relevant for the military domain, and vice versa."

Grafik: BS/pinkeyes, stock.adobe.com

Auch international muss intensiv daran gearbeitet werden, denn die Bedrohung, die Angriffe, insbesondere aus Russland, treffen alle Bereiche. Tagtäglich, tausendfach. Dabei fechten die Angreifer einen ungleichen Kampf aus. Profis, staatliche Hacker, die seit Jahrzehnten nichts anderes machen, als ihre Angriffe weiterzuentwickeln, treffen auf Kommunen, auf Stadtwerke und Krankenhäuser, wo die IT im schlimmsten Falle durch jemanden aus irgendeiner Abteilung mitgemacht wird. Hinzu kommen bei den Verteidigern oftmals Nutzerinnen und Nutzer, deren unbedachter Umgang mit der Technologie erst die Tore für die professionellen Angreifer öffnet.

Der Behörden Spiegel ist daher dankbar, dass wir mit der PITS ein Format liefern können, in dem Kommunen, Länder, Bundesbehörden, die Behörden öffentlicher Sicherheit und Ordnung (BOS), die Streitkräfte und die Industrie gemeinsam ihre Vorstellungen zu der Schaffung eines „Digitalen Immunsystems“ entwickeln, besprechen und darlegen können. Wo gemeinsam an Lösungen gearbeitet wird, die immer auch durch die einfachen Nutzer umsetzbar sein müssen.

Und wir schauen auch über den „Grenzzaun“: Taiwan hat ein Digitalministerium eingerichtet, dessen Ministerin über umfangreiche Befugnisse verfügt – in ihrem Ministerium sind jeweils Abteilungen der anderen wichtigen Ressorts vertreten – ein Modell für Deutschland?

Wir hoffen, dass unser umfassender Ansatz Ihr Interesse findet und wünschen Ihnen viel Freude bei der Lektüre dieses Magazins.

Für die Behörden Spiegel Redaktion

Reinhard Wolski

Ihr Reinhard Wolski

Sicherheit für den grenzenlosen Cyber-Raum

Die Digitalisierung aller Lebensbereiche, deren Bedeutung und Chancen für unsere Gesellschaft außer Frage stehen und die wir weiter voranbringen wollen und müssen, bedarf eines umfassenden Schutzes, da eine Rückkehr in eine „analoge Welt" nicht nur unerwünscht, sondern in den meisten Bereichen auch nicht möglich wäre.

Andreas Könen, Bundesministerium des Innern und für Heimat (BMI)

Die Cyber-Sicherheitslage hat sich im letzten Jahr erneut verschärft. Vorfälle im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine treffen auf eine ohnehin angespannte Bedrohungslage im Cyber-Raum, verursacht insbesondere durch Cyber Crime wie Ransomware und das verstärkte „Big Game Hunting" oder die gezielten Angriffe auf Lieferketten.

Im Zusammenhang mit dem Kriegsgeschehen in der Ukraine ist es auch zu Vorfällen in Deutschland gekommen. Auch wenn es sich hierbei im Wesentlichen um eine Häufung einzelner Vorfälle handelte, die keine groß angelegte und orchestrierte Kampagne gegen Deutschland erkennen ließen, kam es zu Kollateralschäden. So führten russische Cyber-Angriffe auf das Satellitenkommunikationssystem Viasat, mit dem Ziel die Kommunikation in der Ukraine zu stören, zu Problemen bei der technischen Steuerung deutscher Windparks.

Pro-russische Hacktivisten wie „Anonymous Russia" haben sich zu Angriffen auf einige Flughäfen in Deutschland bekannt. Bei diesen sogenannten DDOS-Angriffen wurden Überlastungsangriffe gegen Webseiten durchgeführt, die infolgedessen nicht mehr waren erreichbar oder sicherheitshalber von den Betreibern vorübergehend vom Netz genommen wurden. Es kam auch zu Angriffen auf Behörden oder Hilfsorganisationen.

Gefahr für Kritische Infrastrukturen

Auch wenn bislang noch keine Kritischen Infrastrukturen (KRITIS) betroffen waren, gibt es in unserer vernetzten Welt zunehmend Abhängigkeiten von Infrastrukturen untereinander. Gibt es Ausfälle in einem Sektor, etwa Energie, IT oder Logistik, kann dies schwere Auswirkungen auf andere Sektoren haben. Daher nimmt das Bundesministerium des Innern und für Heimat (BMI) das Gesamtsystem in den Blick.

Eine wichtige Funktion kommt hierbei dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu. Bereits durch das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) 2021 wurde die Rolle des BSI als Meldestelle für Sicherheitslücken gestärkt und ihm wurden neue Möglichkeiten zur Feststellung, aber auch Schließung von Sicherheitslücken gesetzlich eingeräumt.

Zentralstelle für die Cyber-Sicherheit

Gemäß dem Koalitionsvertrag für die 20. Legislaturperiode soll das BSI darüber hinaus als zentrale Stelle im Bereich IT-Sicherheit ausgebaut werden.

Gefahren im digitalen Raum können sich ohne Beschränkung durch Landes- oder Zuständigkeitsgrenzen verbreiten und auswirken. Um dieser übergreifenden Gefährdungslage effektiv begegnen zu können, müssen Bund und Länder auch im Bereich der Cyber- und Informationssicherheit eng verzahnt, kooperativ und komplementär agieren. Nur eine intensive, dauerhafte und fortgesetzte Zusammenarbeit auf Augenhöhe, die auf einem schnellen und möglichst umfassenden gegenseitigen Informationsaustausch basiert, ermöglicht es, den Gefahren im „grenzenlosen Cyber-Raum" eine effektive Antwort entgegenzusetzen. Vor diesem Hintergrund muss die Zusammenarbeit von Bund und Ländern zukunftsfähig ausgerichtet werden.

Der Mehrwert für die Cyber-Sicherheit in Deutschland bestünde in den Synergieeffekten durch die Einrichtung einer zentralen Meldestelle, in der IT-Sicherheitsvorfallmeldungen aus Bund und Ländern zusammenlaufen und ein umfassendes Lagebild generiert wird. Die Zentralstelle stellt ihrerseits den Ländern über eine geeignete Plattformlösung Informationen in Echtzeit zur Verfügung. Hierbei gibt es mit dem Bundeskriminalamt (BKA) und dem Bundesamt für Verfassungsschutz (BfV) seit Jahrzehnten Modelle, wie eine Zentralstellenfunktion des BSI erfolgreich in die gesamtstaatliche Cyber-Sicherheitsarchitektur zu integrieren wäre, ohne die Souveränität der Länder zu beschneiden.

Europäische Probleme, europäische Lösung

Zum Schutz unserer Kritischen Infrastrukturen müssen wir uns aber auch gesamteuropäisch ausrichten. Hier ist die Umsetzung der NIS-2 Richtlinie ein wichtiger Baustein. Sie ersetzt die NIS-Richtlinie (2016), mit der unter anderem EU-weit die Mitgliedsstaaten zur Identifizierung von Betreibern wesentlicher Dienste bzw. Kritischer Infrastrukturen verpflichtet wurden. Mit Umsetzung der NIS-2-Richtlinie werden in der gesamten EU zukünftig mehr Unternehmen in mehr Sektoren wie Energie, Verkehr, Gesundheit und digitale Infrastruktur Cyber-Sicherheitsvorgaben erfüllen müssen. Künftig werden alle Unternehmen ab der Größe eines mittleren Unternehmens in den gelisteten Wirtschaftssektoren vom BSI-Gesetz erfasst werden (sogenannte Size-Cap-Rule).

Kernpunkt der NIS-2-Richtlinie ist eine Ausweitung von Cyber-Sicherheitsmindestanforderungen und Meldepflichten von Sicherheitsvorfällen an das BSI von rund 4.500 (darunter ca. 1.800 KRITIS Betreiber) auf rund 29.000 Unternehmen in Deutschland. Mit dem Referentenentwurf für ein NIS-2-Umsetzungs- und Cyber-Sicherheitsstärkungsgesetz, der im Juli 2023 in die Ressortabstimmung gegeben wurde, hat das BMI einen wichtigen Meilenstein auf dem Weg zur Umsetzung bis zum Jahresende 2023 erreicht.

Mit der „Cybersicherheitsagenda" des BMI haben wir weitere Maßnahmen auf den Weg gebracht, um die Cyber-Sicherheit insgesamt zu erhöhen. Dies umfasst den sicheren Ausbau und die Erneuerung von Netzen und IT-Systemen der Verwaltung, die Stärkung der Sicherheitsbehörden zu Verfolgung von Cyber Crime sowie die Verbesserung der Abwehrfähigkeiten gegen Cyber-Angriffe insgesamt. Das sind notwendige Investitionen in eine sichere, digitale Zukunft.

> *Zum Schutz unserer Kritischen Infrastrukturen müssen wir uns gesamteuropäisch ausrichten.*

Andreas Könen leitet die Abteilung Cyber- und Informationssicherheit (CI) im Bundesministerium des Innern und für Heimat (BMI). Davor war er Vize-Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Foto: BMI

Die Cyber-Dimension nationaler Sicherheit

Mit der neuen Nationalen Sicherheitsstrategie verabschiedet sich die Bundesregierung vom Sicherheitsbegriff des 20. Jahrhunderts: einer Äußeren Sicherheit, die maßgeblich von der Diplomatie und, wo diese versagt, mit militärischen Mitteln verteidigt wird.

Dr. Regine Grienberger, Auswärtiges Amt

Foto: NASA Goddard Flight Center, flickr.com, CC BY 2.0

Sicherheit wird heute viel umfassender definiert. Sie integriert Innere und Äußere Sicherheit und schließt Dimensionen mit ein, die für das Sicherheitsempfinden von Menschen unverzichtbar sind: z. B. die Sicherheit der Versorgung mit Wasser und Nahrung, Energie und im Gesundheitswesen. Hier nimmt die Cyber-Dimension eine ganz besondere Rolle ein, denn unsere digitalisierte Gesellschaft ist in der Wirtschaft, im sozialen Leben, bei der Teilnahme am politischen Geschehen und in vielen weiteren Bereichen abhängig von einem sicheren Cyber-Space, der allen zugänglich ist.

Vernetzung macht unsere Gesellschaft zugleich verletzlich und stark. Verletzlich, weil jedes Gerät, das mit dem Internet verbunden ist, im Prinzip gehackt werden kann. Stark, wenn

eine Gesellschaft Digitalisierung als Element von Resilienz nutzt. Denn das Beispiel der Ukraine im Krieg zeigt: Digitalisierung erlaubt Redundanzen, schnelle Reaktion und zeit- und ortsunabhängigen Zugriff auf Informationen sowie die Organisation großer Gruppen. Deshalb finden sich die Stellen zur Cyber-Sicherheit in der Nationalen Sicherheitsstrategie auch im Resilienz-Kapitel, das zwischen den beiden Kapiteln zur Wehrhaftigkeit und Nachhaltigkeit steht.

Verantwortung in der Cyber-Domäne teilen

Als Bundesregierung wollen wir die Stabilität des Cyber-Raums in erster Linie durch Maßnahmen der passiven Cyber-Sicherheit herstellen. Dazu gehört „Security by Design" für jedes Gerät, das online gehen kann, ein Mindestmaß an Sicherheitsvorkehrungen an jedem Arbeitsplatz (die sogenannte „Cyber-Hygiene") sowie Sicherheitskonzepte für Behörden und Unternehmen, insbesondere solche, die Kritische Infrastruktur bereitstellen. Europäische Regeln wie die neue Richtlinie für Sicherheit von Netzwerken und IT („NIS-2") bilden die Basis, auf der wir aufbauen.

Dr. Regine Grienberger ist seit 2020 Cyber-Botschafterin im Auswärtigen Amt.

Foto: Auswärtiges Amt

Die Bundesregierung versteht Cyber-Sicherheit als gemeinsame Aufgabe von Staat, Privatsektor, technischen Communities, Wissenschaft und Zivilgesellschaft. Dieser Multi-Stakeholder-Ansatz gilt nicht nur nach innen; das Auswärtige Amt vertritt ihn auch nach außen, als zentrales Element der deutschen Cyber-Diplomatie. Nicht überall ist diese geteilte Verantwortung, insbesondere zwischen Staat und privaten Akteuren, selbstverständlich. Autoritäre Regierungen haben diesem Modell längst den Kampf angekündigt. Aus ihrer Sicht sollte der Staat das Internet kontrollieren; das epidemische Auftreten von organisierter Cyber-Kriminalität, aber auch von Desinformation, Hass und Hetze im Netz liefert ihnen den passenden Vorwand.

Aber nicht nur die Systemkonkurrenz beschäftigt die Cyber-Diplomatie; der Cyber-Raum ist neben Luft, Land, See und Weltraum eine weitere Domäne, in der handfeste Konflikte ausgetragen werden. So macht uns die wachsende Präsenz staatlicher Hackergruppen im Netz, oft mit militärischem oder nachrichtendienstlichem Hintergrund, große Sorgen. Längst geht es nicht mehr nur um Spionage; auch Sabotage und Subversion mit Cyber-Mitteln sind mittlerweile an der Tagesordnung.

Aktiv zur Wehr setzen

Neben der Stärkung unserer Resilienz hat es sich die Bundesregierung daher zur Aufgabe gemacht, ein effizienteres Modell der aktiven Abwehr von schwerwiegenden Cyber-Angriffen aus dem In- und Ausland zu erarbeiten. Zusammen mit den für die Gefahrenabwehr zuständigen Länderstellen muss auch der Bund Gefahren im Cyber-Raum frühzeitig erkennen und laufende Gefahren abwehren können. Grundlage dafür ist eine rechtsstaatliche Neuordnung unserer Kompetenzen und Prozesse („Was sollen wir dürfen?") ebenso wie Investitionen in Fähigkeiten („Was sollen wir können?"). Gleichwohl ist aktive Abwehr ein Begriff, zu dem es in der deutschen Öffentlichkeit noch Diskussionsbedarf gibt. Im Spektrum möglicher Instrumente und Einsatzbereiche grenzt sich die Nationale Sicherheitsstrategie einerseits deutlich vom „Hackback" als Vergeltungsmaßnahme mit Cyber-Mitteln ab. Aber auch von der anderen Seite des Spektrums, dem „weiter wie bisher", nimmt die Nationale Sicherheitsstrategie entschieden Abstand. Die Nationale Sicherheitsstrategie ist daher ein Arbeitsauftrag an die verschiedenen Ressorts der Bundesregierung, gemeinsam neue Maßnahmen zur Stärkung unserer Cyber-Sicherheit auf den Weg zu bringen: angefangen mit einem ganzheitlichen Lagebild, über hochsichere Kommunikations- und Informationssysteme bis hin zu einer (zivilen) Cyber-Sicherheitsarchitektur, die der komplexen Bedrohungslage angemessen ist.

Cyber-Sicherheit kennt keine Grenzen

Dass all dies in Einklang mit globalen Normen und dem Völkerrecht stehen muss, versteht sich von selbst. Unsere Partner wie auch mögliche Gegner weltweit schauen genau auf das Modell integrierter Cyber-Sicherheit, das derzeit in Deutschland entwickelt wird. Denn gerade im Cyber-Space sind solche Maßnahmen nie rein national, sondern wirken sich immer international aus.

Wirkliche Cyber-Sicherheit kann man nicht alleine, sondern nur gemeinsam erreichen. Für das Auswärtige Amt ergibt sich daraus ein neuer Schwerpunkt in der Cyber-Diplomatie: der Cyber-Kapazitätsaufbau. Gemeinsam mit unseren Partnern sollen dadurch sowohl deren nationale Fähigkeiten entwickelt als auch Kooperationsformate aufgebaut werden, die von der Krisenintervention und der Bekämpfung von Cyber-Kriminalität bis zur gemeinsamen Arbeit an Regeln und globalen Normen reichen.

Letztlich gibt es im Cyber-Space keine Grenzen. Cyber-Sicherheitspolitik ist daher immer auch Cyber-Außenpolitik.

Präventive Informationssicherheit

Mit seinen Computer Emergency Response Teams gewährleistet das Zentrum für Cyber-Sicherheit der Bundeswehr schnelle und flexible Reaktionen auf Angriffe gegen die IT der Bundeswehr im In- und Ausland und in den Einsätzen.

Generalmajor Jürgen Setzer, Bundeswehr

In heutigen Konfliktszenarien setzen Angreifende auf eine Kombination aus klassischen Militäreinsätzen, Propaganda in den Medien und Sozialen Netzwerken sowie direkten Computerangriffen. Das Vorgehen von scheinbar unsichtbaren Gegnern in „hybrider Kriegsführung“ ist allgegenwärtig. Wie antwortet die Bundeswehr erfolgreich und resilient auf Cyber-Angriffe?

Eine intakte Führungsfähigkeit ist von zentraler Bedeutung für eine verteidigungsfähige Bundeswehr. Die Informationssicherheit ist daher heute eine der wesentlichen Voraussetzungen für die Einsatzbereitschaft und den Einsatz. Ohne die gesicherte Verfügbarkeit, die Integrität und die Vertraulichkeit von Daten können wir heute unseren Auftrag weder im Grundbetrieb noch im Einsatz erfüllen. Deshalb kommt dem Schutz unserer Informationen bei deren Bearbeitung, Übertragung und Speicherung eine entscheidende Bedeutung zu.

Der Kampf gegen (staatliche) Hacker und Kriminelle im Cyber-Raum

Am Freitag, dem 13. Februar 2009, traf ein Computerwurm auch mehrere hundert Rechner der Bundeswehr und legte wichtige Kommunikationsmittel lahm. Die Angreifenden sind bis heute nicht bekannt. Seitdem haben Akteurinnen und Akteure im Cyber-Raum weiter aufgerüstet. Angriffe aus dem Ausland mit Erpresserschadsoftware, sogenannter Ransomware, auf Unternehmen, Krankenhäuser und staatliche Einrichtungen in Deutschland haben bereits 2021 ein bedrohliches Ausmaß angenommen.

2022 steigerte sich diese Bedrohung aus dem Cyber-Raum auf ein noch nicht gekanntes Potenzial sowohl gegen Wirtschaft, staatliche Einrichtungen als auch Kritische Infrastrukturen in Deutschland. Immer wieder wird versucht, zum Beispiel durch „Distributed Denial of Services“(DDoS)-Angriffe, die Verfügbarkeit von Informations- und Kommunikationsplattformen zu stören. Zumeist ist nicht eindeutig zu erkennen, wer die Angreifenden sind. Wird zum Beispiel eine IP-Adresse aus einem bestimmten Adressraum eines Landes genutzt, bedeutet dies noch nicht, dass der Angriff diesem Land oder einer bestimmten Personengruppe zugeschrieben werden kann.

Angreifende bleiben meist im Verborgenen – die Schwierigkeit einer Attribution

Bereits mit niedrigschwelligen Cyber-Angriffen können Gegnerinnen und Gegner unerkannt spürbare Wirkung erzielen. Bei sogenannten DDoS-Angriffen nutzen Angreifende angemietete Bot-Netze, meist aus dem Darknet, deren Geräte weltweit verteilt sind. Wenn es kein „Bekennerschreiben“ im Netz gibt, ist eine Zuordnung zu einem bestimmten Angreifer bzw. einer bestimmten Angreiferin kaum möglich.

Das statistische Nachhalten erkannter Pings, Port-Scans oder einzelner E-Mails, beispielsweise einer Schadsoftwarewelle, liefert zwar sehr große Informationsmengen, die statistische Aussagen zulassen, jedoch keine Bewertung hinsichtlich konkreter Gefährdungen oder Angreiferinnen und Angreifer. Von hoher Relevanz sind dagegen potenziell schädliche Ereignisse innerhalb der Netze der Bundeswehr, also auf Servern und am Arbeitsplatz-PC erkannte Schadsoftware oder schadhafte Ereignisse, die durch die kaskadierten Schutzmaßnahmen nicht erkannt wurden. Hier kann man durch weitergehende Analysen gegebenenfalls die Techniken, Taktiken und Prozeduren (TTP) mit denen bekannter Muster vergleichen und so auf bestimmte Angreiferinnen und Angreifer schließen.

Unabhängig davon, ob es sich um Ereignisse an den Firewalls, auf den Arbeitsplatzrechnern oder im Netzwerk han-

delt: Ob und wie einzelne Ereignisse zu „einem“ Angriff zusammengehören, lässt sich überhaupt nur in wenigen Ausnahmefällen bei konkretem Verdacht mit sehr hohem Aufwand, etwa durch IT-forensische Untersuchungen, feststellen. Die Zuordnung und eine konkrete Attribution jedes Einzelfalles ist also schlichtweg nicht möglich und letztlich zum Festlegen geeigneter Schutzmaßnahmen für unsere Systeme grundsätzlich auch nicht relevant. Große Phishing-Angriffe können zum Beispiel sehr gut durch technische Anpassung geblockt werden. Spear-Phishing-Angriffe, also zielgerichtete und auf das Opfer präparierte Köder, sind durch präventive Awareness-Schulungen besser zu erkennen und abzuwehren.

Kontinuierliche Verbesserung durch ein funktionierendes Information Security Management System (ISMS)

Die Bundeswehr hat sich auf Szenarien im Cyber-Raum bestmöglich vorbereitet. Dazu wurden unterschiedliche Vorkehrungen getroffen. Dies sind zum einen technische Maßnahmen und zum anderen etablierte Prozesse, die die gesamte Kette von Detektion, Reaktion und Prävention umfassen.
Aber die Angreifer entwickeln ständig ihre Techniken weiter. Alle Nutzerinnen und Nutzer von IT stehen daher täglich vor der Herausforderung, sich nicht von den sich ständig ändernden Taktiken der Angreifer überraschen zu lassen.
Seit 2017 ist dem stellvertretenden Inspekteur Cyber- und Informationsraum (CIR) auch das Amt des „Chief Information Officers der Bundeswehr“ (CISOBw) übertragen, welche ich beide im April 2018 übernommen habe. Als Angehöriger des Kommandos CIR in Bonn bin ich daher für die Informationssicherheit in der gesamten Bundeswehr verantwortlich. Als CISOBw ist mir das Zentrum für Cyber-Sicherheit der Bundeswehr in Euskirchen fachlich und seit dem 01.10.2022 auch truppendienstlich unterstellt. Es ist die zentrale Dienststelle zur Gewährleistung eines umfassenden Schutzes der IT-Systeme und -Services der Bundeswehr. Mit seinen Computer Emergency Response Teams (CERT) gewährleistet das Zentrum schnelle und flexible Reaktionen auf Angriffe gegen die IT der Bundeswehr im In- und Ausland und in den Einsätzen.

Ein Botnet ist ein Netzwerk infizierter Computer, das aus der Ferne gesteuert und dazu verwendet werden kann, Spam zu versenden, Malware zu verbreiten oder DDoS-Angriffe durchzuführen – alles ohne die Zustimmung der Gerätebesitzer.

Detektion von Ereignissen und Sicherheitsvorkommnissen

Innerhalb der Netze der Bundeswehr, also zwischen den Netzübergängen in andere Netze zum Beispiel in und aus dem Internet, auf Servern und auf Arbeitsplätzen, wird der Netzwerkverkehr kontinuierlich auf ungewöhnlichen Datenverkehr, zum Beispiel bei Schadsoftware in E-Mails oder

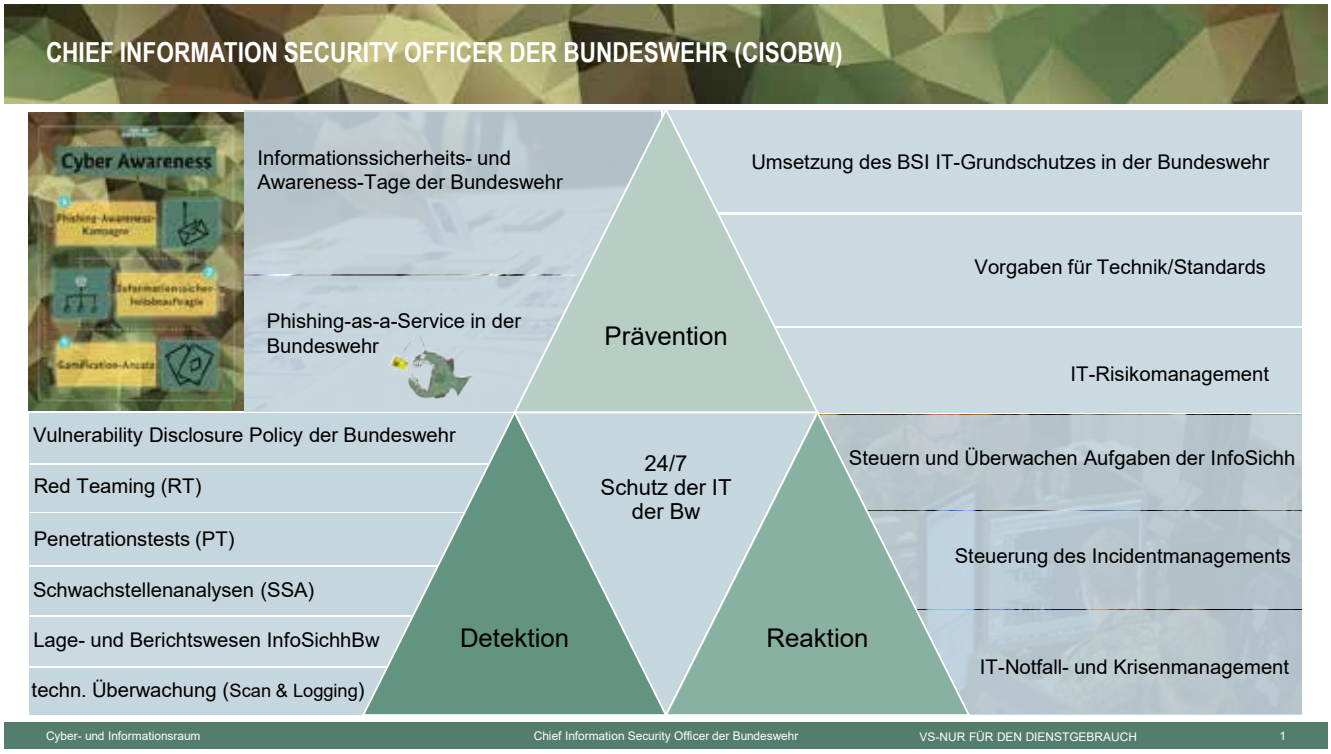


Abb. 1: Schutz der Bundeswehr-IT durch Detektion, Reaktion und Prävention

Grafik: Bundeswehr/Opper

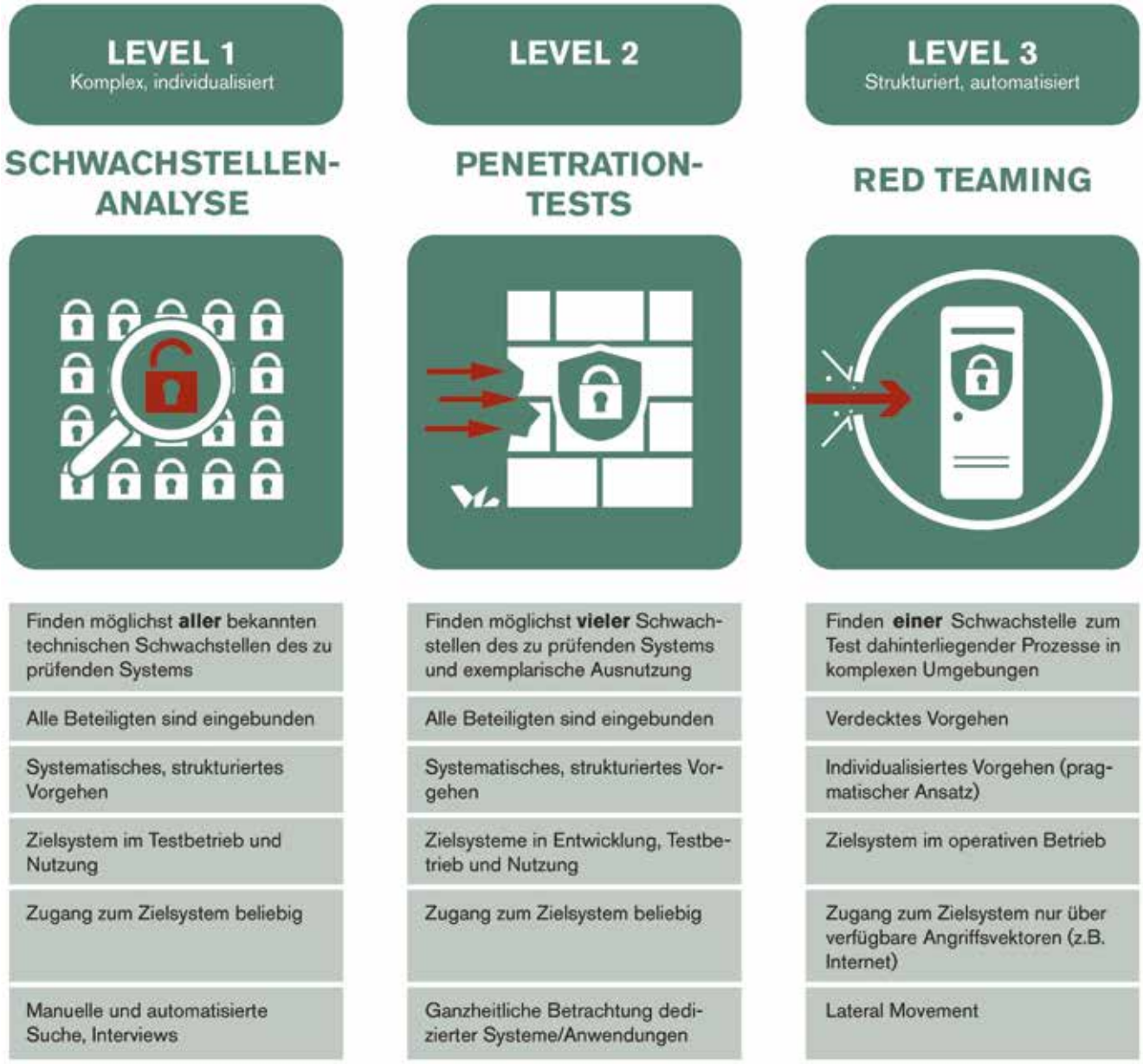


Abb. 2: Maßnahmen zur Cyber-Sicherheit

Grafik: Bundeswehr/PIZ CIR

außergewöhnlichem Abfluss von Datenmengen in das Internet, überwacht. Netzwerksensoren erfassen alle Ereignisse und werden im Rahmen eines Security Information and Event Managements durch Analystinnen und Analysten des Lage- und Überwachungszentrums (LÜZ) im Cyber Security Operations Center der Bundeswehr (CSOCBw) 24/7 ausgewertet und bearbeitet. Das LÜZ ist die zentrale Stelle zur Bearbeitung von Informationssicherheitsvorkommnissen in der Bundeswehr. Von hier aus werden alle wichtigen Stellen für die Behandlung und Eindämmung von sicherheitsrelevanten Vorfällen koordiniert und überwacht.

Die Wirksamkeit umgesetzter Maßnahmen zur Cyber-Sicherheit werden in der Bundeswehr auch regelmäßig durch Sicherheitsinspektionen, Schwachstellenanalysen, Penetrationstests und Red Teaming überprüft, auch unabhängig von besonderen Lagen.

Reaktion

Das CSOCBw im Zentrum für Cyber-Sicherheit der Bundeswehr bearbeitet alle sicherheitsrelevanten Vorkommnisse als zentrale Stelle für den gesamten Geschäftsbereich des BMVg auf operativer Ebene. So kann der Chief Information Security Officer der Bundeswehr die Informationssicherheit mit all ihren komplexen Herausforderungen erfolgreich steuern, überwachen und bedarfsorientiert mit dem IT-Notfallmanagement und IT-Krisenmanagement auf Vorfälle, die strategische Auswirkungen erreichen können, reagieren.

Prävention

Technik und Prozesse sind aber nichts ohne die Wachsamkeit der Soldatinnen und Soldaten sowie der zivilen Mitarbeiterinnen und Mitarbeiter. Ihre Aufmerksamkeit ist entscheidend, ebenso wie die schnelle und richtige Reaktion.

Cyber-Angriffe werden immer komplexer und können nicht immer durch technische Vorkehrungen erkannt und gefiltert werden. Angriffsvektoren nutzen häufig ausgeklügelte Techniken und Taktiken. Es kommt auf jede Soldatin oder zivile Mitarbeiterin und jeden Soldaten oder zivilen Mitarbeiter an. Sie sind, bildlich gesprochen, die letzte Verteidigungslinie – „the last line of defence."
Zudem werden in der Bundeswehr die IT-Grundschutzmaßnahmen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durch Vorgaben und Richtlinien umgesetzt. Durch regelmäßige fachliche Informations- und Awareness-Veranstaltungen bleiben die IT-Nutzenden auf dem aktuellen Stand.

Anwendung einer Vulnerability Disclosure Policy im Behördenumfeld

Trotz sorgfältiger Implementierung der IT, professioneller Konfiguration und umfangreicher Tests können dennoch Schwachstellen vorhanden sein. Seit Oktober 2020 richte ich mich als Chief Information Security Officer der Bundeswehr (CISOBw) darüber hinaus an alle externen IT-Sicherheitsforscherinnen und -forscher, also die gutgesinnten Hacker, die mit ihrer Expertise Schwachstellen in Systemen der Bundeswehr entdecken und melden. Das „Hacken" von IT-Systemen ist grundsätzlich strafrechtlich relevant. Mit der Vulnerability Disclosure Policy der Bundeswehr (VDPBw) wurden die rechtlichen Rahmenbedingungen für die IT-Sicherheitsforschenden geschaffen. Sie erlaubt den IT-Sicherheitsforschenden, Schwachstellen in den Bundeswehr-Systemen zu suchen, sie zu identifizieren und auch mitzuteilen, bevor Angreiferinnen und Angreifer diese missbrauchen können. Dabei kommt es nicht zum Konflikt mit dem Strafgesetzbuch. Diese Experten und Expertinnen verfolgen eine gute Absicht und leisten einen Beitrag zu unserer aller Sicherheit und somit dem Gemeinwohl. Hierbei steht der gemeinsame Sicherheitsgedanke des Internets im Vordergrund.

Unseren Dank und Respekt zeigen wir auch öffentlich

Die hohe Anzahl an Meldungen zeigt, dass der durch die Bundeswehr ausgelobte, nicht monetäre Anreiz wirksam ist. Besonders verdiente IT-Sicherheitsforschende werden mit dem VDPBw-Coin ausgezeichnet. Eine Grundvoraussetzung dafür ist, mindestens drei qualifizierte IT-Schwachstellen bei der Bundeswehr gemeldet zu haben. Die Bundeswehr hat mit der VDPBw einen vorsichtigen Einstieg in dieses Instrument der Schwachstellenmeldungen gewählt. Zwar sind wir bislang alleiniger Vorreiter im Behördenumfeld, aber andere wollen nachziehen. So kann gemeinsam das gesamtstaatliche Sicherheitsniveau verbessert werden.

Großer Dank und Respekt geht an alle IT-Sicherheitsforschenden, die dazu beitragen, die IT-Systeme der Bundeswehr sicherer zu machen. Diesen Dank machen wir öffentlich mit dem individuellen Eintrag und der Namensnennung auf einer Dankesseite auf bundeswehr.de. Warum das ein zusätzlicher Anreiz sein kann? Welcher Hacker kann schon legal von sich behaupten, dass er die Bundeswehr gehackt hat und mit seiner Hilfe dort eine Schwachstelle gefunden und das Internet ein wenig sicherer gemacht wurde?

Mit dem VDPBw-Coin werden besonders verdiente IT-Sicherheitsforschende ausgezeichnet. *Foto: Bundeswehr/Stefan Uj*

Die Anwendung der VDPBw kann deshalb – als Ergänzung zu den durch bundeswehreigene Kräfte durchgeführten Untersuchungen – Informationen zu unbekannten Schwachstellen und Sicherheitslücken in den Systemen der Bundeswehr liefern. Sie trägt dazu bei, jene Schwachstellen und Lücken zu schließen und so das Risiko eines erfolgreichen Angriffs gegen die Bundeswehr-Informationstechnik zu vermindern. Als Chief Information Security Officer der Bundeswehr und damit auch der gesamten deutschen Streitkräfte setze ich auch auf das Wissen und die Hilfe der Cyber-Community für ein sichereres Internet in Deutschland und Europa.

Fazit

Die Bundeswehr hat ein umfangreiches Informationssicherheitssystem eingerichtet, das kontinuierlich optimiert und an die jeweils aktuelle Bedrohungslage angepasst wird. Dieses System umfasst nicht nur technische (Hard- und Software), sondern auch organisatorische (Rollen und Rechte) und personelle (Ausbildung, Sensibilisierung) Maßnahmen. Damit sind wir jederzeit auf eine Verschärfung der Sicherheitslage vorbereitet und unsere mobilen Computer Emergency Response Teams sind rund um die Uhr verfügbar, um bei akuten Notfällen eingreifen zu können. Wir sind hier gut aufgestellt, aber um dieses Niveau zu halten, müssen wir uns ständig weiterentwickeln.

Generalmajor Jürgen Setzer ist stellvertretender Inspekteur CIR und Chief Information Security Officer der Bundeswehr (CISOBw).

Das Nationale Cyber-Abwehrzentrum sichert behördenübergreifenden Informationsfluss

Die Bedrohungslage im Cyber-Raum ist auf einem unverändert sehr hohen Niveau. Ransomware-Angriffe legen längst nicht mehr nur die Produktion von Unternehmen lahm. Wenn es Landkreise, Kommunen oder gar Krankenhäuser trifft, sind oftmals auch Bürgerinnen und Bürger betroffen.

Roland Hartmann, BSI

Oberstleutnant Jan Pangerl, Bundeswehr

Foto: vxla, CC BY 2.0, flickr.com

Die Aktivitäten der Cyber-Spionage und -sabotage durch staatliche Akteure zielen auf politische Entscheidungsprozesse, die Wirtschaft sowie durch Desinformation auch auf alle Bürgerinnen und Bürger. Um das Vertrauen der Gesellschaft in die Funktionsfähigkeit des Staates, wichtige Dienstleistungen und Infrastrukturen zu stärken, ist Cyber-Sicherheit eine essenzielle Voraussetzung.

Ein strategischer Rahmen

Die Nationale Sicherheitsstrategie (NSS) beschreibt Cyber-Sicherheit „als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft“ und betrachtet sie „angesichts der Bedeutung des digitalen Raums“ als „essenziellen Teil von integrierter Sicherheit“. Hier setzt die Bundesregierung auf „das Zusammenwirken der staatlichen Institutionen für Cybersicherheit und Strafverfolgung sowie von Nachrichtendiensten, Diplomatie und Militär bei der Abwehr von Cyberbedrohungen“ und sieht die Erstellung und Haltung eines gesamtstaatlichen Cyber-Lagebildes beim Nationalen Cyber-Abwehrzentrum (Cyber-AZ) vor. Die zuletzt 2021 fortgeschriebene „Cybersicherheitsstrategie“ (CSS) bereitet die strategischen Themenfelder der Cyber-Sicherheit strukturiert auf und hebt damit verbundene Handlungsnotwendigkeiten auch für das Cyber-AZ hervor. Dabei sind das BSI und das Kommando CIR nur zwei von mehreren Akteuren, die mit der CSS adressiert werden und die im Cyber-AZ an deren Umsetzung mitwirken.

Koordinierte Cyber-Abwehr

Cyber-Abwehr umfasst alle Maßnahmen mit dem Ziel, den Erfolg von tatsächlichen oder geplanten Cyber-Angriffen zu verhindern oder abzuschwächen. Dabei obliegt den am Cyber-AZ beteiligten Behörden die Ausübung ihrer operativen Befugnisse zur Cyber-Abwehr. Die Hauptaufgaben des Cyber-AZ sind ein umfassendes Lagebild bereitzustellen und die Koordination von Maßnahmen zwischen den zuständigen Behörden durch Informationsaustausch sicherzustellen.

Auf Bundesebene arbeiten acht gleichberechtigte Kernbehörden im Cyber-AZ zusammen. Hinzu kommt eine Reihe assoziierter Behörden und Einrichtungen aus Bund und Ländern. Sie führen ihre jeweils eigene Lage zusammen, um möglichst frühzeitig Informationen auszutauschen. So können sie gemeinsam die Gesamtlage bewerten und Maßnahmen im Cyber-AZ koordinieren.

Das BSI wirkt dabei als die Informationssicherheitsbehörde des Bundes. Als zentrale Meldestelle für Informationssicher-

heitsvorfälle – sowohl in der Bundesverwaltung als auch von KRITIS-Betreibern – verfügt das BSI über eine Vielzahl von Informationen über die aktuelle Informationssicherheitslage und trägt damit zur Cyber-Sicherheitslage bei.

Wird ein IT-Sicherheitsvorfall erkannt oder gemeldet, nehmen das Nationale IT-Lagezentrum und CERT-Bund im BSI eine Erstbewertung vor. Bei Bedarf und unter Berücksichtigung der Interessen der Betroffenen kann sich das BSI im Cyber-AZ dazu mit anderen Behörden austauschen und weitere Maßnahmen koordinieren, um bestmöglich helfen zu können.

Für die Bundesverwaltung und Kritische Infrastrukturen kann weitere BSI-Expertise in den Bereichen Schadprogramm-Analyse, digitale Forensik oder Logdatenanalyse ergänzend in die Vorfallanalyse eingebracht werden. In besonders herausgehobenen Fällen kann das BSI ein Mobile Incident Response Team (MIRT) zur Unterstützung vor Ort entsenden.

Lageinformationen mit gesamtstaatlichem Bezug werden in die Lagebesprechungen des Cyber-AZ eingebracht, so den anderen Behörden zur Verfügung gestellt und durch diese mit jeweils eigenen, in die Lagebesprechung eingebrachten Informationen angereichert und gegebenenfalls gemeinsam bewertet. So ergibt sich ein Gesamtlagebild mit weiteren Perspektiven, das zusammen aussagekräftiger ist als die Summe der einzelnen Zuarbeiten.

Cyber-Abwehr als integraler Bestandteil der Cyber-Verteidigung

Cyber-Verteidigung definiert die CSS 21 als die Gesamtheit der Maßnahmen der Bundeswehr im „Rahmen ihres verfassungsmäßigen Auftrages und der vorhandenen defensiven und offensiven Fähigkeiten zum Wirken im Cyber-Raum, die zur Einsatz- und Operationsführung geeignet und erforderlich sind oder zur Abwehr von (militärischen) Cyber-Angriffen und damit dem Schutz eigener Informationen, IT, sowie Waffen- und Wirksysteme dienen. Dazu gehören auch die Nutzung und Mitgestaltung von Strukturen, Prozessen und Meldewesen der Cyber-Abwehr unter verteidigungsrelevanten Aspekten und Situationen.“ Damit ist auch das Cyber-AZ adressiert.

Dies sind unter anderem Maßnahmen und Fähigkeiten eigener Kräfte und Dienstleister der Bundeswehr zum sicheren Betrieb von IT-Services und Kommunikationsnetzen für die taktische und operative Ebene sowie die Gewährleistung der Informationssicherheit und des Schutzes der IT der Bundeswehr im Inland oder Einsatzgebieten. Dies stellt somit die Basis für die Kommunikation der Streitkräfte in allen Dimensionen zur Verfügung.

Weiterhin wird durch das Zentrum für Cyber-Sicherheit der Bundeswehr die zentrale Überwachungs- und Reaktionsfähigkeit (Incident Response) im Inland und in Einsatzgebieten für die Informationssicherheit der Bundeswehr sichergestellt.

Wesentlicher Bestandteil der Cyber-Verteidigung ist daneben die Aufklärungsleistung des Militärischen Nachrichtenwesens in allen Dimensionen (Land, Luft, See, CIR und Weltraum). So werden Operationen in allen Dimensionen durch zusammengeführte Erkenntnisse aus allen Aufklärungsdisziplinen unterstützt.

Schließlich stellt der Organisationsbereich CIR Wirkmöglichkeiten für die eigene oder dimensionsübergreifende Operationsführung bereit.

Landes- und Bündnisverteidigung sind als Gesamtverteidigung nur gesamtstaatlich zu leisten. Dies gilt auch für den Anteil Cyber-Verteidigung. Aufgrund der vielfältigen Beziehungen und gegenseitigen Abhängigkeiten betrachten die Streitkräfte die Cyber-Abwehr als integralen Bestandteil der Cyber-Verteidigung. Wesentliche Erkenntnisse aus diesem Bereich müssen immer – also auch schon im Frieden – in das eigene Lagebild der Streitkräfte einfließen und Maßnahmen der unterschiedlichen Akteure miteinander abgestimmt werden. Hierzu ist der Austausch im Cyber-AZ ein wesentlicher Faktor.

Blick in die Zukunft

Alle im Cyber-AZ vertretenen Einrichtungen und Behörden nutzen das Cyber-AZ als Koordinationsplattform. Seine eingespielten Kommunikationsstränge und eingeübten Prozesse verhindern, dass bei Handlungsnotwendigkeiten überhaupt „Sand ins Getriebe“ kommt. Falls doch, stellen sie sicher, dass er schnell wieder entfernt wird. Auf diese Weise wird durch Erfahrung und Dokumentation ein Prozess etabliert, der eine kontinuierliche Optimierung der Cyber-Abwehr und somit auch der Cyber-Verteidigung ermöglicht.

Entsprechend der Nationalen Sicherheitsstrategie soll das Cyber-AZ zukünftig die gesamtstaatliche Cyber-Lage führen. Hier gilt es, jetzt die entsprechende Grundlagenarbeit in Ableitung der Anforderungen aus der Strategie zu leisten, um in der Folge Rahmenbedingungen und Voraussetzungen für dieses umfassende und gesamtstaatliche Cyber-Lagebild sowie dessen Bereitstellung zu schaffen.

Roland Hartmann arbeitet beim Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, und ist stellvertretender Koordinator des Nationalen Cyber-Abwehrzentrums.

Oberstleutnant Jan Pangerl gehört dem Kommando Cyber- und Informationsraum (KdoCIR) der Bundeswehr, Bonn, an und ist stellvertretender Koordinator des Nationalen Cyber-Abwehrzentrums.

Die Nationale Sicherheitsstrategie braucht dringend Updates

Die internationale Bedrohungslage für Deutschland im Cyber-Space nimmt in Quantität und Qualität stark zu. Gemäß dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Bedrohungslage im Cyber-Raum so hoch wie nie zuvor. Sie stellt eine echte Bedrohung für Staat, Gesellschaft und Wirtschaft dar.

Dr. Reinhard Brandl, MdB (CDU/CSU)

Russland setzt in seinem Angriffskrieg auf die Ukraine neben konventionellen Waffen auch Instrumente zur Cyber-Kriegsführung ein. Das zeigen ganz deutlich die rund 3.000 Windräder in Deutschland, deren Funktionen bei einem mutmaßlich russischen Angriff auf den vom ukrainischen Militär genutzten Satelliten-Betreiber Viasat als Kollateralschaden gestört wurden.

Die behördlichen Zuständigkeiten im Cyber-Raum zeichnen sich in der Bundesrepublik Deutschland dagegen aktuell vor allem dadurch aus, dass der Bund bei einem großen Cyber-Angriff auf Deutschland nur zuschauen kann. Zwar ist das BSI unter der Dienstaufsicht des Bundesministeriums des Innern und für Heimat (BMI) auf Bundesebene für die Cyber-Sicherheit verantwortlich. Für die Abwehr von Gefahren – und damit auch von Cyber-Gefahren – sind derzeit aber grundgesetzlich die Bundesländer zuständig. Das BSI hilft nur dann, wenn die Länder darum bitten. Die Befugnisse und Instrumente des Bundes im Cyber-Raum sind daher rein präventiver und beratender Natur. Auch die Zuschreibung von Cyber-Angriffen zu Akteuren ist damit gegenwärtig häufig nur sehr schwer möglich. Welche Kompetenzen das gut aufgestellte Kommando CIR der Bundeswehr im Falle

Foto: Peter H, pixabay.com

eines Cyber-Angriffs hat, ist darüber hinaus völlig unklar. Kurz gesagt: Im Ernstfall steht Deutschland im Cyber-Raum blank da.

Verfügbares Schutzprogramm getestet: Nationale Sicherheitsstrategie defizitär

Die Ampel-Regierung hat mit der Nationalen Sicherheitsstrategie im Sinne eines ganzheitlichen Ansatzes versucht, eine „One fits all"-Lösung für alle sicherheitspolitischen Bereiche vorzulegen. In der Analyse der Gefahrenlage im Cyber-Raum und der Defizite in der Cyber-Sicherheitsarchitektur liegt sie weitgehend richtig. Erfreulicherweise erkennt sie auch, dass die historisch gewachsene, strikte institutionelle Trennung der Äußeren und Inneren Sicherheit für den Cyber-Raum überholt scheint und wir stattdessen in diesem Punkt die Zusammenarbeit der beiden Dimensionen intensivieren müssen.

Wenn es dann aber an konkrete Vorschläge geht, wie Deutschland der steigenden Bedrohung im Cyber-Raum begegnen kann, sind der Nationalen Sicherheitsstrategie die in der Presse berichteten Streitereien innerhalb der Ampel-Koalition deutlich anzumerken. Zwar enthält sie einige gute Vorschläge wie die Erstellung eines ganzheitlichen Cyber-Lagebilds. Dennoch bleibt mit der Nationalen Sicherheitsstrategie die Zeitenwende in der Cyber-Abwehr aus folgenden Gründen erst einmal aus.

Erstens verkündet die Ampel zwar eine Weiterentwicklung der „Cybersicherheitsstrategie" der Bundesregierung. Das tut sie damit aber bereits zum dritten Mal, nachdem diese erst im Koalitionsvertrag im Jahr 2021 und dann in der „Cybersicherheitsagenda" des BMI im Jahr 2022 groß angekündigt war. Bis heute liegt immer noch keine neue Cybersicherheitsstrategie der Ampel vor. Fraglich ist deshalb, ob die Ampel vor lauter Streitereien die Weiterentwicklung überhaupt noch in dieser Legislaturperiode schafft.

Zweitens duckt sich die Ampel ebenfalls aufgrund interner Streitereien bei der Antwort auf die Frage nach einer aktiven Cyber-Abwehr weg und flüchtet sich in einen wachsweichen Prüfauftrag. Damit bleibt Deutschland in der Cyber-Sicherheit weiterhin nur bedingt abwehrbereit.

Drittens ist die erneute Ankündigung der Ampel, das BSI unabhängiger aufstellen zu wollen, eine absolute Farce. Denn zum einen musste Bundesinnenministerin Faeser im April eingestehen, dass die Absetzung des BSI-Präsidenten Arne Schönbohm ungerechtfertigt war. Dafür hat Ministerin Faeser sich bis heute nicht öffentlich entschuldigt oder Herrn Schönbohm rehabilitiert. Zum anderen hat die Ampel-Koalition in diesem Jahr ein Gesetz geändert, mit dem die Präsidentin des BSI vom BMI jederzeit in den einstweiligen Ruhestand versetzt werden kann. Somit befindet sich die neue BSI-Präsidentin in einer völligen Abhängigkeit in allen ihren Entscheidungen gegenüber der Bundesregierung. Das ist das genaue Gegenteil der Forderung im Ampel-Koalitionsvertrag nach einem unabhängigeren BSI.

Viertens enthält die Nationale Sicherheitsstrategie keine konkreten Maßnahmen, wie die Zusammenarbeit von Innerer und Äußerer Sicherheit im Cyber-Raum spürbar intensiviert werden soll. Die Gründung eines Nationalen Sicherheitsrats beispielsweise, der genau der richtige Ort für die strategische Integration aller sicherheitspolitischen Bereiche wäre, ist in der Nationalen Sicherheitsstrategie nicht enthalten. Wie aus der Presse zu erfahren ist, konnte sich die

Stehen als Kollateralschäden seit dem Krieg Russlands in der Ukraine öfter im Fokus: Windräder als Teil der Kritischen Infrastruktur. Die Resilienz von Deutschlands Cyber-Sicherheitsarchitektur wird immer wichtiger.

Foto: Peter H, pixabay.com

Ampel nicht darauf einigen, wo der Nationale Sicherheitsrat angesiedelt wäre.

Zusammenfassend sieht eine schlagkräftige Nationale Sicherheitsstrategie aus Perspektive der Cyber-Sicherheit definitiv anders aus. Vielmehr führt der vorgelegte Ampel-Kompromiss am Ende in die weitgehende Handlungsunfähigkeit Deutschlands bei der Cyber-Abwehr.

Day-One-Patch nötig: Lücken in der Cyber-Abwehr schnell schließen

Im Folgenden unterbreite ich fünf konstruktive Vorschläge für eine Neuaufstellung der Cyber-Abwehr unter gesamtstaatlichen Gesichtspunkten.

Erstens, die Cybersicherheitsstrategie darf nicht mehr nur von der Bundesregierung angekündigt, sondern sie muss endlich vorgelegt werden.

Zweitens, der Bund sollte nicht nur eine Zuständigkeit zur Abwehr von schweren Cyber-Angriffen aus dem In- und dem Ausland bekommen. Er sollte diese auch aktiv zuordnen und beenden können. Dabei lehne ich den Begriff des Hackbacks ab. Er impliziert Maßnahmen im Sinne von zerstörerischen Vergeltungsschlägen. Darum geht es nicht. Dem Bund sollten dennoch aktive Cyber-Abwehrfähigkeiten an die Hand gegeben werden, um auch in fremden Netzen laufende Angriffe unterbrechen und forensische Analysen zur Attribution des Angriffs durchführen zu können. Dafür müssen wir die rechtlichen, personellen und technischen Voraussetzungen schaffen.

Drittens, das ganzheitliche Cyber-Lagebild sollte auch tatsächlich alle staatlichen Ebenen und die wesentlichen Kritischen Infrastrukturen umfassen.

Viertens, in einer Gefahrenlage müssen die Abwehrprozesse reibungslos funktionieren. Deshalb darf nicht nur die Bundesregierung flexible Abstimmungs- und Entscheidungswege einüben. Vielmehr müssen alle föderalen Ebenen in der Cyber-Abwehr eingespielter werden. Dafür brauchen wir regelmäßige gemeinsame Cyber-Übungen der Bundes-, der Länder- und der Kommunalebene – inklusive der Bundeswehr.

Fünftens schlage ich zur intensiveren Verzahnung der zivilen und militärischen Cyber-Fähigkeiten einen Personalaustausch zwischen BSI und der Bundeswehr vor. Soldatinnen und Soldaten sollen in Friedenszeiten beim BSI unter dessen Hoheit in den MIRTs (Mobile Incident Response Teams) eingesetzt werden und dort Praxiserfahrung sammeln. Im Verteidigungsfall würden sie mit den erlernten Fähigkeiten in die Bundeswehr zurückkehren.

Geopolitische Lage duldet keinen Aufschub

Auch nach der Veröffentlichung der Nationalen Sicherheitsstrategie bleibt die Forderung nach mehr gesamtstaatlicher Verantwortung Deutschlands im Cyber-Raum aktuell. Die Anpassung der Cyber-Sicherheitsarchitektur an die aktuellen Herausforderungen ist erst einmal weiter auf die lange Bank geschoben. Die derzeitige geopolitische Lage duldet aber keinen weiteren Aufschub. Jeden Tag könnte Deutschland ein großer Cyber-Angriff treffen. Daher braucht die Nationale Sicherheitsstrategie dringend wichtige Updates für die Cyber-Abwehr. Sonst werden unsere Sicherheitslücken irgendwann ausgenutzt.

Dr. Reinhard Brandl ist digitalpolitischer Sprecher der CDU/CSU-Fraktion im Bundestag.

Foto: Tobias Koch

Gezielte Cyber-Angriffe im Teamwork stoppen

Cloud-Dienste revolutionieren die Arbeitswelt, sorgen aber mit sich auflösenden Netzwerkgrenzen für neue Ansprüche in Sachen Cyber-Security. Die performante IT lässt sich mit traditionellen IT-Sicherheitsprodukten nicht mehr schützen – die effektive und NIS-2-konforme Lösung bietet Cyber-Security as a Service.

Foto: BS/Wynn Pointaux, pixabay.com

Die frühzeitige Erkennung von und Reaktion auf Gefahren ist für staatliche Verwaltungen und öffentliche Einrichtungen nichts Neues. Bestes Beispiel sind Brandmeldeanlagen für den vorbeugenden Brandschutz und begleitende Räumungsübungen. In der IT verhält sich der Sachverhalt nicht anders: Ein effektive Frühwarnerkennung ist ein essenzieller Baustein für die moderne Cyber-Abwehr, geht jedoch auch mit dem Auflaufen großer Datenmengen einher, die wiederum von Spezialisten analysiert und in Reaktionen umgesetzt werden müssen.

In Zeiten technologisch hochgerüsteter Cyber-Attacken ist es wichtiger denn je, zum frühestmöglichen Zeitpunkt zu entdecken, dass im Netzwerk eine nicht berechtigte Person ihr Unwesen treibt. Allerdings liegt genau hier auch das Hauptproblem für Security-Verantwortliche: Kaum eine Gemeinde oder Verwaltung, egal welcher Größe, ist in er Lage, das entsprechende IT-Security-Personal vorzuhalten, um die nach aktueller NIS-2-Richtlinie nötige kontinuierliche Überwachung des Netzwerks zu gewährleisten.

Genau hier kommen Cyber-Security-Services wie Managed Detection and Response (MDR) zu Einsatz. Diese externen Experten können bestehende Lücken ausfüllen – rund um die Uhr. Dabei haben Services wie z. B. Sophos MDR noch einen anderen, entscheidenden Vorteil gegenüber den traditionellen Security Operation Centern (SOCs). Diese SOC-Teams haben typischerweise den Überblick über das eigene IT-Ökosystem, weitere Daten fließen oft gar nicht oder nur beschränkt in die Analyse ein. Die Sophos Threat Hunter können hingegen auf die Daten von über 100 Millionen Anwendern weltweit zurückgreifen – ein entscheidender Vorteil bei der frühzeitigen Erkennung von Angriffswellen und der Einleitung von Gegenmaßnehmen schon bevor die eigentliche Attacke erfolgt. Die Sophos-Services helfen als offiziell vom BSI qualifizierter APT-Response-Dienstleister (Advanced Persistent Threat) für KRITIS dabei, Security-Maßnahmen gemäß den gesetzlichen Anforderungen rechtzeitig anzupassen und notwendige Aktivitäten einzuplanen.

Sophos MDR ist dabei zudem als bislang einziges Produkt in der Lage, in großem Umfang Sicherheitstelemetrie von externen Anbietern automatisch zu konsolidieren, zu korrelieren und mit Erkenntnissen aus dem Sophos „Adaptive Cybersecurity Ecosystem“ und der Sophos „X-Ops Threat Intelligence Unit“ zu priorisieren.

Auf diese Weise individuell zurechtgeschnittene Cyber-Security as a Service, in Kombination mit einer zentral gesteuerten sowie sich ständig weiterentwickelnden Technologie, sorgt langfristig für Sicherheit. Eine entscheidende Investition in die Zukunft, waren laut einer Sophos-Umfrage („State of Ransomware Report 2023“) unter 3.000 IT-Verantwortlichen doch 69 % der befragten Organisationen aus dem Bereich „Public Sector“ im letzten Jahr von einer Ransomware-Attacke betroffen.

Die starren Strukturen aufbrechen und zusammenarbeiten

Die Zahl der Cyber-Angriffe in Deutschland nimmt stetig zu. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bewertet in seinem Jahresbericht 2022 die Gefährdungslage im Cyber-Raum als „so hoch wie nie".

Alexander Handschuh, Deutscher Städte- und Gemeindebund

Nach Schätzungen des Digitalverbandes Bitkom entstehen durch derartige Attacken massive finanzielle Schäden in Deutschland, die in Summe deutlich über 200 Milliarden Euro pro Jahr betragen. Während lange Zeit vor allem Unternehmen im Fokus von Cyber-Attacken standen, rücken nun zunehmend auch Kommunen ins Visier der Angreifer.

Die Liste der bekannt gewordenen Attacken auf Städte, Gemeinden oder Landkreise in den vergangenen Monaten ist lang. Am meisten Aufmerksamkeit erregte in den vergangenen zwei Jahren wohl der Angriff auf den Landkreis Anhalt-Bitterfeld im Juli 2021, der über lange Zeit gravierende Auswirkungen hatte. Mehrere Server des Landkreises waren mit Ransomware infiziert, der Landrat weigerte sich vollkommen zu Recht, das geforderte Lösegeld zur Datenfreigabe zu zahlen. Aufgrund der massiven Einschränkungen der Arbeitsfähigkeit der Verwaltung musste der Katastrophenfall ausgerufen werden, der mehr als sechs Monate andauerte. Bis zur vollständigen Wiederherstellung aller Systeme dauerte es über ein Jahr, es entstand ein Schaden in Millionenhöhe.

In den Jahren 2021 und 2022 registrierte allein das BKA mehr als 20 Angriffe auf Kommunalverwaltungen und öffentliche Unternehmen, unter anderem im Rhein-Pfalz-Kreis, in der Region um Schwerin und auf mehrere Verwaltungen in kleineren Gemeinden. Auch im Jahr 2023 reißt die Serie der Angriffe nicht ab. Unter anderem waren über den Jahreswechsel Potsdam und im Frühjahr das hessische Rodgau betroffen.

Insgesamt ist davon auszugehen, dass bei steigender Zahl der Angriffe mehr Kommunen ins Visier der Angreifer geraten, auch wenn sie nicht explizit ins Zentrum der verbrecherischen Interessen rücken. Klar ist, dass sich der öffentliche Sektor insgesamt, aber auch die kommunale Ebene, besser gegen derartige Angriffe wappnen müssen. Handlungsfelder sind zum einen die Prävention von Angriffen, zum anderen die verbesserte Reaktionsfähigkeit im Schadensfall.

Nur als Gemeinschaftsausgabe zu lösen

Die Verbesserung der Cyber-Sicherheit und die Stärkung der Resilienz gegen derartige Vorfälle ist eine Gemeinschaftsaufgabe. Dabei geht es nicht nur um eine enge Zusammenarbeit zwischen Bund, Ländern und Kommunen. Wichtig ist auch ein enger Austausch mit dem BSI, den Sicherheitsbehörden wie etwa dem Bundeskriminalamt (BKA) sowie den entsprechenden Einrichtungen auf Ebene der Länder. Außerdem ist auch eine konstruktive Zusammenarbeit mit den privaten IT-Konzernen, wie Google oder Microsoft, nicht

nur sinnvoll, sondern sogar eine zwingende Voraussetzung, um bestmöglich gegen Attacken gewappnet zu sein. Vielfach verfügen diese Unternehmen über einen deutlich besseren Überblick über die Gefahrenlage und können dabei helfen, Schadensfälle zu verhindern.

Bei der Zusammenarbeit zwischen den föderalen Ebenen ist es dringend notwendig, die vielfach zu starren Strukturen aufzubrechen, um flexibel und schnell auf Zwischenfälle reagieren zu können. Daher ist es sinnvoll, die Kompetenzen des BSI zu stärken und es der Bundesbehörde zu ermöglichen, im Ernstfall auch vor Ort, etwa in den Kommunen, unterstützen zu können. Zusätzlich ist eine engere und noch bessere Kooperation zwischen den Städten und Gemeinden und den jeweiligen Bundesländern wichtig. Teilweise haben einzelne Bundesländer hier bereits entsprechende Unterstützungsstrukturen geschaffen und CERTs oder MIRTs aufgebaut, die im Krisenfall auch in den Kommunen eingesetzt werden können.

Auch die Städte und Gemeinden sind noch mehr als bisher gefordert, sich gerade im Bereich der Prävention noch besser aufzustellen. Dabei stellt der Aufbau einer Basisabsicherung und des IT-Grundschutzes vielfach derzeit aber noch eine Herausforderung dar, da es vor allem an personellen und finanziellen Ressourcen mangelt. Vor diesem Hintergrund sind gemeinsame Kampagnen, wie beispielsweise das vom BSI und den kommunalen Spitzenverbänden gestartete Modellprojekt „Wege in die Basisabsicherung“, von hohem Wert. Eine wertvolle Hilfe für Kommunalverwaltungen sind auch die vom BSI und einigen Landesbehörden bereitgestellten Informationsmaterialen oder Checklisten. In einem kontinuierlichen Prozess und in Zusammenarbeit mit Bund und Ländern, aber auch mit anderen Kommunen kann es gelingen, das Schutzniveau in den Verwaltungen sukzessive zu verbessern.

Erfolg nicht per Gesetz erreichbar

Umgekehrt wird es nicht funktionieren, Cyber-Sicherheit per Gesetz oder Verordnung bis in die kleinste Kommune zu bringen. Ein solcher Ansatz wird immer wieder diskutiert und hat durch die nun anstehende Umsetzung der sogenannten „NIS-2“-Richtlinie der EU in nationales Recht neue Relevanz bekommen. Hier steht zur Diskussion, ob neben den nationalen und regionalen auch die kommunalen Verwaltungen als Kritische Infrastrukturen eingestuft werden sollen. Dass es sich um wichtige und im Sinne der allgemeinen Definition auch tatsächlich Kritische Infrastrukturen handelt, steht außer Frage. Klar ist aber auch, dass mit einer solchen gesetzlichen Festschreibung keine Fortschritte erzielt, sondern im Gegenteil die bisherigen Schritte Richtung besserer Zusammenarbeit gefährdet würden. Auch wenn die Verantwortung der Kommunen gesetzlich festgeschrieben wird, stehen weder mehr Finanzmittel noch mehr Personal zur Verfügung.

> *Wir müssen – gerade im Bereich von Schutz vor Cyber-Angriffen – das althergebrachte Denken in Silos überwinden und zu einem gemeinsamen Lösungsansatz kommen.*

Wir müssen – gerade im Bereich von Schutz vor Cyber-Angriffen – das althergebrachte Denken in Silos überwinden und zu einem gemeinsamen Lösungsansatz kommen. Dieser Lösungsansatz muss sich ohne Zweifel an klaren Standards und Prinzipien wie „Zero Trust“ orientieren. Was sicher nicht hilft, ist das Beharren auf Zuständigkeiten und die Delegation von Verantwortlichkeiten. Cyber-Sicherheit ist Gemeinschaftsaufgabe und kann nur gelingen, wenn sich alle föderalen Ebenen und der privatwirtschaftliche Sektor auf der „hellen Seite“ gegenseitig im Kampf gegen die zunehmenden Bedrohungen durch die „dunkle Seite“ unterstützen.

Dr. Alexander Handschuh ist Sprecher des Deutschen Städte- und Gemeindebunds (DStGB). Neben politischen Grundsatzfragen beschäftigt er sich mit Grundsatzfragen der Digitalisierung und neuen Medien.

Foto: Bernhard Link, Farbtonwerk

Die Nationale Sicherheitsstrategie Deutschlands – zwischen Anspruch und Wirklichkeit

Erstmals in der Geschichte Deutschlands hat das Bundeskabinett eine nationale Sicherheitsstrategie verabschiedet. Das Dokument soll Antworten auf die internationalen Machtverschiebungen und systemischen Rivalitäten mit Blick auf den Schutz unserer Demokratie und die damit verbundene freiheitlich-demokratische Grundordnung geben.

Stephan Ursuleac, Bitkom e. V.

Ziel der Nationalen Sicherheitsstrategie ist eine umfassende Betrachtung von Sicherheit, u. a. für die Bereiche Verteidigung, Außenpolitik und Entwicklungszusammenarbeit (mit Fokus auf eine feministische Außenpolitik), Innere Sicherheit, Wirtschaftsschutz, Cyber-Sicherheit, Weltraum, Schutz Kritischer Infrastrukturen, Energie- und Rohstoffsicherheit, neue Technologien, Bildung, Ernährungssicherheit und Nachhaltigkeit, Lieferketten u. v. m. Das Ziel ist, dass Deutschland auch zukünftig wehrhaft, resilient und nachhaltig in Frieden, Freiheit und Sicherheit leben kann.

Strategie oder Absichtsbekundungen?

Die Strategie bleibt hinter den Erwartungen zurück und offenbart das Mindestmaß an Konsens in der Koalition. Klare Prioritäten und Lösungen sind kaum erkennbar. Eine Strategie legt Handlungsziele und daraus abgeleitete Maßnahmen fest (Wer macht was, wann, wozu, wo?). Dazu ist eine Ist-Analyse der gegenwärtigen Situation in den verschiedenen Bereichen Wirtschaft, Hard- und Softpower, Ressourcen (inkl. Daten), Technologie, Bevölkerung, Politik und Geografie vorzunehmen. Unter Einbeziehung aller relevanten Stakeholder (u. a. Wirtschaft, Gesellschaft, Bundesländer, Bundestag, Wissenschaft usw.) können dann Handlungsoptionen, Maßnahmen etc. abgeleitet werden. Das Einbeziehen der Stakeholder erfolgte jedoch nur rudimentär. Die Folgen sind allgemeine Absichtsbekundungen. So ist u. a. unklar, wie immer neue Behördenkompetenzen oder Personalressourcen vor dem Hintergrund des demografischen Wandels oder die Sicherstellung des Zugangs zu neuen Technologien gewährleistet werden sollen bzw. wie Deutschland aufgrund der wirtschaftlichen und politischen Verschiebungen zukünftig noch Einfluss ausüben kann.

Ressortübergreifender Ansatz geht nicht ohne übergreifende Koordinierung

Eine angedachte ressort- und themenübergreifende Sicherheitspolitik benötigt ein Gremium im Bundeskanzleramt, welches eine systematische Linie koordiniert. Die Absage eines Nationalen Sicherheitsrates ist daher bedauerlich. Ge-

rade durch die Verzahnung der Innen- und Außenpolitik in mehreren Bereichen kann eine solche Koordinierung nicht nur in einem Ressort liegen.

Digitale Souveränität macht resilient, wehrhaft und nachhaltig

Deutschland befindet sich in einer angespannten Lage. Die exportstarke deutsche Wirtschaft hängt in hohem Maße von stabilen Verhältnissen auf globaler Ebene ab und braucht gleichermaßen Zugang zu günstiger Energie und Rohstoffen wie auch zu ihren Kundinnen und Kunden. Das alles steht derzeit auf dem Spiel. Hinzu kommen folgende Besonderheiten: die digitale Transformation, mit Konsequenzen in Wirtschaft, Technologie, Politik und Ressourcen sowie Hard- und Softpower und der demografische Wandel. Gerade die Digitalisierung braucht kluge, digital kompetente Köpfe. Genau die aber fehlen: 137.000 Stellen für IT-Fachkräfte sind derzeit in Deutschland unbesetzt und in vielen Fällen auch nicht zu besetzen.

Um den Wohlstand in Deutschland zu sichern, bedarf es der Fähigkeit, innovative Lösungen zu entwickeln und eines ungestörten Zugangs zu relevanten Schlüsseltechnologien. Dies erfordert eine digitale Sicherheitspolitik mit dem Ziel der digitalen Souveränität.

Digitale Souveränität gestalten

Digitale Souveränität ist die Möglichkeit zur digitalen Handlungs- und Gestaltungsfreiheit. Deutschland muss auf Augenhöhe Schlüsseltechnologien, Geschäftsmodelle und Ökosysteme in der Prägung internationaler Standards mitgestalten, sowohl durch Forschung als auch durch Entwicklung.

Global verteilte Liefer- und Wertschöpfungsketten sind kreativ und intelligent durch Risikoabschätzungen zu nutzen und gegebenenfalls zu formen. Gleichzeitig sollten sie in der Lage sein, Technologien und Dienstleistungen von vertrauenswürdigen nationalen und internationalen Partnern erwerben zu können. Gerade durch diese komplementäre Stärke der Wirtschaftsräume können Innovations- und Effizienzgewinne entstehen, wenn die grenzüberschreitende Zusammenarbeit auf Augenhöhe und regelbasiert stattfindet. Um dies sicherzustellen, braucht es eine Initiative der Bundesregierung und der EU-Kommission zur fortlaufenden Bewertung der digitalen Souveränität. Dabei müssen unterschiedlichste Perspektiven, z. B. in der Form eines „Multi-Stakeholder-Observatoriums“, eingebunden werden. Nur so können Lücken identifiziert und gezielt geschlossen werden.

Deutschland und Europa müssen zum Erhalt ihrer digitalen Souveränität sicherstellen, dass Schlüsseltechnologien nicht aus Europa abwandern. Es bedarf eines wirksamen digitalen Binnenmarktes, der intensiv politisch und regulativ vorangetrieben wird, um die europäische Nachfrage nach Schlüsseltechnologien zu aggregieren. Dies beinhaltet im Zuge der Zeitenwende auch einen NATO-Binnenmarkt ohne restriktive Exportbeschränkungen.

Auch ist eine strategische Abstimmung der Aspekte Industrie, Rohstoffe, Handel und Bildung in die Sicherheitspolitik einzubetten. Zusätzlich sollten die sicherheitspolitische Lage und deren Auswirkungen auf Lieferketten und die Abhängigkeiten Deutschlands (u. a. Taiwan-Frage) sowie die Verschiebung internationaler Machtkonstellationen berücksichtigt werden. Dazu zählen der Wiederaufstieg Chinas sowie das Interagieren mit Staaten wie Brasilien, Indien, der Region Afrika oder dem postsowjetischen Raum. Diese Regionen verfügen über massive Rohstoffvorkommen und Absatzmärkte und orientieren sich teilweise noch an der Europäischen Union (EU). Dies erfordert sowohl eine engere, zentrale Koordination der Ministerien, u. a. des Auswärtigen Amtes, des Bundesministeriums des Innern und für Heimat, des Bundesministeriums der Verteidigung und des Bundesministeriums für Wirtschaft und Klimaschutz, als auch eine stärkere politische Initiative durch den Bundestag.

Insbesondere sollte der Blick in Richtung einer nationalen Cyber-Sicherheitsstrategie unter Berücksichtigung einer europäischen Gesetzgebung fokussiert werden. Diese garantiert die Grundlagen einer funktionierenden Wirtschaft und Gesellschaft. Zu begrüßen ist die Erkenntnis, dass der Weltraum eine Kritische Infrastruktur darstellt, ohne die das Funktionieren der Gesellschaft kaum mehr möglich ist. Um dieses Thema zu koordinieren, bedarf es eines oder einer Weltraumbeauftragten im Bundeskanzleramt. Diese Stelle muss, ähnlich wie in Frankreich und Großbritannien, die weitere Koordination des Themas – u. a. bei einem einheitlichen Weltraum-Sicherheitslagebild oder der Koordination von ressortübergreifenden Projekten (z. B. zu Themen wie Kollisionsvermeidung und Integrität von Weltraumlagedaten usw.) – sicherstellen. Dies ist durch ein gleichberechtigtes Ökosystem aus Staat, Wirtschaft und Wissenschaft zu begleiten.

Schließlich müssen ein geostrategisches Mindset sowie eine strategische Denkschule, die Themen länger als eine Legislaturperiode betrachtet, geschaffen werden.

Die Bundesregierung muss nun liefern, mit spezifischen Zeitlinien, Forderungen und Maßnahmen, wobei der Bitkom sich gerne einbringt.

Stephan Ursuleac ist Bereichsleiter Verteidigung & öffentliche Sicherheit beim Digitalbranchenverband Bitkom.

Foto: Bitkom

Zero Trust: die nächste Generation der Sicherheitsarchitektur

Beim Thema Digitalisierung denken die meisten an die positiven Effekte – die Flexibilität von Cloud Services und die Vereinfachung komplizierter Verfahren. Die Möglichkeiten von IT sind gewaltig. Genau diese Möglichkeiten lassen sich aber auch missbrauchen, um unseren Staat und unsere Unternehmen digital anzugreifen. Um diesen Bedrohungen standzuhalten, muss die Cyber Security parallel zur Digitalisierung weiterentwickelt werden: Ein wesentliches Konzept dabei ist „Zero Trust".

Andreas Ritschel und Hendrik Vagts, BWI GmbH

Ob Identitätsdiebstahl bei Bürgerinnen und Bürgern oder die Erpressung von Unternehmen und Behörden mit Krypto-Trojanern und exfiltrierten Daten: Die Frequenz von erfolgreichen Cyber-Angriffen steigt kontinuierlich an und richtet in den westlichen Volkswirtschaften inakzeptable Schäden an. Staatsnahe und staatliche Angreifergruppen haben sich in den letzten zehn Jahren zunehmend professionalisiert und eigene Schatten-IT-Ökosysteme mit Arbeitsteilung und eigener Software-Entwicklung aufgebaut.

Sicherheitsherausforderungen der neuen Zeit

In Zukunft werden wir dabei auch mehr und mehr die Nutzung von generativer Künstlicher Intelligenz (KI) sehen, die solchen Angriffskampagnen eine völlig neue Dimension geben wird. Dadurch wird es für die Benutzer immer schwerer, professionelle Angriffe wie z. B. Spear Phishing zu erkennen. Zusätzlich zu den steigenden Fähigkeiten von Angreifern stehen Sicherheitsorganisationen heute vor Herausforderungen, die sich aus einer veränderten IT- und Arbeitswelt ergeben:

- Endpoints bis hin zu verschiedenen Plattformen, die sowohl klassische Geräte als auch Industriesteuerungsanlangen umfassen, müssen abgesichert werden.
- Innerhalb der Sicherheitsorganisation werden die anfallenden Aufgaben immer zahlreicher und gleichzeitig sind Security-Lösungen in vielen Fällen Silos, die überwiegend über organisatorische Prozesse miteinander in Verbindung stehen.
- Hersteller von IT-Lösungen bieten ihre Produkte vermehrt nicht mehr oder nur noch eingeschränkt on-premise an. Wesentliche Funktionen sind oftmals nur über die Public Cloud nutzbar, was für staatliche Organisationen, die auch den Geheimschutz beachten müssen, schwierig ist.
- Security-Spezialisten einzustellen, um Teams zu vergrößern oder Fluktuationen auszugleichen, ist aufgrund eines gravierenden Fachkräftemangels zu einem ernsthaften Problem geworden.

Als Antwort auf diese herausfordernde Situation müssen Sicherheitsarchitekturen so weiterentwickelt werden, dass sie Silos abbauen, einen hohen Automatisierungsgrad zulassen und den Schutz der Daten selbst ins Zentrum stellen. Alle

Aktivitäten und Zugriffe im Netzwerk müssen als potenziell unsicher betrachtet werden. Es darf nicht nur das Ziel verfolgt werden, Sicherheitsverletzungen zu verhindern, sondern es muss gleichzeitig das Schadenspotenzial bei einer erfolgreichen Kompromittierung so weit wie möglich eingedämmt werden. Genau das ist die Idee hinter Zero Tust.

Null Vertrauen zu niemandem

Zero Trust verfolgt das Grundprinzip, dass einer handelnden Person oder einem IT-System Vertrauen niemals implizit gewährt wird, sondern dass dieses Vertrauen kontext- und zustandsorientiert erarbeitet und ständig überprüft werden muss. Eine Zero-Trust-Architektur arbeitet mit einem „End-to-End"-Ansatz und bedient sich aus einer Vielzahl von integrierten Datenquellen wie Identitäten, Zustandsdaten der Endpunkte, Lokalitäten, Datenklassifizierungen, gültigen Anwendungsszenarien und historischen Daten, um dynamisch und hochautomatisiert Entscheidungen über Art und Umfang der Datennutzung treffen zu können.

Bei derzeitigen Sicherheitsarchitekturen liegt der Fokus auf dem „Grenzschutz" einzelner Zonen, z. B. der Intranet-Zone oder der Rechenzentrumszone als Ganzes, die Benutzer einmal an der Perimetergrenze authentifiziert. Eine Authentifizierung und Autorisierung an einzelnen Ressourcen innerhalb der Zone erfolgt erst an der Ressource selber. Somit besteht eine überproportional große Angriffsfläche innerhalb einer Zone, was die Risiken von Lateralbewegungen bei erfolgreichen Angriffen massiv steigert.

Eine Zero-Trust-Architektur setzt dem die permanente Auswertung aller Zugriffsanforderungen gemäß dynamischer Regeln entgegen. Durch die Auswertung von Zustandsinformationen kann festgestellt werden, ob ein Zugriff zulässig ist und gewährt werden kann, bevor der Handelnde mit der eigentlichen Ressource kommuniziert. Dadurch, dass nur zulässige Kommunikationsanfragen eine Ressource erreichen können, wird die Angriffsfläche reduziert.

Zero Trust ist dabei für IT-Sicherheitsspezialisten als Idee nicht neu, aber durch die aktuellen Entwicklungen der IT-Sicherheitsprodukte und Cloud-Technologien endlich an der Schwelle zur skalierbaren Umsetzbarkeit.

Implementieren mit offenen Schnittstellen

Die Umsetzung von Zero Trust ist jedoch aufwendig, auf einer technischen wie auf einer organisatorischen Ebene, und erfordert eine hohe Reife von Schlüssel-IT-Fähigkeiten. Zu den wichtigsten Voraussetzungen zählen:

- transparente Inventarisierung aller IT-Assets,
- Bewertung, Klassifikation und Kenntlichmachung von Daten,
- betriebsumgebungsübergreifende, starke Identitäten für Personen und IT-Systeme,
- durchgehende und lückenlose Protokollierung der IT-Landschaft sowie
- Auswertung von Protokollen auf Anomalien

> *Zero Trust ist als Idee nicht neu, aber durch die aktuellen Entwicklungen endlich an der Schwelle zur skalierbaren Umsetzbarkeit.*

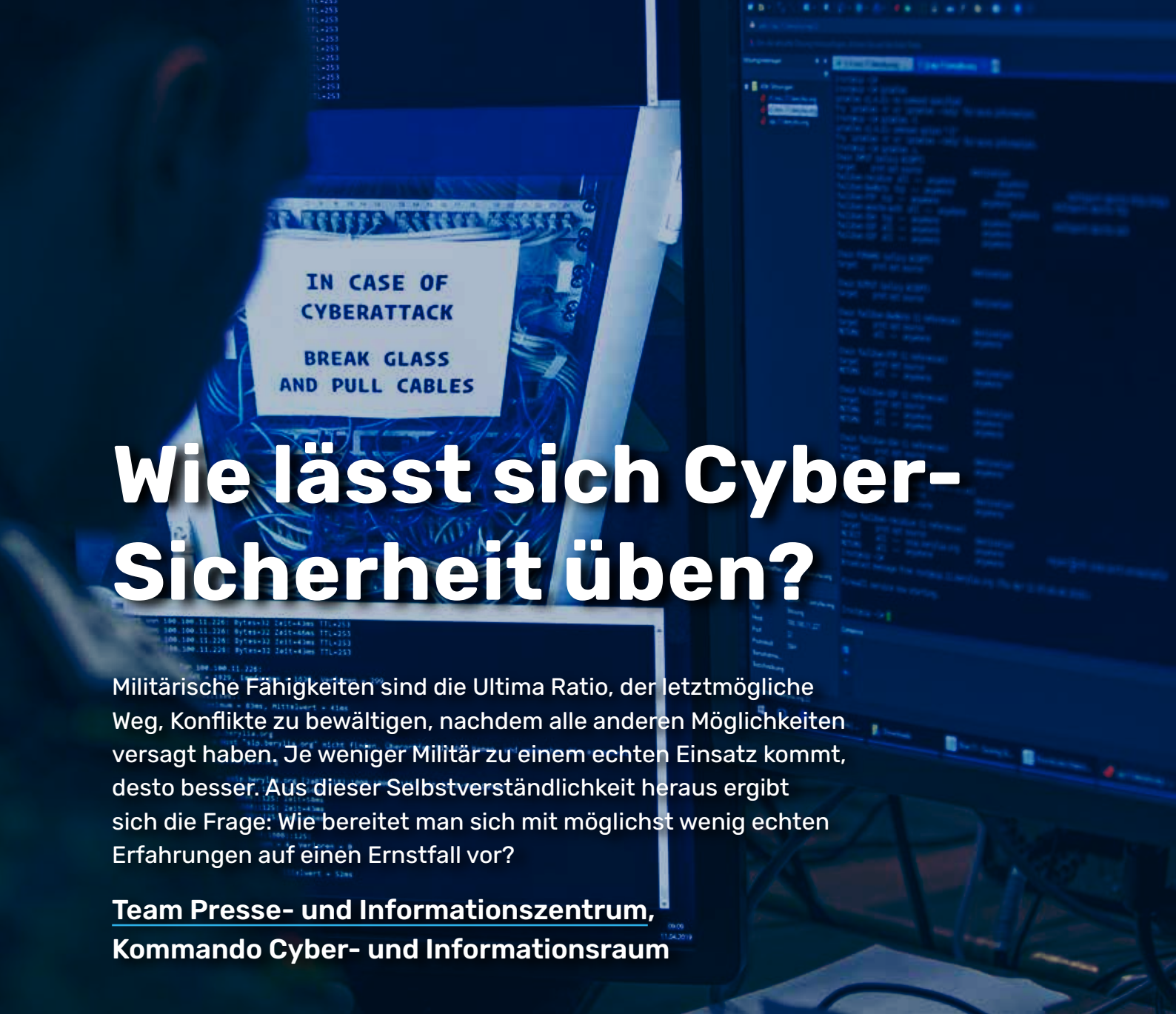
Heute kann man Zero Trust nicht als Lösung kaufen und die Produkte, die angeboten werden und darauf einzahlen, müssen aufwendig integriert werden. Für den Public Sector braucht es daher in der Fläche einen Zero-Trust-Implementierungsstandard und offene Schnittstellen, die über die Ökosysteme der Hersteller hinweg eine gemeinsame Sprache und saubere Performance bieten. Es müssen modulare Lösungen entstehen, die es uns erlauben, Private Clouds dynamisch in Zero-Trust-Architekturen zu integrieren. Ideen und Initiativen dahin gibt es. Jetzt müssen Hersteller, Regulatorik und der Public Sector gemeinsam reife und kompatible Lösungen entwickeln.

Andreas Ritschel ist Cyber-Security-Programmdirektor bei der BWI GmbH.

Foto: BWI/Ritschel

Hendrik Vagts ist Enterprise Lead Architekt bei der BWI GmbH.

Foto: BWI/Vagts



Wie lässt sich Cyber-Sicherheit üben?

Militärische Fähigkeiten sind die Ultima Ratio, der letztmögliche Weg, Konflikte zu bewältigen, nachdem alle anderen Möglichkeiten versagt haben. Je weniger Militär zu einem echten Einsatz kommt, desto besser. Aus dieser Selbstverständlichkeit heraus ergibt sich die Frage: Wie bereitet man sich mit möglichst wenig echten Erfahrungen auf einen Ernstfall vor?

Team Presse- und Informationszentrum, Kommando Cyber- und Informationsraum

Die Antwort ist seit Jahrtausenden dieselbe: Militär exerziert, Militär führt Manöver durch, Militär übt. In allen militärischen Dimensionen muss geübt werden, ob zu Lande, in der Luft, im Weltraum oder zur See. Im Cyber- und Informationsraum (CIR) als eigenständiger militärischer Dimension gehen die Herausforderungen jedoch noch weiter. Im Cyber-Raum haben wir ständig Fühlung mit dem Feind und müssen unsere Fähigkeiten trotzdem weiter erhalten und ausbauen. Das Ziel: auch auf zukünftige Angriffe vorbereitet sein.

Während zivile Organisationen die Cyber-Sicherheit im Fokus haben, besteht für die Dimension CIR zusätzlich der Auftrag zur Verteidigung. Die Unterscheidung ist notwendig, weil für Streitkräfte mindestens zwei deutlich zu unterscheidenden Situationen bestehen: Der Grundbetrieb (Frieden, Cyber-Sicherheit), der im Wesentlichen den Anforderungen im zivilen Bereich entspricht. Daneben ist der Kernauftrag, für die Landes- und Bündnisverteidigung (Cyber-Verteidigung) vorbereitet zu sein.

Besonderheiten der Verteidigung in der Dimension CIR

Im Fall der Verteidigung ergeben sich besondere Herausforderungen, die für Streitkräfte im Vergleich zum zivilen Bereich einzigartig sind. Ortsfeste Liegenschaften mit idealer Anbindung und Infrastruktur bestehen dann nicht mehr. Die zu schützende IT steht auf dem Gefechtsfeld oder räumlich nahe. Daraus ergeben sich Einschränkungen, die zu beachten und ständig zu üben sind.

Übung ist auch in den Streitkräften nicht gleich Übung.

Foto: Bundeswehr/Martina Pump

Cyber-Verteidigung zu trainieren, unterscheidet sich in einigen Punkten deutlich vom klassischen militärischen Manöver, wie man es vom Truppenübungsplatz kennt. Einige der Herausforderungen in der militärischen Dimension CIR sind einzigartig und unterscheiden sich maßgeblich von denen in anderen Dimensionen, auch wenn das Übungswesen das Gleiche ist.

Um zu verstehen, wie Cyber-Verteidigung geübt wird, muss man zunächst betrachten, wie Cyber-Verteidigung funktioniert. Zwei Aspekte sind für den Entwurf eines Übungsszenarios entscheidend: Die verteidigende Truppe ist auch im Grundbetrieb ständig im Einsatz. In der Bundeswehr sind das die Expertinnen und Experten aus dem Zentrum für Cyber-Sicherheit mit Hauptsitz in Euskirchen, aber auch die vielen Fachleute vor Ort überall dort, wo IT betrieben wird. Ein Grundrauschen, ständige Wachsamkeit und regelmäßige, scharfe Einsätze müssen nicht extra geübt werden: Das Fachpersonal ist 24/7 und an 365 Tagen im Jahr im Einsatz. Es bleibt dabei nicht bei der reinen Bedrohungslage. Die Bundeswehr – wie fast alle staatlichen Akteure – ist ein beliebtes Ziel für Angriffe aus anderen Staaten. Diese Angriffe zu erkennen, zu verhindern, einzugrenzen und Schäden zu minimieren, ist Tagesgeschäft des Zentrums für Cyber-Sicherheit der Bundeswehr. Mit dem Nebeneffekt, dass ein Grundniveau an Übung und Expertise ständig vorhanden ist.

Herausfordernder wären großangelegte Cyber-Attacken, bis hin zu solchen, die man als kriegerischen Akt verstehen mag. Die Bundeswehr agiert auf diese Angriffe in der Verfahrensweise ähnlich zu zivilen Organisationen: Mit der Entsendung eines Incident Response Teams (IRT) kann flexibel und vor Ort auf die Attacke reagiert werden. Wie groß dieses Team ist und welche Fähigkeiten es mitbringt? Das ist jeweils angepasst an Auftrag und Lage.

Hier lässt sich die Brücke zur Übung bauen. In einem flexibel aufgestellten IRT zu arbeiten, vielleicht mit Expertinnen, die man bis dato nicht kannte? Das lässt sich üben. Ortsfremd – sowohl in der physischen Welt als auch in völlig unbekannten virtuellen Systemen – zu arbeiten und diese zu verteidigen? Das lässt sich üben. Innerhalb weniger Stunden einsatzbereit sein und in eine bereits eskalierende Lage geworfen werden? Das lässt sich ebenfalls üben. Und zu guter Letzt: Innerhalb von Stunden – und gegebenenfalls für Tage bis Wochen – dieselbe Quantität und Qualität von Attacken bekämpfen, die sich sonst vielleicht über Jahre strecken? Auch das lässt sich üben.

Flexibilität als Grundvoraussetzung

In der Welt der Cyber-Sicherheit spricht man von „Blue Teams“, wenn es um die Defensive geht. Diese Terminologie kann sich auf Übungen beziehen, der Begriff findet aber auch genauso in der Realität und außerhalb militärischer Wirklichkeit Anwendung. Kein größeres IT-Unternehmen kommt im 21. Jahrhundert ohne ein Blue Team aus. Das militärische Blue Team muss aber über die eigenen IT-Systeme hinaus handlungsfähig bleiben. Dabei können sich spontan aus anderen Bereichen Bedrohungen ergeben, auf die flexibel reagiert werden muss, um eine erfolgreiche Verteidigung sicherzustellen.

Es wird Seite an Seite mit anderen Behörden geübt, beispielsweise dem BSI, aber auch mit zivilen Partnern aus Wissenschaft und Wirtschaft.

Foto: Bundeswehr/Martina Pump

Eigene Führungsfähigkeit absichern

Wie angeführt, ergeben sich im militärischen Bereich besondere Herausforderungen, die gesondert geübt werden müssen. Auf nationaler Ebene werden diese in der Bereichsübung „Gelber Merkur“ geübt. Nicht nur alle Fähigkeiten aus der Dimension CIR sind hier beteiligt, auch die anderen militärischen Dimensionen nehmen regelmäßig daran teil, sodass die Zusammenarbeit als militärisches Blue Team geübt wird.

Ein Teil eines solchen Blue Teams kann ein militärisches IRT sein, wie es in zivilen Organisationen auch eingesetzt wird. Der präventive Anspruch liegt aber deutlich höher. Während im Zivilen Produktions- und Verwaltungsprozesse in der IT abgebildet sind, muss die IT für Streitkräfte auch das Führen und Wirken zur Auftragserfüllung sicherstellen. Somit ist die

wesentliche Leistung, eine Einschränkung oder gar einen Ausfall von IT-Systemen und Fähigkeiten in den Gefechtsständen durch „Cyber Capability Protection Teams“ nur so weit zuzulassen, dass der Auftrag der Bundeswehr weiterhin erfolgreich durchgeführt werden kann. Dafür werden die Fähigkeiten Sensorik, Schwachstellenanalyse, Penetrationstest und Netzwerküberwachung zwingend benötigt.

Einsatz in nationalen Systemen

Der Lage angepasst, werden diese durch weitere Kräfte ergänzt. Kräfte, die vorher nicht bekannt sind, nicht zwangsläufig Angehörige der Streitkräfte sind und die erst in Prozesse integriert werden müssen. Die Bundeswehr übt dies dadurch, dass Blue Teams bei ihren Übungen fast immer gemischt sind. Es wird geübt, Seite an Seite mit anderen Behörden wie beispielsweise den Polizeidienststellen, aber auch mit zivilen Partnern aus Wissenschaft und Wirtschaft. Das Wissen um Cyber-Sicherheit wird so breit in die Gesellschaft getragen, was deren grundsätzliche Resilienz stärkt. Gleichzeitig lernen Führungskräfte der Bundeswehr den Umgang mit externen Fachleuten und deren Integration ins Team kennen und die Arbeitsebene(n) können sich gegenseitig im konkreten „Doing“ auf Stand bringen. Eine Win-win-Situation, geboren aus der Absicht, möglichst realitätsnah zu trainieren.

Einsatz in fremden Systemen

Wie sich Konflikt- und Kriegsszenarien entwickeln, ist schwer vorherzusehen. Wo welcher Angriff stattfinden wird und welches System im Konfliktfall geschützt werden muss, ist vielseitig. Für eine Armee im Krieg ist der Schutz eines Staudamms vielleicht genauso relevant wie der der eigenen Kommunikationskanäle – das hat spätestens die Sprengung des Kachowka-Staudamms in der Ukraine gezeigt. Nur wird der nächste Staudamm vielleicht mit einer Cyber-Attacke angegriffen. Erschwerend kommt hinzu: Die Bundeswehr denkt Landes- und Bündnisverteidigung im 21. Jahrhundert zusammen, der fiktive Staudamm als Platzhalter für beliebige Angriffsziele muss kein Ziel in Deutschland sein.
Für Übungsszenarien der Bundeswehr ist die Konsequenz klar: maximale Flexibilität und Vielseitigkeit in der Lage. Während der jährlich von der NATO ausgerichteten Übung zur Cyber-Verteidigung „Locked Shields“ wird das konsequent umgesetzt: fremde Systeme eines fiktiven Staates mit in jedem Jahr wechselnden Details. 2022 war ein ziviles Satellitensystem Teil der Lage, 2023 komplex vernetzte Flugabwehr. Die „Cyber Capability Protection Teams“ müssen abstrakt üben. Es kommt auf Verfahren und das grundsätzliche technische Know-how an, weniger auf Erfahrungen mit bestimmten Anlagen. Solche Erfahrungen helfen, können aber keine Voraussetzung sein. In der Erstellung von Übungsszenarien wird das berücksichtigt, indem beispielsweise Expertinnen und Experten für ein System dabei unterstützen. Wie in der Realität auch, würde sich ein „Cyber Capability Protection Team“ dabei regelmäßig auf ortskundiges Personal abstützen. Um erfolgreich zu sein, müssen die Fachleute vor Ort (Administratoren) mit den Experten für Cyber-Sicherheit schnell und effektiv zusammenarbeiten können. Dann bildet sich ein wirksames Blue Team.

Maximale Intensität für maximale Ergebnisse

Ein wichtiger Bestandteil jeder militärischen Übung ist die erhöhte Intensität. Innerhalb kürzester Zeit muss ein Vielfaches der üblichen Attacken abgewehrt werden. Übungen wie Locked Shields oder die britische Übung „Defence Cyber Marvel“, an der die Bundeswehr teilnimmt, sind bewusst so angelegt, dass nicht alle Angriffe verhindert oder komplett abgewehrt werden können. Konkret bedeutet das zum Beispiel gezielte Angriffe auf bekannte Schwachstellen, davon vielleicht mehrere gleichzeitig. Die Verteidigerinnen und Verteidiger müssen priorisieren und gegebenenfalls mitigieren, also die Folgen durch erfolgreiche Angriffe abmildern und eindämmen. Das gehört genauso zum Job der „Cyber Capability Protection Teams“ dazu wie das Härten der Systeme, um bereits bekannte Schwachstellen zu stärken und so bekannte Angriffe zu verhindern oder zumindest ihre Auswirkung zu minimieren.

Red Teams verfolgen ihr Ziel genauso intensiv, wie sie es in einem realen Szenario tun würden. *Foto: Bundeswehr/Stefan Uj*

Um diese Intensität zu erreichen, stützt sich das Übungswesen der Bundeswehr auf zwei Faktoren ab. Zum einen: Geübt wird mit realistischen Gegnern, den „Red Teams“. Es handelt sich dabei um Cyber-Operateure, die ihren eigent-

lichen Auftrag – in feindliche Systeme eindringen und dort einen Auftrag erfüllen – hier ausführen. Sie agieren dabei so, wie sie auch in Wirklichkeit agieren würden. Das beinhaltet unter anderem Scheinangriffe, parallele Angriffe, um Verteidiger zu überfordern, koordiniertes Vorgehen und Wechsel der Vorgehensweise. Red Teams sind meist nur wenigen Übungskünstlichkeiten unterworfen. Sie verfolgen ihr Ziel genauso intensiv, wie sie es in einem realen Szenario tun würden: Damit sind sie der perfekte Sparringspartner und um ein Vielfaches realistischer als gekünstelte Übungsfälle. Es geht in einer Übung zur Cyber-Verteidigung eben nicht darum, Rätsel zu lösen oder knifflige Programmieraufgaben zu stemmen, sondern darum, sich ein digitales Gefecht (mit echten Menschen) zu liefern und dieses Gefecht für sich zu entscheiden.

Cyber Range – der virtuelle Übungsplatz

Cyber Range des Forschungsinstitutes CODE in München, die auch bei der Cyber Coalition, eine der größten Cyber-Abwehr-Übungen der NATO, eingesetzt wird. *Foto: Bundeswehr/ Maximilian Maiwald*

Der andere Faktor, der das Katz-und-Maus-Spiel zwischen Blue und Red Teams erst möglich macht, ist eine Infrastruktur, die die Realität virtuell kopiert und ein realitätsgetreues Üben ermöglicht. Grundlage dieser Infrastruktur ist Virtualisierung, also das Darstellen von Anlagen, die physisch nicht existieren. Beliebige Systeme, wie zum Beispiel die Anlagen des bereits erwähnten Staudamms, werden virtuell nachgebildet und so potenzielle Ziele. Sogenannte Cyber Ranges ermöglichen zudem den Live-Fire-Betrieb der Beteiligten an einem zentralen Ort, da sie Raum und Material bieten. Innerhalb des Systems sind diese künstlichen Systeme maximal realitätsgetreu und schaffen damit einen Rahmen, den man sich wie einen virtuellen Übungsplatz vorstellen kann. Zu Cyber Ranges, wie sie beispielsweise vom Forschungsinstitut CODE an der Universität der Bundeswehr in München angeboten werden, gehört auch eine Infrastruktur, die die Auswertung und die Steuerung der Szenarien durch Trainer ermöglicht. Diese „White Team“ genannte Übungsleitung kann so externe Faktoren nachbilden, die zusätzlich zu den virtuellen Gefechten zwischen Red und Blue Teams das Stresslevel und den Realitätsgrad erhöhen. Ein weiterer Vorteil: Weitere Teilnehmer können zusätzlich remote an der Übung teilnehmen, es gibt also keinen Nachteil zu disloziert stattfindenden Live Fire Exercises. Bei internationalen Übungen mit gemischten Teams können diese sich von ihren jeweiligen Standorten aus verbinden und das Red Team bleibt die unbekannte und meistens anonyme Gefahr aus dem Netz.

„Train as you fight“

Militärische Cyber-Verteidigungsübungen unterscheiden sich in den Details also maßgeblich von anderen militärischen Übungen. Die abstrakten Grundzüge und Prinzipien sind jedoch dieselben. „Train as you fight“ ist ein geflügeltes Wort in der Bundeswehr. Die Bundeswehr bereitet sich auf vielfältige Einsatzszenarien der Cyber-Verteidigung vor: sowohl mit der konsequenten Ausrichtung an realen Bedrohungen als auch dem Willen – wie im realen Einsatz – auch externe Expertinnen und Experten einzubeziehen sowie mittels Übungsszenarien mit realistisch agierenden Red Teams. Denn nur so kann die Bundeswehr ihre Aufgaben in der Gegenwart meistern und in der Zukunft das verteidigen, was schützenswert ist.

SVA

CYBER SECURITY IST FESTER BESTANDTEIL ALL DESSEN, WAS WIR TUN.

Wir betrachten Cyber Security nicht als ein notwendiges Übel zur Risikominimierung und Erfüllung von Compliance-Vorgaben, sondern als einen wichtigen Baustein zur Erreichung von Unternehmens- und Behördenzielen – Cyber Security macht Digitalisierung möglich.

Hierzu zählen:
- Beratung zur Cybersicherheit
- BSI-Grundschutz und Auditierung
- Architektur und Integration
- Penetration Testing
- Aufbau & Betrieb sicherer Infrastrukturen
- Sensibilisierungsmaßnahmen

Sie möchten mehr über digitale Sicherheit erfahren?

//www.sva.de

Cyber-Sicherheit geht alle an – ressortübergreifende Zusammenarbeit im Kommando Cyber- und Informationsraum

Der Cyber- und Informationsraum (CIR) als Dimension kennt weder institutionelle noch politische Grenzen. Erfolgreiches Handeln innerhalb dieser Dimension ist nur gesamtstaatlich und ressortübergreifend denkbar.

Oberstleutnant Peter Leffler, Bundeswehr

Oberstleutnant Jan Pangerl, Bundeswehr

Die Wahrnehmung des Auftrages der Streitkräfte in der Dimension CIR muss sich diesen Rahmenbedingungen anpassen und Cyber-Sicherheit gesamtstaatlich als elementaren und integralen Bestandteil der Landes- und Bündnisverteidigung begreifen. Dieser Ansatz wird im Kommando Cyber- und Informationsraum der Bundeswehr seit seiner Aufstellung verfolgt und auch in der Zusammenarbeit des Kommandos mit nationalen Partnern im behördlichen und nicht-behördlichen Umfeld außerhalb des Verteidigungsressorts abgebildet.

Die Nationale Sicherheitsstrategie beschreibt Cyber-Sicherheit „als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft“ und betrachtet sie „angesichts der Bedeutung des digitalen Raums“ als „essenziellen Teil von integrierter Sicherheit“. Hier setzt die Bundesregierung auf „das Zusammenwirken der staatlichen Institutionen für Cyber-Sicherheit und Strafverfolgung sowie von Nachrichtendiensten, Diplomatie und Militär bei der Abwehr von Cyber-Bedrohungen“.

Zuständigkeit nicht immer eindeutig

In der aktuellen Cyber-Sicherheitsstrategie für Deutschland aus dem Jahr 2021 sind den verschiedenen Ressorts der Bundesrepublik Deutschland unterschiedliche Aufgaben zugewiesen. Dem Verteidigungsressort kommt in diesem Kontext die Aufgabe der Cyber-Verteidigung zu. In Abgrenzung dazu verantwortet das Bundesministerium des Inneren die Cyber-Abwehr und das Auswärtige Amt die Cyber-Außen-

Foto: Bundeswehr/Martina Pump

politik. Die Cyber-Sicherheitsstrategie für Deutschland beschreibt den Bereich Cyber als Dimension ohne eindeutige geografische, politische oder institutionelle Grenzen. Damit ist die Zuordnung von genauen Zuständigkeiten nicht immer eindeutig. Insbesondere mit Blick auf den Kernauftrag der Streitkräfte ist es notwendig, die Verschränkung von Cyber-Abwehr und -verteidigung ernsthaft zu betrachten. Die nationale Cyber-Sicherheitsvorsorge Deutschlands kann demnach nur ressortübergreifend und gesamtstaatlich gedacht und umgesetzt werden.

Im Weißbuch 2016 wurde dieser gesamtstaatliche Ansatz aufgegriffen und die Notwendigkeit der Bündelung aller im Cyber- und Informationsraum agierenden Kräfte der Bundeswehr „unter einem Dach“ beschrieben. Diese Bündelung wurde mit der Bildung der Abteilung Cyber- und Informationstechnik im Bundesministerium der Verteidigung noch im Jahr 2016 und mit der Aufstellung des Organisationsbereichs Cyber- und Informationsraum der Bundeswehr im April 2017 auch strukturell umgesetzt.

Ressortübergreifende Zusammenarbeit zur gesamtstaatlichen Cyber-Sicherheitsvorsorge

Innerhalb des Kommandos Cyber- und Informationsraum wurde mit dem Referat „Ressortübergreifende Zusammenarbeit“ sowie mit dem Verbindungselement in das Nationale Cyber-Abwehrzentrum in der Operationszentrale des Kommandos dieser gesamtstaatliche und auch multinationale Ansatz strukturell hinterlegt. Hierbei wird durch das Referat

Ressortübergreifende Zusammenarbeit die Kooperation des gesamten Organisationsbereichs Cyber- und Informationsraum koordiniert und es werden ministerielle Vorgaben und Schwerpunkte umgesetzt. In der Praxis wird die Kooperation mit Partnern aus Industrie und Wirtschaft, aus Forschung und Lehre sowie mit Behörden außerhalb des Verteidigungsressorts gemeinsam gestaltet. Alle genannten Akteure sind wichtige Teile einer gesamtstaatlichen Cyber-Sicherheitsvorsorge.

Dabei kommt es regelmäßig zu anlassbezogenen Kooperationen, beispielsweise bei Fachkonferenzen, aber auch zu verstetigten Kooperationsformaten basierend auf geregelten Strukturen, Inhalten und Rhythmen.

Im Rahmen dieser strukturierten Zusammenarbeitsbeziehungen bearbeiten die Kooperationspartner jeweils gleichberechtigt gemeinsam festgelegte Aufgaben- und Handlungsfelder. Die Inhalte der Arbeit werden dann bei Arbeitsbesuchen und -tagungen auf Leitungsebene vorgestellt, diskutiert und weiterentwickelt.

Der Inspekteur Cyber- und Informationsraum, Vizeadmiral Dr. Thomas Daum, leitet die 4. Arbeitstagung mit dem Bitkom e. V. ein.

Foto: Bundeswehr/ Kjell Tandetzke

Kooperationspartner für Cyber- und IT-Themen

Die Zusammenarbeit mit dem Digitalverband Bitkom e. V. ist ein Beispiel, das aufzeigt, wie Kooperationen angebahnt, ausgebaut und strukturiert werden können. Unter dem Dach des Bitkom e. V. sind rund 2.700 Unternehmen der digitalen Wirtschaft organisiert. Darunter sind gut 1.000 Mittelständler, über 500 Start-ups und nahezu alle Global Player der Branche vertreten. Der Bitkom e. V. ist damit einer der wichtigsten Ansprechpartner für Cyber-/IT-Themen, Digitalisierung und Zukunft in Deutschland und ein idealer Kooperationspartner, um die Digitalisierung in den Streitkräften, deren Auswirkungen auf die Bundeswehr und letztlich auf die Bundesrepublik verstehen und vorantreiben zu können. Mit der Unterzeichnung der Kooperationsvereinbarung zwischen dem Kommando Cyber- und Informationsraum und dem Bitkom e. V. im April 2019 wurden Ziele sowie gemeinsame Arbeits- und Interessensfelder abgesteckt. Bereits wenige Wochen später konnte eine erste gemeinsame Arbeitstagung mit großem Erfolg durchgeführt werden, die inzwischen jährlich veranstaltet wird und bereits viermal ausgerichtet wurde.

Seit 2018 besteht die Kooperationsvereinbarung zwischen der Telekom und dem Kommando Cyber- und Informationsraum: Der Stellvertretende Inspekteur CIR und CISOBw Generalmajor Jürgen Setzer besichtigt das SOC der Telekom in Bonn.

Foto: Bundeswehr/Martina Pump

Derartige strukturierte Kooperationen existieren auch mit weiteren nationalen Partnern wie zum Beispiel der Telekom Security, bei der es neben gemeinsamen Aus- und Weiterbildungsmaßnahmen unter anderem auch zu wöchentlichem Austausch zwischen den jeweiligen Computer Emergency Response Teams kommt.

Mit dem Fraunhoferinstitut FKIE werden gemeinsame Forschungsvorhaben angegangen, die die Fähigkeiten des Organisationsbereichs Cyber- und Informationsraum auf künftige Herausforderungen ausrichten werden.

Innerhalb des Cyber Security Clusters Bonn, einem Verein aus in Bonn und Umgebung ansässigen DAX-Unternehmen, Mittelständlern, Universitäten und Ausbildungseinrichtungen sowie Bundesbehörden, der sich das Ziel gesetzt hat, die Region zum führenden Cyber-Security-Standort Deutschlands zu entwickeln, engagiert sich das Kommando Cyber- und Informationsraum im Beirat.

Zusammenarbeit über das Nationale Cyber-Abwehrzentrum

NATIONALES
CYBER-ABWEHRZENTRUM

Das Nationale Cyber-Abwehrzentrum ist die Plattform für gesamtstaatliche Lageführung und die reaktionsschnelle Koordination von Behörden auf Bundesebene.

Grafik: Nationales Cyber-Abwehrzentrum

Die direkte tägliche operative Zusammenarbeit gesamtstaatlicher Cyber-Sicherheit findet über das Nationale Cyber-Abwehrzentrum statt. Auf Bundesebene arbeiten die Kernbehörden Bundesamt für den Militärischen Abschirmdienst, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bundesamt für Verfassungsschutz, Bundeskriminalamt, Bundesnachrichtendienst, Bundespolizei, Bundesamt für Sicherheit in der Informationstechnik und das Kommando Cyber- und Informationsraum im Nationalen Cyber-Abwehrzentrum zusammen. Hinzu kommt eine Reihe assoziierter Behörden und Einrichtungen aus Bund und Ländern. Sie führen ihre jeweils eigene Lage zusammen, um möglichst frühzeitig Informationen auszutauschen. So können sie gemeinsam die Gesamtlage bewerten und Maßnahmen im Cyber-Abwehrzentrum koordinieren. Dabei obliegt den am Zentrum beteiligten Behörden die Ausübung ihrer operativen Befugnisse auch im Cyber-Raum.

Das Nationale Cyber-Abwehrzentrum ist somit die Plattform für gesamtstaatliche Lageführung und die reaktionsschnelle Koordination von Behörden auf Bundesebene und leistet durch die koordinierende operative und interdisziplinäre Fallbearbeitung unverzichtbare Beiträge zur gesamtstaatlichen Cyber-Sicherheit und somit – auch im Krisenfall – zur Handlungsfähigkeit der Bundesregierung.

Für den Verteidigungsauftrag sind ein umfängliches Lagebild zur Cyber-Sicherheit und die Integration wesentlicher Erkenntnisse aus diesem Bereich in das eigene Lagebild der Streitkräfte – auch schon im Frieden – unerlässlich. Insbesondere aufgrund der vielfältigen Beziehungen und gegenseitigen Abhängigkeiten betrachten die Streitkräfte die Cyber-Abwehr und Cyber-Sicherheit als integralen Bestandteil der Cyber-Verteidigung. Maßnahmen der unterschiedlichen Akteure in diesem Bereich müssen daher miteinander abgestimmt werden. Hierzu ist der Austausch im Cyber-Abwehrzentrum ein wesentlicher Faktor.

Oberstleutnant Peter Leffler ist Referent Nationale Zusammenarbeit im Referat Ressortübergreifende Zusammenarbeit, Kommando Cyber- und Informationsraum der Bundeswehr, Bonn.

Oberstleutnant Jan Pangerl ist stellvertretender Koordinator des Nationalen Cyber-Abwehrzentrums, Kommando Cyber- und Informationsraum der Bundeswehr, Bonn.

Die Umsetzung von NIS-2: Herausforderungen und Lösungsansätze

Mit der NIS-2-Richtlinie will die EU die Cybersecurity kritischer Infrastrukturen stärken. Die Umsetzung stellt viele Organisationen jedoch vor Herausforderungen, da die Zahl der Unternehmen, die als Betreiber kritischer Infrastrukturen gelten, stark zunimmt und viele neue Akteure strengere Cybersecurity-Standards erfüllen müssen. Die Wahl geeigneter Cybersecurity-Tools und die genaue Meldung von Vorfällen sind weitere Herausforderungen, bei Verstößen drohen Strafen. Auch die knappe Umsetzungsfrist (17.10.2024) für die EU-Mitgliedstaaten erhöht den Druck, da bis dahin klare Pläne zur Einhaltung der Richtlinie vorliegen müssen.

Um die Anforderungen der NIS-2-Richtlinie zu erfüllen, müssen Betreiber kritischer Infrastrukturen drei wesentliche Schritte unternehmen. Sie müssen ihre Einstufung als „wesentlich“ oder „wichtig“ nach NIS 2 klären und die erste Risikoanalyse durchführen. Dazu gehört die Definition der im Sinne von NIS 2 kritischen Services, Prozesse und Assets der Organisation. Im Rahmen einer umfassenden Risikobewertung im nächsten Schritt werden diese segmentiert, um gezielte Cybersecurity-Maßnahmen zu planen. Abschließend werden geeignete Präventions-, Detektions- und Reaktionsmaßnahmen implementiert.

Um die Anforderungen von NIS 2 erfolgreich umzusetzen, empfiehlt sich ein proaktiver Ansatz. Bestehende Standards aus dem IT-Sicherheitsgesetz 2.0, eine Zusammenarbeit mit Aufsichtsbehörden sowie die Beratung durch Experten können Unternehmen und Behörden bei der Wahl der für sie passenden Tools und Strategien unterstützen.

27. Europäischer Polizeikongress

16.—17. April 2024

CityCube Berlin

THE SAVE DATE

www.europaeischer-polizeikongress.de

12.–13. März 2024

DIGITALER STAAT

schneller, stärker, souveräner – GEMEINSAM.

Andel's Berlin

SAVE THE DATE

Illustration: BSR, Basiert unter Verwendung von Tatiana; alukard; Sergey Niven, (de.stock.adobe.com)

DIGITALER-STAAT.ORG

Behörden Spiegel

Sicheres Arbeiten mobil und im Home Office.

Mit der SINA Workstation sind sensible Daten premiumsicher.

Die SINA Workstation erfüllt als einzige Lösung standardmäßig alle BSI-Anforderungsprofile an einen sicheren Arbeitsplatz. VPN-Client, 2-Faktor-Authentisierung, Festplattenverschlüsselung und Schnittstellenkontrolle in einem Gerät.

secunet.com **protecting digital infrastructures**

secunet