IDW KNOWLEDGE PAPER

CYBERRISK

TEIL 1: GRUNDLAGEN – DEFINITIONEN, MASSNAHMEN, RISIKOLAGE UND ORGANISATIONEN

STAND 25.10.2021

IDW
INSTITUT DER WIRTSCHAFTSPRÜFER

INHALT

1. EINLEITUNG

In zunehmender Regelmäßigkeit beeinträchtigen Cyberattacken das tägliche Leben. Während sich die Auswirkungen solcher Angriffe für viele Menschen darauf beschränken, dass sie bestimmte Dienstleistungen vorübergehend nicht in Anspruch nehmen können, können Cyberattacken für viele Unternehmen schnell existenzbedrohend werden. Die Auswirkungen der Coronavirus-Pandemie befeuerten diese Entwicklung.

Vor diesem Hintergrund rückt das Thema Cyberrisk bei Politik, Aufsicht und Wirtschaft zunehmend in den Fokus. Auch Wirtschaftsprüfer widmen sich im Rahmen ihrer Tätigkeit den Gefahren, die von Cyberrisk ausgehen.

Das IDW hat eine Vielzahl von allgemeinen Fragestellungen zu Cyberrisk zusammengestellt. Ausgewählte Themenbereiche werden jeweils gebündelt in einem IDW Knowledge Paper behandelt. Der hier vorliegende Teil 1 dieser Reihe soll faktenbasierte Grundlagen vermitteln. Das Papier dient daher auch als Basis für die folgenden, weitergehenden IDW Veröffentlichungen zu Cyberrisk. Ausgangspunkt für die Erläuterungen in Teil 1 ist eine Zuordnung bekannter Cybercrimefälle in die grundlegenden Arten von Cyberattacken. Anhand von Beispielen wird der Ablauf derartiger Angriffe verdeutlicht. Hieran knüpft eine beispielhafte Darstellung von Präventions-, Schutz- und Abwehrmaßnahmen gegen Cyberattacken an. Es folgt eine Lagebestimmung für Deutschland. Den Abschluss bilden die Einordnung der wichtigsten Institutionen, die sich der Verhinderung von Cyberrisk widmen, sowie eine Erläuterung der europäischen und nationalen Strategien gegen solche Risiken.

2. WELCHE GRUNDLEGENDEN ARTEN VON CYBERATTACKEN GIBT ES UND WIE FUNKTIONIEREN DIESE?

Cyberattacken umfassen ein breites Spektrum an Tätern und Angriffsvektoren[1]. Auf Seiten der Täter reicht das Spektrum von sog. Skriptkiddies[2] bis hin zu staatlichen Angreifern. Die organisierte Cyberkriminalität setzt zunehmend auf typische industrielle Vorgehensweisen wie Outsourcing und Spezialisierung. Beispielsweise gibt es spezialisierte Anbieter, die anderen Tätern Zugang zu Netzwerken verschaffen, sog. Access Broker, während sich andere Anbieter auf die Entwicklung von Schadsoftware konzentrieren. Diese Dienstleistungen werden gegen entsprechende Lizenzgebühren angeboten.[3] Angreifer können sich also solche Cybercrimeleistungen einkaufen („Cybercrime as a Service"). Sie benötigen dann weder eigenes Know-how noch eigene technische Ressourcen.[4] Bei größeren Attacken kommt es auch vor, dass sich verschiedene Angreifer zusammenschließen. Zudem spielen bei vielen Cyberattacken Wirtschaftlichkeitsüberlegungen und Skalierungseffekte eine große Rolle.[5]

Auch die Angriffsvektoren variieren stark. Sie reichen von einfachen Phishing-Mails bis hin zu komplexen Advanced Persistent Threats, bei denen unter Aufbietung großer Ressourcen verschiedene Vorgehensweisen und Techniken kombiniert werden. Nachfolgend werden die wichtigsten Kategorien von Cyberattacken vorgestellt und anhand von Beispielen näher erläutert.

2.1. Phishing

Phishing stellt wohl die bekannteste und gleichzeitig einfachste Form von Cyberattacken dar. Jeder Bankkunde, der über einen Online-Banking-Zugang verfügt, kennt die Warnungen vor Phishing-Mails, mit denen Kriminelle versuchen, an die Zugangsdaten zum Online-Banking zu kommen. Nicht immer resultiert aus den durch Phishing erlangten Informationen ein unmittelbarer Schaden. Oftmals dient Phishing der Vorbereitung von komplexeren Cyberangriffen oder anderen Straftaten.

Seit Beginn der Coronavirus-Pandemie konnte ein deutlicher Anstieg an Phishing-Aktivitäten verzeichnet werden. Google bezifferte Mitte April 2020 die Anzahl der allein für den E-Mail-Dienst Gmail geblockten Phishing-Mails auf mehr als 100 Millionen täglich. Hiervon hatten täglich etwa 18 Millionen Mails Bezug zur Coronavirus-Pandemie.[6] In ihrem „Phishing and Fraud Report 2020" stellen die Autoren von F5 Labs für 2020 einen Anstieg bei Phishing-Vorfällen um 15% im Ver-

gleich zum Vorjahr fest. Im gleichen Zug wie sich die Unsicherheit während der Pandemie erhöhte, nahmen auch die Phishing-Aktivitäten zu. In Hochzeiten wurden gegenüber dem Vergleichsdurchschnitt früherer Jahre 2,2-mal so viele Phishing-Attacken verzeichnet. [7]

Massenhaft versandte Phishing-Mails stellen allerdings nur eine Spielart dieser Angriffskategorie dar. Phishing ist eine Unterart des Social Engineering[8] und beschreibt die Beschaffung persönlicher Daten anderer Personen (bspw. Passwörter, Kreditkartennummern, o.Ä.) mittels gefälschter E-Mails oder Websites. Zu den wichtigsten Varianten von Phishing-Attacken gehören[9]:

- **Deceptive Phishing**: Deceptive Phishing nutzt die Technik des Domain Spoofings. Domain Spoofing beschreibt die Vortäuschung einer gefälschten Website eines Unternehmens. Die Opfer erhalten E-Mails von vermeintlich vertrauenswürdigen Absendern (beispielsweise eines Kreditinstituts). Mit dieser E-Mail wird das Opfer zum Besuch der Website aufgefordert (z.B. um sich im Online-Banking anzumelden aufgrund einer Sicherheitsüberprüfung). In der E-Mail ist i.d.R. ein Link hinterlegt, der vermeintlich auf die Website des Absenders verweist. Wird der Link angeklickt, wird das Opfer auf eine gefälschte Website umgeleitet. Meldet sich das Opfer nun im Online-Banking an, fangen die Täter die Nutzerdaten ab und haben nun Zugriff auf den Account des Kunden.

- **Pharming**: Eine Weiterentwicklung des Deceptive Phishing stellt das Pharming dar. Hierbei werden betrügerische E-Mails von authentischen Quellen verschickt und die Opfer beispielsweise aufgefordert, eine Passwortänderung durchzuführen. Der angegebene Link verwendet dabei dieselbe Webadresse wie das Original. Anstatt auf die Original-Website wird der Nutzer aber auch hier auf eine gefälschte Website umgeleitet. Das geschieht entweder durch Infektion des Computers, oder durch Manipulation eines DNS-Servers, so dass die vom Benutzer eingegebene, korrekte Internetadresse in eine falsche IP-Adresse umgewandelt wird.

- **Spear Phishing**: Bei dieser Art des Phishings suchen sich die Täter gezielt bestimmte Personen innerhalb eines Unternehmens heraus. Sie verwenden Social-Engineering Techniken, um ihre E-Mails auf das Opfer maßzuschneidern. Diese Attacken werden i.d.R. so an den Adressaten angepasst, dass traditionelle Spamfilter sie nicht erkennen. Weitere Unterarten des Spear Phishings sind das Whaling, bei dem hochrangige Führungskräfte ins Visier genommen werden, um sich deren weitreichende Befugnisse zu Nutze zu machen, und der CEO Fraud, bei dem der Absender sich als Führungskraft ausgibt und sich an untergeordnete Mitarbeiter wendet.

- **Clone Phishing**: Hierbei wird eine Original-E-Mail, die das Opfer bereits erhalten hat, kopiert und dem Opfer nochmals zugestellt. Dabei werden Links und Anhänge der ursprünglichen E-Mail durch gefälschte Links und Anhänge ausgetauscht.

- **Watering Hole Phishing**: Hierbei werden reguläre Websites, die oft von den Opfern besucht werden, mit Malware infiziert. Beim Besuch der Website wird die Malware automatisch auf den Computer der Opfer geladen. Die Schadsoftware ermöglicht den Angreifern Zugriff auf die Daten der Opfer.

- **Evil Twin**: Hierbei wird in betrügerischer Absicht ein drahtloser Wi-Fi-Zugangspunkt angeboten. Der Angreifer hält sich hierzu in der Nähe eines regulären Hot-Spots auf und findet durch Software dessen Funkfrequenz und den SSID (Service Set Identifier) heraus. Anschließend sendet er sein eigenes Funksignal mit gleicher SSID. Wenn der Benutzer dann eine Verbindung herstellt, kann der Angreifer den Netzwerk-Verkehr mitlesen.

- **Smishing/Vishing**: Beim SMS-Phishing (Smishing) werden statt E-Mail betrügerische SMS an die Opfer versendet. Voice Phishing (Vishing) nutzt automatisierte Anrufe, um persönliche Daten zu erlangen.

In den letzten Jahren wurden einige spektakuläre Phishing-Attacken verzeichnet: So verloren beispielsweise der Autozulieferer Leoni oder der Luftfahrtzulieferer FACC im Jahr 2016 40 bzw. 50 Millionen Euro durch CEO-Fraud. Im gleichen Jahr verlor die Zentralbank von Bangladesch 80 Millionen Dollar aufgrund gefälschter Zahlungsanweisungen.

2.2. Malware

Unter Malware („Malicious Software“) werden Schadprogramme wie Viren, Würmer, Trojaner, Ransomware oder Spyware subsumiert.[10]

Folgende Arten von Malware können beispielsweise unterschieden werden:

- **Computer-Würmer**: Würmer sind eigenständige Programme. Sie müssen also vom Benutzer mindestens einmal explizit gestartet werden.

- **Computer-Viren**: Viren sind Computerprogramme, die sich Wirtsprogrammen bedienen, sich selbst vervielfältigen können und sich auf diesem Weg vermehren. Neben dieser Grundfunktion enthalten Viren auch andere (Schad-)Funktionen. Viren sind stets an Wirtsprogramme gebunden.

- **Trojaner**: Bei Trojanern handelt es sich um vermeintlich nützliche Programme, die neben ihrer eigentlichen Funktion noch weitere, dem Benutzer nicht bekannte Funktionen ausführen. Diese Funktionen laufen für den Benutzer i.d.R. unbemerkt ab. Im Gegensatz zu Viren und Würmern können sich Trojaner nicht selbst replizieren.

- **Ransomware**: Ransomware beschreibt Software, durch welche die Daten eines Nutzers verschlüsselt werden.

- **Spyware**: Spyware ist Software, welche die Daten eines Nutzers ohne dessen Wissen oder Zustimmung an einen Dritten sendet.

2.2.1. Computer-Würmer

Im Juni 2010 erlangte eine unter dem Namen Stuxnet bekanntgewordene Malware internationale Bekanntheit und veränderte die IT-Sicherheitsindustrie nachhaltig. Stuxnet ist ein Computer-Wurm, der speziell für die Sabotage des iranischen Atomprogramms konzipiert wurde. Stuxnet zirkulierte weltweit auf tausenden Rechnern, richtete aber nur dann Schaden an, wenn er auf eine sehr spezifische Konfiguration von Reglereinheiten stieß. Dabei handelte es sich um die Steuerung der Uranzentrifugen im iranischen Natanz.[11] Nur in dieser Umgebung manipulierte Stuxnet die Drehgeschwindigkeit der angeschlossenen Motoren. In den Jahren 2009 und 2010 zerstörte Stuxnet auf diese Weise schätzungsweise 1000 der 9000 vorhandenen Zentrifugen in Natanz.[12] Stuxnet nutzte zum Eindringen in die Systeme mehrere Sicherheitslücken aus. Die Verbreitung von Stuxnet erfolgt über USB-Speichermedien. Abhängig vom eingesetzten Betriebssystem und damit den vorhandenen Sicherheitslücken wurden mehrere Varianten des Schadcodes ausgeführt. Der eigentliche Schadcode installierte sich danach in einem eigenen, vom System als vertrauenswürdig eingestuften Prozess. Dadurch war es Stuxnet möglich, sich regelmäßig zu aktualisieren.[13]

Während es sich bei Stuxnet um eine hochentwickelte und für einen speziellen Zweck konstruierte Cyberwaffe handelt, sind die meisten Computer-Würmer und -Viren nicht so komplex aufgebaut. Welche Schadfunktionen Würmer ausführen, lässt sich nur sehr schwer bestimmen. Die Schadfunktionen können beispielsweise darin bestehen, dass vertrauliche Daten ausgespäht werden, dass Dateien und Programme gelöscht bzw. verändert werden, oder dass Sicherheitslücken geschaffen werden, durch die Angreifer die befallenen Computer übernehmen können.

Computer-Würmer lassen sich beispielsweise anhand ihrer Verbreitungsart wie folgt unterteilen:[14]

- **E-Mail-Würmer**: E-Mail-Würmer verbergen sich entweder in Datei-Anhängen von E-Mails oder werden durch Anklicken von in E-Mails enthaltenen Links geladen. E-Mail-Würmer greifen oftmals auf die Adressbücher von E-Mail-Programmen zu und versenden automatisch E-Mails mit dem Schadcode an die dort hinterlegten Empfänger.

- **Instant-Messaging-Würmer**: Instant-Messaging-Würmer verbreiten sich durch das Anklicken von Links, die in Instant-Messaging-Nachrichten eingebunden sind.

- **P2P-Würmer**: Bei Peer-to-Peer-Netzwerken, d.h. bei Netzwerken, bei denen eine Direktverbindung zwischen den einzelnen Benutzern besteht, können sich Computer-Würmer beispielsweise über geteilte Dateien oder Sicherheitslücken in einzelnen Rechnern verbreiten.

- **Würmer für Wechseldatenträger**: Hier erfolgt die Übertragung mittels USB-Sticks oder anderen Speichermedien. Die Würmer kopieren sich selbstständig auf die Datenträger, um sich weiter zu verbreiten. Die Computer-Würmer werden i.d.R. beim automatischen Start der Speichermedien aufgerufen.

- **Würmer für USB-Geräte**: Hier enthalten die infizierten USB-Geräte einen Kleinprozessor, der eine Tastatur nachbildet. Werden die infizierten USB-Geräte an den Computer angeschlossen, sendet die gefälschte Tastatur Befehle an das System, die scheinbar von einem echten Benutzer stammen. Auf diese Weise wird die Schadsoftware gestartet, die sich auf dem eingebauten USB-Datenträger befindet.

- **Handywürmer**: Hier erfolgt die Verbreitung oftmals über Bluetooth-Verbindungen bzw. MMS.

2.2.2. Computer-Viren

Das Computer-Virus mit dem bislang größten geschätzten Schaden hört auf den Namen Mydoom und verbreitete sich überwiegend zwischen Januar und Februar 2004. Mydoom infizierte zwischenzeitlich rund zwei Millionen Rechner und 20% - 30% des weltweiten E-Mail-Verkehrs. Experten schätzten den durch Mydoom verursachten Schaden auf rd. 38,5 Milliarden Euro. Mydoom blockierte Server mittels Spam und spähte Passwörter und andere sensible Daten aus. Mit diesen Informationen wurde Geld von Bankkonten gestohlen und Dienstleistungen ohne Bezahlung in Anspruch genommen. Die Verbreitung von Mydoom erfolgte über E-Mail.[15]

Zu den grundlegenden Funktionen von Viren wie Mydoom gehört es, dass diese Schäden auf dem infizierten Computer anrichten, indem sie Dateien löschen oder Inhalte verändern. Manche Viren haben auch nur das Ziel, den Benutzer zu verunsichern, indem Ausgaben am Bildschirm verändert oder akustische Signale erzeugt werden. Möglich ist es zudem, dass sich Viren tarnen oder verstecken.

Exkurs: Versteckte Viren

Eine mit einem Virus verseuchte Datei kann normalerweise anhand der Dateigröße erkannt werden. Durch das Anfügen des Virus wird die Datei größer.

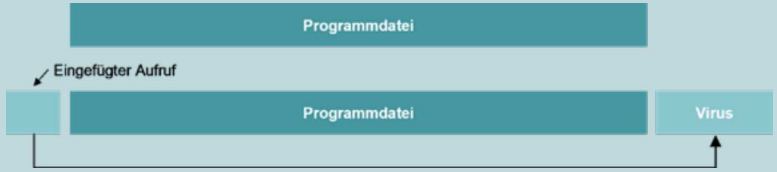

Abbildung 1: Versteckte Viren (angelehnt an: Fuhs.de [Computerviren und ihre Vermeidung – Kapitel 3])

Das Virus kann diese Auffälligkeit tarnen, in dem es im Programm einen Block zusammenhängender Nullen sucht. Diesen Block löscht das Virus und kopiert sich selbst hinein. Beim Starten des Programms wird nun das Virus aufgerufen und überschreibt im Programm den gelöschten Block wieder mit Nullen.

Grundsätzlich lassen sich folgende Arten von Viren unterscheiden:[16]

- **Bootviren**: Diese Viren gehörten zu den ersten Viren überhaupt, sind mittlerweile aber fast nicht mehr zu finden. Sie infizieren den Bootsektor von Disketten und Festplattenpartitionen oder den Master Boot Record (MBR) einer Festplatte.[17] Durch diese Vorgehensweise wird stets das Bootvirus vor dem Betriebssystem aufgerufen und kann die Schutzmechanismen des Betriebssystems aushebeln.

- **Dateiviren**: Dateiviren infizieren einzelne (Programm-)Dateien. Wird die infizierte Datei geöffnet / das Programm gestartet, lädt sich das Virus in den Hauptspeicher und versucht, dort sesshaft zu werden. Gelingt ihm dies, bleibt es auch nach der Beendigung des Wirtsprogramms im Speicher. Beim Start von weiteren Programmen versucht das Virus auch diese Programme zu infizieren, indem beispielsweise der Viruscode an das Ende der Datei angehängt wird.

- **Makroviren**: Hierbei handelt es sich um eine Unterart der Dateiviren, die sich in den Makros[18] von Dokumentdateien verstecken (beispielsweise Word-Dokumente).

- **Skriptviren**: Skriptviren ähneln Makroviren. Sie verstecken sich statt in Makros in sog. Skripten. Bei einem Skript handelt es sich um eine Abfolge von Befehlen, die von einem bestimmten Programm (z.B. einem Webbrowser) ausgeführt werden. Skripte werden zum Beispiel zur Generierung von Webseiten benutzt.

2.2.3. Trojaner

Einer der bekanntesten Trojaner und gleichzeitig ein Beispiel dafür, wie sich Schadprogramme weiterentwickeln, ist das ursprünglich als Banking-Trojaner entwickelte Schadprogramm Emotet. Emotet wurde erstmals im Jahr 2014 erkannt. Das ursprüngliche Ziel von Emotet war es, in fremde Geräte einzudringen und sensible private Daten (Zugang zum Online-Banking) auszuspähen. Emotet verbreitet sich vor allem durch sehr authentisch wirkende Spam-E-Mails. Die E-Mail enthält dabei einen bösartigen Link oder ein infiziertes Dokument mit aktivierten Makros. Durch Herunterladen des Dokuments bzw. Öffnen des Links werden automatisch weitere Schadprogramme auf den Computer heruntergeladen.

Emotet hat sich mittlerweile zu einem Dropper weiterentwickelt. Unter einem Dropper wird eine eigenständig ausführbare Programmdatei verstanden, die der erstmaligen Freisetzung von Computerviren dient. Der Dropper fungiert dabei als Wirtsprogramm für das Computervirus. Der eigentliche Schaden wird dann durch das freigesetzte Computervirus verursacht. Die häufigsten durch Emotet nachgeladenen Programme sind:

- **Trickbot**: Ein Banking-Trojaner, der dem Ausspähen von Online-Banking-Daten dient.
- **Ryuk**: Ein Verschlüsselungstrojaner (Ransomware), der die Daten auf dem Computer verschlüsselt, um Lösegeld zu erpressen.

Emotet befiel im Jahr 2018 unter anderem das Klinikum Fürstenfeldbruck, welches daraufhin 450 Computer abschalten und sich bei der Rettungsleitstelle abmelden musste. Im September 2019 war das Berliner Kammergericht betroffen und im Dezember 2019 die Uni Gießen. Auch die Medizinische Hochschule Hannover und etwa die Stadtverwaltung von Frankfurt am Main wurden von Emotet infiziert.[19]

Die Gefahr von Emotet ist vor allem dem Umstand geschuldet, dass Emotet in der Lage ist, gängige Antivirenprogramme zu täuschen. Emotet liest hierzu den E-Mail-Verkehr der betroffenen Nutzer aus und erzeugt auf dieser Basis authentische E-Mails. Meist enthalten die Mails dabei ein infiziertes Word-Dokument, das man herunterladen soll oder einen gefährlichen Link. Als Absender wird dabei stets der korrekte Name angezeigt.[20] Zusätzlich ist Emotet dazu übergegangen, W-LAN-Verbindungen anzugreifen. Sobald sich Emotet auf einem Gerät eingenistet hat, das mit einem WLAN verbunden ist, scannt Emotet alle WLANs, die sich in der Nähe befinden. Mithilfe einer Passwortliste versucht der Virus anschließend, Zugriff auf die Netzwerke zu bekommen und somit weitere Geräte zu infizieren.[21]

Im Januar 2021 gaben die Generalstaatsanwaltschaft Frankfurt am Main – Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) – und das Bundeskriminalamt (BKA) bekannt, dass die Emotet-Infrastruktur im Rahmen einer international konzertierten Aktion „übernommen und zerschlagen“ wurde. Strafverfolgungsbehörden aus Deutschland, den Niederlanden, der Ukraine, Frankreich, Litauen sowie aus England, Kanada und den USA waren Teil der Aktion. Die Strafverfolgungsbehörden teilten mit, dass insgesamt mehr als 100 Server der Emotet-Infrastruktur deaktiviert wurden, 17 davon allein in Deutschland.[22]

Emotet deckt ein breites Einsatzspektrum von Trojanern ab. Hierzu gehören regelmäßig das Kopieren, Löschen, Modifizieren und Blockieren von Daten sowie die Einschränkung der System- und Netzwerkleistung. Trojaner werden regelmäßig anhand der Aktionen klassifiziert, die sie auf dem Computer durchführen. Zu den bekanntesten Arten zählen:[23]

- **Fake-Anti-Virus-Trojaner**: Fake-Anti-Virus-Trojaner simulieren die Aktivität von Anti-Viren-Software.
- **Backdoor-Trojaner**: Durch die Schaffung von sog. Backdoors wird es den Angreifern ermöglicht, die Remote-Steuerung über den infizierten Computer zu übernehmen.

- **Rootkits**: Rootkits dienen zur Verschleierung bestimmter Aktivitäten oder Objekte auf dem Computer.
- **Banking-Trojaner**: Diese Trojaner dienen dem Ausspähen von Online-Banking-Daten.
- **DDoS-Trojaner**: DDoS-Trojaner dienen der Durchführung von DDoS-Attacken.
- **Download-Trojaner**: Durch diese Trojaner wird automatisch Software heruntergeladen.
- **Dropper**: Dropper dienen als Wirtsprogramme für Viren.
- **Mailfinder-Trojaner**: Mailfinder-Trojaner sammeln E-Mail-Adressen auf dem Computer.
- **SMS-Trojaner**: SMS-Trojaner versenden automatisiert SMS an kostenpflichtige Telefonnummern.
- **Spy-Trojaner**: Spy-Trojaner spionieren Benutzer aus, indem sie beispielsweise Tastaturanschläge aufzeichnen oder Screenshots aufnehmen.

2.2.4. Ransomware

Im Jahr 2017 versetzte der wohl bislang bekannteste Vertreter der Klasse Ransomware, WannaCry, die Öffentlichkeit in Aufruhr und sorgte für hohe Schäden und sogar für die Beeinträchtigung des öffentlichen Lebens. Während WannaCry beispielsweise in Deutschland die Anzeigetafeln von vielen Bahnhöfen lahmlegte, war in Großbritannien die medizinische Versorgung massiv beeinträchtigt, da WannaCry das staatliche Gesundheitssystem NHS befallen hatte und den Zugriff auf Patientendaten verhinderte.[24] Derartige Angriffe haben in jüngster Vergangenheit verstärkt zugenommen. Im Mai 2021 waren die Colonial-Ölpipeline in den USA und die US-Tochter des weltgrößten Fleischproduzenten JBS Opfer eines Cyberangriffs mit Ransomware geworden.[25] Im Juli 2021 wurde der Landkreis Anhalt-Bitterfeld Opfer einer Attacke mit Ransomware und musste zwischenzeitlich sogar den Katastrophenfall ausrufen.[26] Hierbei nutzten die Angreifer eine Sicherheitslücke in der Druckfunktion von Windows, die Anfang Juli bekannt geworden war und kurze Zeit später geschlossen wurde.[27] Im selben Zeitraum wurde ein ähnlicher Angriff auf Kunden des amerikanischen IT-Unternehmen Kaseya, darunter eine große schwedische Supermarktkette, durchgeführt. Hierbei nutzten die Angreifer eine Schwachstelle in der von Kaseya angebotenen Fernwartungssoftware VSA und infizierten über Updates die Rechner der betroffenen Firmen („Third Party Risk“).[28]

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern, um Lösegeld zu erpressen. Die Angreifer erreichen dies i.d.R. durch Verschlüsselung der Daten, oftmals verbunden mit der Drohung, sensible Daten zu veröffentlichen. Der für die Entschlüsselung notwendige Schlüssel wird dann, wenn überhaupt, nur gegen Lösegeld ausgehändigt.[29] Die Anfänge von Ransomware reichen bis ins Jahr 1998 zurück, als die erste Ransomware, bekannt unter dem Namen AIDS-Trojaner oder PC Cyborg, auf Disketten verschickt wurde. Die Zahlung sollte damals noch auf ein normales Konto in Panama erfolgen. Mit verstärkter Nutzung des Internets wurde die Ausbreitung leichter. Ab dem Jahr 2006 wurde für Ransomware erstmals die effektivere asymmetrische RSA-Verschlüsselung eingesetzt, die im folgenden Exkurs erläutert wird.

Exkurs: RSA-Verschlüsselung

Bei der RSA-Verschlüsselung handelt es sich um eine Public-Key-Verschlüsselung. Hierbei werden die zu verschlüsselnden Daten mit einem öffentlich bekannten Schlüssel (public key) verschlüsselt. Für die Entschlüsselung wird hingegen der private key benötigt.

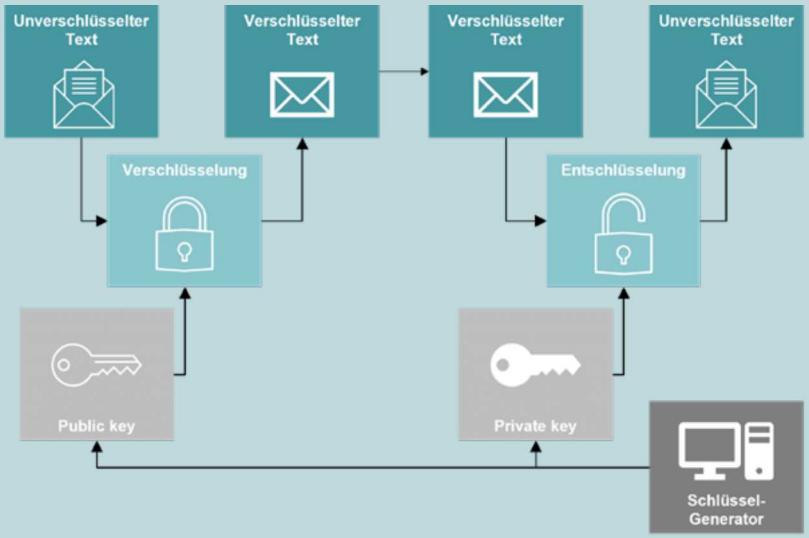

Abbildung 2: RSA-Verschlüsselung (angelehnt an: Java RSA Encryption and Decryption Example | ECB Mode + 4096 Bits + OAEPWITHSHA-512ANDMGF1PADDING (javainterviewpoint.com))

Ab 2011 breiteten sich verschiedene Ransomware-Varianten aus. Ein weiterer Entwicklungsschritt für diese Cyberattacken war die Verwendung von Bitcoin für Lösegeldzahlungen ab dem Jahr 2013. Bitcoin erlangte zu diesem Zeitpunkt zunehmend Akzeptanz als Zahlungsmittel und gewährleistete eine erhöhte Anonymität.

Eine echte Zäsur in der Entwicklung der Ransomware stellte das Jahr 2016 dar. Damals wurde erstmals die Ransomware Petya beobachtet, die neben der Verschlüsselung der Daten auch den Master-Boot-Record (MBR) der Festplatte überschrieb und damit das Betriebssystem von einem ordentlichen Neustart abhielt. 2017 trat dann erstmals WannaCry in Erscheinung. Die Vorgehensweise von WannaCry entsprach grundsätzlich der von Petya. Das höhere Schadenspotenzial von WannaCry er-

gab sich aber aus der Art der Verbreitung. WannaCry nutzte für seine Verbreitung eine weit verbreitete Schwachstelle (Eternalblue) im Betriebssystem Windows aus und verbreitete sich als Wurm auf alle von einem infizierten Rechner erreichbaren Windowssysteme.

Die nächste Entwicklungsstufe stellte die Ransomware NotPetya dar. Diese trat kurz nach WannaCry in Erscheinung. NotPetya gab dem Opfer nicht die Möglichkeit, die Daten wieder zu entschlüsseln und war insofern eher ein Instrument zur Lösegelderpressung.

Gerade NotPetya verdeutlicht das eigentliche Schadenspotenzial von Ransomware. Der potenzielle Schaden beschränkt sich nicht auf das zu zahlende Lösegeld, sondern besteht u.a. im Verlust von Unternehmensdaten. Selbst wenn es einen Schlüssel zum Entschlüsseln gibt, kann eine Entschlüsselung an technischen Gegebenheiten scheitern, oder bereits der zeitweise Ausfall von Kritischen Systemen hohe Schäden verursachen.

Aufgrund dessen ist es wichtig, sich mit den Angriffsvektoren für Ransomware auseinander zu setzen, um das Eindringen bzw. die Verbreitung solcher Software zu unterbinden. Zu den gebräuchlichsten Angriffsvektoren gehören[30]:

- **Spam**: In den Anhängen von meist sehr professionell gestalteten Spam-Mails werden meist kleine Programme versteckt, die die eigentliche Schadsoftware aus dem Internet nachlädt. Derartige Programme können beispielsweise in Makros von Microsoft Office Dokumenten versteckt werden.

- **Drive-By Infektionen mittels Exploit-Kits**[31]: Unter Drive-By-Infektionen werden Infektionen durch das schlichte Besuchen von Websites bezeichnet. Beim Besuch einer Website, die beispielsweise Java-Funktionen nutzt, können Programmcodes über den Browser auf das eigene System geladen und dort gestartet werden. Der Programmcode hat nun dieselben Rechte wie der aktuell eingeloggte Benutzer. Eine gängige Variante hiervon ist die Drive-by-Infektion per Malvertising. Hierbei versteckt sich der Schadcode in auf der Website eingebundener Werbung.

- **Schwachstellen in Servern**: Hierbei wird versucht, in Server, die aus dem Internet erreichbar sind, einzudringen. Dies kann durch Ausnutzung von Schwachstellen oder durch das Erraten von schwachen Passwörtern (Brute-Force-Angriffe) geschehen.

- **Ungeschützte Fernwartungszugänge**: Hierbei scannen die Täter das Internet aktiv nach Systemen, welche Fernwartungszugänge ins Internet anbieten, wie zum Beispiel Microsoft Remote-Desktop (RDP). Dort führen sie Brute-Force-Angriffe auf das Passwort durch. Bei einem erfolgreichen Login wird die Schadsoftware installiert.

Exkurs: Brute-Force-Angriffe
Ein Brute Force-Angriff beschreibt das einfache Ausprobieren jeder möglichen Passwortkombination. Die Erfolgschancen für Brute Force-Angriffe sind dabei abhängig von der Länge des Passworts, der Anzahl der möglichen Zeichen und der Rechnergeschwindigkeit. Die Anzahl der möglichen Passwortkombinationen ergibt sich, indem die Anzahl der möglichen Zeichen mit der Anzahl der Stellen des Passworts potenziert wird.

Wird beispielsweise das Alphabet (52 Zeichen) und die Ziffern 0–9 (10 Zeichen) verwendet und ist das Passwort 6 Stellen lang, ergeben sich hieraus $62^6 = 56.800.235.584$ Möglichkeiten. Das erscheint zunächst viel, jedoch können die derzeit schnellsten moderne Rechner bis zu 2 Billionen Passwörter pro Sekunde überprüfen. Ein solcher Rechner könnte in rd. 30 Sekunden alle möglichen Passwörter ausprobieren.

2.1.1. Spyware

Im Jahr 2014 kam es vermehrt zu gezielten Cyberattacken auf hochrangige Führungskräfte auf Geschäftsreise. Bei der unter dem Namen Dark Hotel bekannt gewordenen Vorgehensweise wurden ausgewählten Opfern sensible Daten mittels Spyware gestohlen. Hierfür wird ein kompromittierter WLAN-Access-Point bereitgestellt. Verbindet sich das Opfer mit dem Hotel-WLAN, erscheint eine Aufforderung, ein Update für eine Standardsoftware wie Google Toolbar, Adobe Flash oder Windows Messenger zu installieren. Statt des Updates wird jedoch ein Backdoor-Programm heruntergeladen und installiert. Über dieses Backdoor-Programm wird anschließend Spyware, wie Keylogger, nachgeladen. Die Spyware sammelt Daten über das System und die darauf installierte Antivirensoftware, liest alle Tastaturanschläge mit und sucht in Webbrowsern nach gespeicherten Passwörtern sowie nach Zugangsdaten für Mailkonten und soziale Netzwerke. Nach der erfolgreichen Attacke werden in der Regel die Spuren auf dem Computer beseitigt.[32]

Bei Spyware, wie sie bei Dark Hotel eingesetzt wird, handelt es sich um verschiedene Arten von Programmen, die sich tarnen und somit unbemerkt im Hintergrund laufen. Sie sammeln laufend Informationen und erlauben ggf. den Fernzugriff auf das infiltrierte System. Die Erscheinungsformen von Spyware und die Funktionen sind höchst unterschiedlich. Mögliche Erscheinungsformen sind:

- **Key-Logger**: Hierbei werden die Tastatureingaben aufgezeichnet und an einen Dritten meist in Form einer Text-Datei gesendet.
- **Tracking-Cookies**: Cookies sind Text-Dateien, die von Webseiten in den Browserverlauf des Nutzers gespeichert werden. Bei Tracking-Cookies kann der Server beispielsweise nachvollziehen, wie oft und wie lange eine Seite vom gleichen Nutzer besucht wird. Hierdurch lassen sich Profile über die Nutzer erstellen.
- **Trojaner-Spyware**: Trojaner-Spyware ändert beispielsweise die Sicherheitseinstellungen und erlaubt die Fremdsteuerung des Geräts.

2.3. Distributed Denial of Service (DDoS)

Im Januar 2020 sah sich ein großes deutsches Kreditinstitut einer sog. Distributed Denial of Service-Attacke (kurz DDoS) ausgesetzt. Zuerst kollabierte das Online-Brokerage, anschließend brachen die Website und das Online-Banking zusammen. Die Ausfälle zogen sich über Tage hin.[33] Während zunächst von einer Hacker-Attacke ausgegangen wurde, stellte sich im Juni 2020 heraus, dass es sich bei dem Angriff um zwei Jugendliche handelte, die im Verdacht stehen, ab Juli 2019 mehrere Unternehmen durch schwere Computersabotage angegriffen und geschädigt zu haben. Interessant hierbei war einerseits, dass die Jugendlichen für ihre Attacken kein tieferes Hacker-Wissen benötigten. Die für die Angriffe notwendige Infrastruktur konnten sie einfach im Darknet mieten.[34]

Interessant war zudem, dass die Anfragen, welche die Website des Instituts blockierten, nicht von normalen Computern kamen, sondern überwiegend von internetfähigen Haushaltsgeräten. Hierbei kann es sich beispielsweise um Babyfone, Rauchmelder, Kühlschränke oder Waschmaschinen handeln.

Die Funktionsweise einer DDoS-Attacke soll nachfolgend anhand von Mirai, einem der bekanntesten Vertreter dieser Art von Cyberattacken, erläutert werden. Mirai ist eine Art Malware, die internetfähige Geräte infiziert. Sobald ein Gerät infiziert wurde, wird das Gerät zu einem ferngesteuerten Bot und Teil eines Bot-Netzwerks. Diese Bot-Netzwerke werden Dritten zur Miete angeboten.[35]

Das nachfolgende Schaubild[36] gibt eine Übersicht über die Struktur einer DDoS-Attacke:

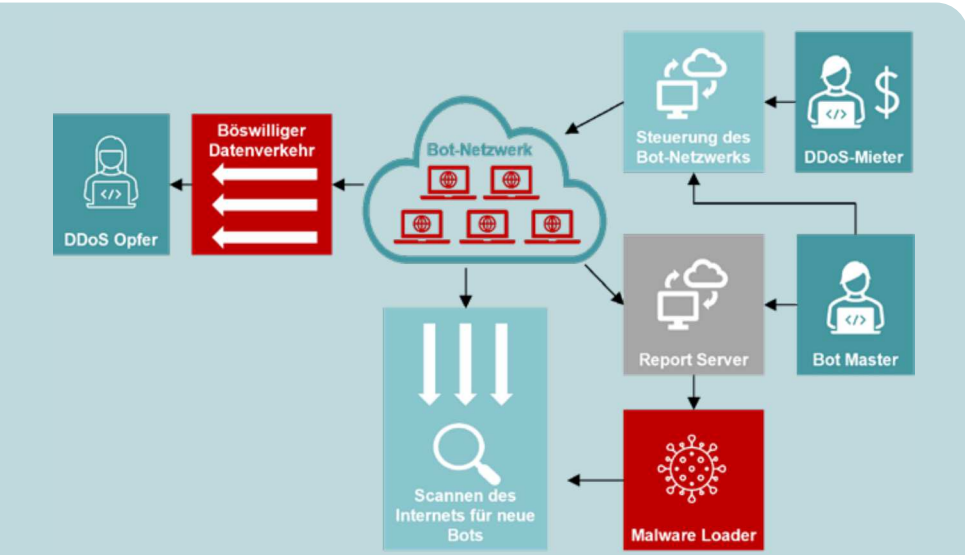

Abbildung 3: DDos-Attacke (angelehnt an: Mirai DDoS Attack Explained (imperva.com))

Das durch den sog. Bot-Master betriebene Bot-Netzwerk wird durch einen Angreifer für seinen Angriff gemietet. Gegen Zahlung eines Entgelts bekommt er Zugriff auf die Steuerung des Bot-Netzwerks und kann durch dieses mit böswilligem Datenverkehr die Server des Opfers überlasten. Netzwerkressourcen, wie z.B. Webserver, können nämlich nur eine bestimmte Anzahl von Anfragen gleichzeitig verarbeiten. Werden zu viele Anfragen gleichzeitig gestellt, erfolgt die Antwort auf Anfragen deutlich langsamer oder gar nicht.[37]

Das Bot-Netzwerk selbst wächst ständig, indem es das Internet nach potenziellen Bots durchsucht. Werden geeignete Kandidaten gefunden, werden diese an den Report Server gemeldet. Der Report Server veranlasst die Assimilation der Kandidaten über den Malware Loader.

2.4. Advanced Persistent Threats

Advanced Persistent Threats beschreiben eine spezielle Angriffsmethodik bei Cyberattacken bzw. eine spezielle Motivation hinter diesen. Ein Advanced Persistent Threat (APT) liegt nach der Definition des Bundesamts für Sicherheit in der Informationstechnik (BSI) dann vor, wenn ein gut ausgebildeter, typischerweise staatlich gesteuerter Angreifender zum Zweck der Spionage oder Sabotage über einen längeren Zeitraum hinweg sehr gezielt ein Netz oder System angreift, sich unter Umständen darin bewegt und/oder ausbreitet und so Informationen sammelt oder Manipulationen vornimmt.[38]

Derartige Angriffe richten sich überwiegend gegen Unternehmen und benötigen i.d.R. entsprechend große Ressourcen. Das Hauptziel von Advanced Persistent Threats ist meist der Diebstahl von geistigem Eigentum wie Patente, innovative Designs oder andere vertrauliche Daten.[39]

Die Unterschiede zwischen „normalen" Cyberattacken und Advanced Persistent Threats lassen sich auch gut an der Dauer solcher Attacken festmachen. Nach einer Untersuchung des Unternehmens FIREEYE betrug die durchschnittliche Verweildauer von Angreifern im Unternehmen bis zur Aufdeckung der Cyberattacke im Jahr 2019 rd. 56 Tage.[40] In letzter Zeit verschwimmt dieses Unterscheidungskriterium aber zusehends, da sich mittlerweile auch Ramsomeware-Attacken wochenlang in den internen Netzwerken abspielen können.[41]

Technisch greifen Advanced Persistent Threats auf die in diesem Kapitel erläuterten verschiedenen Angriffsvektoren und Werkzeuge zurück. Ausgangspunkt für Advanced Persistent Threat-Angriffe waren früher meist infizierte E-Mail-Anhänge oder Links auf Schadcode-Websites. Mittlerweile variieren die Angriffsvektoren aber zunehmend. Zu den Angriffsvektoren zählen beispielsweise die Kompromittierung von legitimen Software-Produkten, die Ausnutzung von Schwachstellen in Fernwartungsdiensten, das Wiederverwenden von ausgespähten Zugangsdaten oder die Nutzung der Infrastruktur und Zugangsdaten von Zulieferern, um die eigentlichen Ziele zu kompromittieren. Eine relativ neue Methode stellt die Kompromittierung von Unternehmensroutern[42] dar.[43]

Der Ablauf von Advanced Persistent Threats lässt sich idealtypisch anhand des folgenden Zyklus beschreiben:[44]

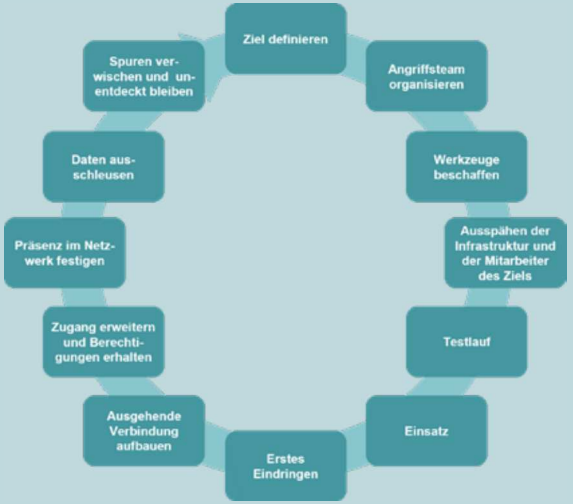

Abbildung 4: The Advanced Threat Lifecycle (angelehnt an: 5 Warning Signs of Advanced Persistent Threat | Tips to Prevent APT | Kaspersky)

Typische Warnhinweise für Advanced Persistent Threats können sein:[45]

- **Spear-Phishing-Attacken**: Diese werden häufig genutzt, um Zugang zum Netzwerk des Unternehmens zu bekommen. Ziel ist es, vertrauliche Informationen wie Passwörter zu sammeln oder die Opfer dazu zu verleiten, Links und Anhänge mit Malware zu öffnen.

- **Ungewöhnliche Logins**: Wenn sich Angreifer im System anmelden, kann es zu Auffälligkeiten kommen. Beispielsweise werden verstärkt Logins zu ungewöhnlichen Uhrzeiten registriert.

- **Identifizierung von Backdoor-Trojanern**: Hacker nutzen oftmals Backdoor-Trojaner, um sich fortlaufenden Zugang zu Systemen zu sichern.

- **Ungewöhnliche Datenflüsse**: Advanced Persistent Threats haben ein bestimmtes Ziel. Werden ungewöhnliche Datenflüsse innerhalb des Netzwerks registriert (z.B. Verschiebung von großen Datenmengen), kann dies ein Anzeichen von Advanced Persistent Threats sein.

- **Ungewöhnlich große Datenpakete**: Um Daten aus dem Netzwerk hinaus zu schleusen werden diese i.d.R. an einem Ort gesammelt und dort komprimiert. Große Datenpakete an unüblichen Speicherstellen können ein Anzeichen für Cyberattacken sein.

3. WELCHE SCHUTZMASSNAHMEN GIBT ES GEGEN CYBERATTACKEN?

3.1. Schutzziele

Cyberattacken haben, wie im vorigen Kapitel aufgezeigt, unterschiedliche Zielsetzungen. Aus den Zielsetzungen von Cyberangriffen können Schutzziele für den Aufbau und die Organisation von Schutzmaßnahmen abgeleitet werden. Beispielsweise steckt hinter Phishing-Attacken oftmals die Motivation, Zugriff auf vertrauliche Informationen zu erlangen. Das korrespondierende Schutzziel ist die Wahrung der Vertraulichkeit der Daten. Nur wenn Schutzmaßnahmen konsequent anhand von Schutzzielen ausgerichtet werden, können diese auch wirksam sein. Die IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1) benennt folgende elementare Schutzziele:[46]

- **Vertraulichkeit**: Das Schutzziel Vertraulichkeit verlangt, dass Daten nicht unberechtigt weitergegeben oder veröffentlicht werden.

- **Integrität**: Das Schutzziel Integrität ist dann erfüllt, wenn die Daten korrekt und unverändert sind.

- **Verfügbarkeit**: Verfügbarkeit verlangt zum einen, dass das Unternehmen zur Aufrechterhaltung des Geschäftsbetriebs die ständige Verfügbarkeit der IT-Infrastruktur, der IT-Anwendungen sowie der Daten gewährleistet. Zum anderen müssen die IT-Infrastruktur, die IT-Anwendungen und Daten sowie die erforderliche IT-Organisation in angemessener Zeit funktionsfähig bereitstehen.

- **Autorisierung**: Autorisierung bedeutet, dass nur im Voraus festgelegte Personen auf Daten zugreifen können (autorisierte Personen) und dass nur sie die für das System definierten Rechte wahrnehmen können.

- **Authentizität**: Authentizität ist gegeben, wenn ein Geschäftsvorfall einem Verursacher eindeutig zuzuordnen ist.

- **Verbindlichkeit**: Unter Verbindlichkeit wird die Eigenschaft von IT-gestützten Verfahren verstanden, gewollte Rechtsfolgen bindend herbeizuführen. Transaktionen dürfen durch den Veranlasser nicht abstreitbar sein, weil beispielsweise der Geschäftsvorfall nicht gewollt ist.

Das Zusammenwirken der Schutzziele lässt sich am Beispiel einer Online-Banking-Überweisung gut illustrieren.

Will ein Kunde eine Überweisung über sein Online-Banking vornehmen, so muss er sich zuerst mit seinem Account anmelden. Dies bedingt, dass das Online-Banking auch aufgerufen werden kann (Verfügbarkeit). Für die Anmeldung gibt er seine Anmeldeinformationen ein und diese werden vom System überprüft. Nur wenn er die richtigen Anmeldeinformationen eingibt (Autorisierung), erhält er Zugriff auf das Online-Banking und die dort hinterlegten Daten (Vertraulichkeit). Durch Maßnahmen wird im Hintergrund sichergestellt, dass die ihm angezeigten Daten korrekt sind (Integrität). Nimmt er nun eine Überweisung vor, muss er diese i.d.R. im Wege einer zweifachen Autorisierung bestätigen (Verbindlichkeit), z.B. durch eine entsprechende TAN (Autorisierung). Die Überweisung wird durch die IT-Systeme mit einem entsprechenden Datensatz zum Geschäftsvorfall versehen, um eine spätere Identifizierung und Zuordnung zu gewährleisten (Authentizität).

Zur Erreichung der Schutzziele bedarf es einer Vielzahl an organisatorischen und technischen Maßnahmen. Die wichtigsten technischen Maßnahmen werden nachfolgend vorgestellt. Zu beachten ist, dass die Wirksamkeit der technischen Maßnahmen stets von der Einbettung in den organisatorischen Gesamtkontext abhängig ist. Nur wenn die einzelnen Maßnahmen sinnvoll auf die betrieblichen Prozesse abgestimmt sind und die Mitarbeiter das notwendige Bewusstsein für Cyberrisk an den Tag legen bzw. entsprechend geschult werden, können die Schutzziele erreicht werden.

3.2. Firewalls

Eine wichtige Komponente beim Schutz vor Cyberattacken sind Firewalls. Firewalls dienen als Sicherungssystem, um ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Zugriffen zu schützen. Firewalls sind regelbasiert. Sie sind selbst nicht in der Lage, Angriffe auf ein Netzwerk zu erkennen. Um die grundlegende Funktionsweise einer Firewall zu verstehen, hilft ein Verständnis des ISO/OSI-Referenzmodells.[47]

Das ISO/OSI-Referenzmodell dient der Strukturierung von Aufgaben innerhalb eines Rechnernetzes. Die Aufgaben sind sehr unterschiedlich und reichen von der Kodierung einzelner Bits bis hin zur Steuerung von Netzwerkanwendungen. Das ISO/OSI-Referenzmodell teilt diese Aufgaben in ein Schichtenmodell ein. Insgesamt umfasst das Modell sieben Schichten, die nach ihrer Entfernung zur Hardware sortiert sind. Jede Schicht kann nur Dienste der darunterliegenden Schicht in Anspruch nehmen und stellt selbst wiederum Dienste für die nächsthöhere Schicht zur Verfügung.

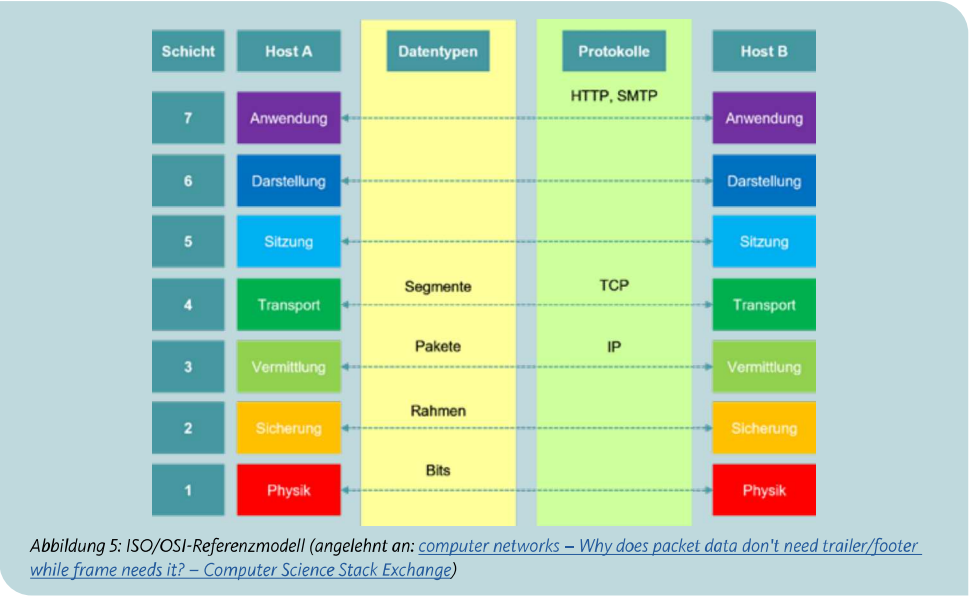

Abbildung 5: ISO/OSI-Referenzmodell (angelehnt an: computer networks – Why does packet data don't need trailer/footer while frame needs it? – Computer Science Stack Exchange)

Die Aufgaben der einzelnen Schichten sind:

- **Physik**: Die physikalische Schicht regelt die Kodierung und Übertragung einzelner Bits auf einem Übertragungskanal. Hierzu werden die Bits in ein zum Medium passendes Signal umgewandelt.

- **Sicherung**: Die Sicherungsschicht stellt für die darüberliegenden Schichten sicher, dass Datenblöcke (Rahmen) zu einem Empfänger in demselben physikalischen Netz zugestellt werden können. Hierfür werden die Datenpakete der darüberliegenden Schichten in Frames segmentiert.

- **Vermittlung**: Die Vermittlungsschicht sorgt bei leitungsorientierten Diensten für das Schalten von Verbindungen und bei paketorientierten Diensten für die Weitervermittlung von Datenpaketen sowie die Stauvermeidung. Die Datenübertragung geht in beiden Fällen jeweils über das gesamte Kommunikationsnetz hinweg und schließt die Wegsuche (Routing) zwischen den Netzwerkknoten ein. Diese Funktionen werden im Internet Protocol (IP) geregelt.

- **Transport**: Zu den Aufgaben der Transportschicht zählt es, Datenströme zu segmentieren, d.h. in Pakete aufzuteilen, die über die Vermittlungsschicht zum Zielknoten (Empfänger) geleitet werden können und die Sicherstellung einer fehlerfreien Übertragung dieser Segmente. Diese Aufgaben werden u.a. anhand des Transmission-Control-Protocols (TCP) abgearbeitet.

- **Sitzung**: Eine Sitzung ist ein andauernder, aber nicht zwingend kontinuierlicher Datenaustausch zwischen Client und Server. In der Sitzungsschicht werden Maßnahmen getroffen, um eine Sitzung zu beginnen, während ihrer Laufzeit zu verwalten und schließlich zu beenden.

- **Darstellung**: Die Darstellungsschicht sorgt für die systemunabhängige Präsentation der Daten. Hier werden empfangene Daten für die Präsentation aufbereitet und zu sendende Daten in die für die Übertragung geeigneten Formate überführt. Außerdem werden der Darstellungsschicht auch die Aufgaben der Verschlüsselung und Komprimierung zugeordnet.

- **Anwendung**: Die Anwendungsschicht bietet Applikationen[48] die Schnittstelle zur Kommunikation über Netzwerke.

Die Struktur der übermittelten Daten stellt sich wie folgt dar:

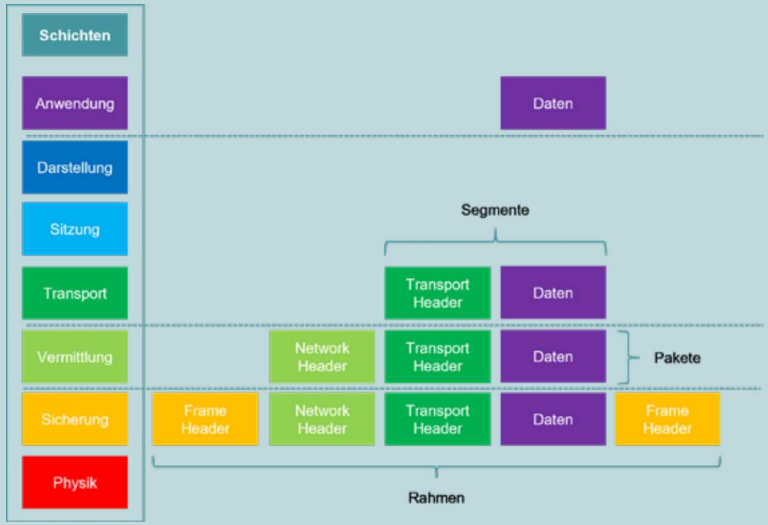

Abbildung 6: Struktur der Daten im ISO/OSI-Referenzmodell (angelehnt an: EmbeddedGeeKs – Encapsulation)

Die hinter einer Firewall stehenden technischen Konzepte setzen an der Vermittlungsschicht, der Transportschicht und an der Anwendungsschicht an. Die wichtigsten technischen Konzepte sind:

Paketfilter

Die Grundfunktion einer Firewall ist ein Paketfilter, der auf der Vermittlungsschicht arbeitet. Der Paketfilter arbeitet nach statischen Regeln und überprüft jedes Datenpaket einzeln, kann aber keine Verbindungen zu anderen Paketen herstellen. Je nach Status der Überprüfung werden Pakete ihren Zielen entweder zugeführt oder geblockt. Die Überprüfung erfolgt anhand von IP-Adressen, Pakettypen oder Portnummern.

Exkurs: Internet Protocol (IP)
IP ist ein verbindungsloses paketvermittelndes Protokoll für logische Netzwerke auf Ebene der Vermittlungsschicht, das auf der Sicherungsschicht aufsetzt. Es gruppiert Knoten mittels logischer Adressen in Netzwerke mit gemeinsamen Adressteilen und erlaubt so effiziente Wegefindung.

Die von IP vergebenen Adressen werden aktuell in zwei Versionen eingesetzt:
- IPv4 mit 32-Bit-Adressen
- IPv6 mit 128 Bit-Adressen

Exkurs: Ports
IP-Adressen bestimmen einen Knoten im Netzwerk eindeutig, jedoch muss ein eintreffendes Paket letztlich einer der laufenden Anwendungen auf dem Knoten zugeordnet werden können. Hierzu wird auf der Transportschicht jeder lokalen Anwendung ebenfalls eine Adresse zugeordnet. Diese Adresse ist eine 16-Bit-Zahl und wird als Port bezeichnet.

Beispiele für Standard-Ports sind:
- HTTP-Server: Port 80
- SMTP-Server: Port 25
- DNS-Server: Port 53

Die Kombination aus IP-Adresse und Port-Nummer wird als Socket bezeichnet.

Exkurs: Transmission-Control-Protocol (TCP)
TCP ist ein Netzwerkprotokoll, das definiert, auf welche Art und Weise Daten (Segmente) zwischen Knoten im Netzwerk ausgetauscht werden sollen. TCP setzt in den meisten Fällen auf das IP auf.

Der Aufbau einer gültigen TCP-Verbindung ist an die Voraussetzung geknüpft, dass beide involvierten Endpunkte bereits über eine eindeutige IP-Adresse (IPv4 oder IPv6) verfügen und den gewünschten Port für die Datenübertragung deklariert und freigegeben haben. Während erstere als Identifikationsmerkmal fungiert, ist letzterer für die Zuordnung der Verbindungen zu den konkreten Client- und Serveranwendungen durch das Betriebssystem relevant.

Protokolltypisch befinden sich die entscheidenden Daten, die für den Verbindungsaubau und die Datenübertragung mit TCP benötigt werden, im Header eines TCP-Pakets. Diese Kopfdaten (auch Steuerinformationen) stehen der zu übertragenden Nutzlast (Payload) voran und haben typischerweise eine Größe von 20 Byte, gefolgt von bis zu 40 Byte Zusatzinformationen, die optional sind und nicht in allen Paketen Verwendung finden.

Stateful Packet Inspection

Stateful Packet Inspection stellt eine Weiterentwicklung von einfachen Paketfiltern dar und kann als dynamische Art der Paketfilterung verstanden werden. Stateful Packet Inspection-Firewalls entscheiden auf Grundlage von Status, Port und Protokoll, ob der Datenverkehr zugelassen oder blockiert wird. Hierzu wird der mitgelieferte Header ausgewertet. Stateful Packet Inspection-Firewalls überwachen nach dem Öffnen einer Verbindung alle Aktivitäten, bis die Verbindung wieder geschlossen wird. Filterentscheidungen werden auf Grundlage sowohl von durch den Administrator festgelegten Regeln als auch auf Basis des Kontexts getroffen. „Kontext" bezieht sich hierbei auf Informationen über vorherige Verbindungen und Pakete, die zur selben Verbindung gehören.[49] Das Regelwerk von Stateful Packet Inspection ist dabei relativ einfach. Es wird davon ausgegangen, dass eine HTTP-Anfrage nur von einem Rechner an einen anderen erfolgen kann. Da der dynamische Paketfilter die Kommunikationsverbindung speichert, darf nur der zweite Computer dem anfragenden Computer antworten. Mittels Stateful Packet Inspection lassen sich auch DDoS-Attacken erkennen.

Deep Packet Inspection

Während bei der Stateful Packet Inspection nur der Header hinsichtlich der relevanten Verkehrsinformationen ausgewertet wird, wird bei Deep Packet Inspection auch der Payload[50] ausgewertet, in dem sich der Informationsinhalt befindet. Der Router erkennt hierdurch die Datei und prüft, ob es sich um eine Text-, Grafik-, Audio- oder Videodatei handelt. Diese Nutzdaten werden durch Zusatzgeräte analysiert und interpretiert. Mittels Deep Packet Inspektion kann neben DDoS-Attacken auch Schadsoftware erkannt werden.

Proxy-Firewall

Bei einer Proxy-Firewall werden sog. Proxy-Server als Gateway eingesetzt. Sie arbeiten auf der Anwendungsschicht zwischen internen Clients und Webservern und können die Zugriffe auf bestimmte Websites und Webservices kontrollieren und begrenzen.

Eine Proxy-Firewall kann den gesamten Datenverkehr auf der Anwendungsschicht überwachen. Sie arbeitet mit Stateful Packet Inspection und Deep Packet Inspection und überwacht den eingehenden Datenverkehr.

Proxy-Firewalls arbeiten als Vermittlungsinstanz und verhindern den direkten Kontakt zwischen den verschiedenen Systemen. Sie haben eigene IP-Adressen und empfangen darüber die Datenpakete, die sie anschließend über eine neue Verbindung an die Zieladresse weitervermitteln. Proxy-Firewalls verfügen über umfangreiche Monitoring-Funktionen, in denen sie die Verbindungen und die Sicherheitsprobleme für das Sicherheitsmanagement dokumentieren.[51]

Contentfilter

Contentfilter suchen in den Datenströmen nach Keywords, nach bestimmten Dateitypen oder verdächtigen E-Mail-Anhängen. Die Überprüfung des Datenverkehrs dient beispielsweise dazu, Websites mit unerwünschtem oder jugendgefährdendem Inhalt zu sperren, aber auch zur Analyse von Datenströmen, die aus Unternehmen herausgehen und für Datenverlust sorgen. Contentfilter überwachen die Übergänge zwischen dem Internet und den Unternehmensnetzen und erhöhen dadurch die Content-Sicherheit. Bei direkter Internetverbindung sind sie auf dem Client installiert.

3.3. Intrusion-Detection- und Prevention-Systeme

Während Firewalls dazu dienen, Angreifern den Zugang zum Netzwerk so schwer wie möglich zu machen, dienen Intrusion-Detection- und Prevention-Systeme der Eindringungserkennung und ggf. dem Stoppen erkannter Vorfälle. Während Intrusion-Detection-Systeme sich darauf beschränken, verdächtige Vorfälle zu erkennen und zu melden, versuchen Intrusion-Prevention-Systeme zusätzlich Gegenmaßnahmen zu ergreifen, um das Netz zu schützen.

Derartige Gegenmaßnahmen können beispielsweise das Ändern von Firewall-Regeln sein, wodurch verdächtigen Netzwerkstationen der Zugriff auf die Unternehmensressourcen untersagt wird.

Sowohl Intrusion-Detection-Systeme als auch Intrusion-Prevention-Systeme werden danach unterschieden, ob sie einzelne Server überwachen (s.g. „Host-based Intrusion Detection Systems“) oder das ganze Netzwerk (s.g. „Network Intrusion Detection Systems“) überwachen. Host-based Intrusion-Detection-Systeme überprüfen fortlaufend, ob Angreifer wichtige Betriebssystemdateien auf einem Rechner kompromittieren, während Network Intrusion-Detection-Systeme den Netzwerkverkehr analysieren.

Eine weitere Unterscheidung von Intrusion-Detection- und Prevention-Systemen kann hinsichtlich der Funktionsweise der Eindringungserkennung vorgenommen werden. Bei Signatur-basierten Lösungen wird der Datenverkehr auf bekannte Muster von Cyberattacken ausgewertet. Werden solche Muster festgestellt, erfolgen eine Warnmeldung an die zuständigen Stellen und ein Eintrag in eine Datenbank. Dem gegenüber stehen Intrusion-Detection- und Prevention-Systeme, die auf statistische Analysen setzen. Hierbei wird ein Idealmodell des Datenverkehrs angenommen, der dem täglichen Betrieb im Netzwerk entspricht. Weicht der registrierte Datenverkehr von diesem Idealmodell ab, erfolgen wiederum eine Warnmeldung und ein Eintrag in eine Datenbank. Der Vorteil von auf statistischen Analysen basierenden Intrusion-Detection- und Prevention-Systemen liegt darin, dass auch bislang unbekannte Angriffsmuster erkannt werden. Gleichzeitig sind diese Systeme jedoch wesentlich wartungsaufwendiger.

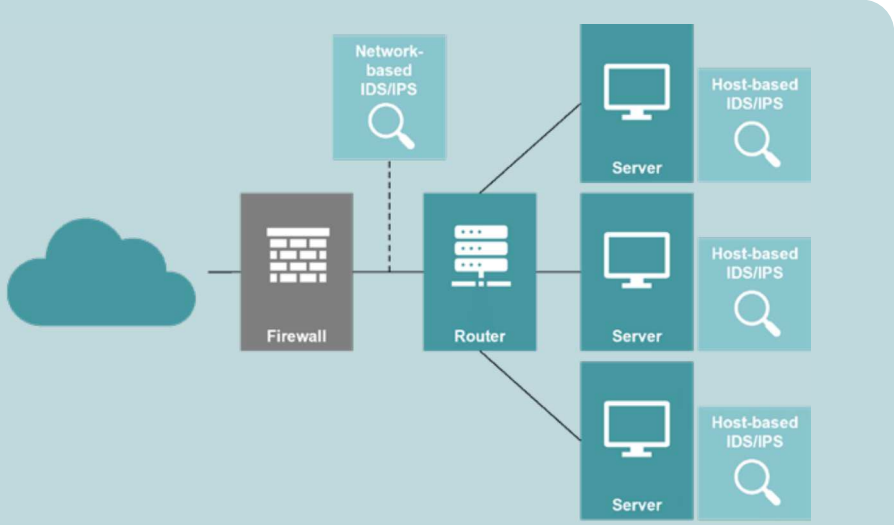

Abbildung 7: Network Intrusion Detection System (angelehnt an: What is IDS and IPS? | Juniper Networks)

3.4. Anti-Viren-Programme

Unter Anti-Viren-Programmen wird die Vielzahl an Softwarelösungen verstanden, die Malware aufspüren, blockieren und wenn möglich beseitigen soll. Anti-Viren-Programme basieren dabei auf ähnlichen Grundfunktionen wie Intrusion-Detection- und Prevention-Systeme. So stützen sich auch Anti-Viren-Programme i.d.R. auf die Signaturerkennung bekannter Schadsoftware bzw. auf statistische Analysen.

Wichtig beim Einsatz von Anti-Viren-Programmen ist, dass diese allein keinen wirksamen Schutz vor Cyberattacken darstellen. Dies liegt einerseits daran, dass sie Angriffe nicht von vornherein verhindern. Andererseits können die meisten Anti-Viren-Programme nur bereits bekannte Schadprogramme erkennen. Ein weiteres Problem besteht in dem Umstand, dass sich bestimmte Viren tarnen können (vgl. Kapitel 2.2.2.) und sich somit einer Entdeckung durch Anti-Viren-Programme entziehen.

Die von Anti-Viren-Programmen genutzten Scanner lassen sich grundsätzlich unterschieden in:

- **Echtzeitscanner**: Echtzeitscanner sind im Hintergrund aktiv und scannen alle Dateien, Programme, den Arbeitsspeicher und ggf. den HTTP- und FTP-Verkehr. Hierzu werden so genannte Filtertreiber verwendet, die die Schnittstelle zwischen dem Echtzeitscanner und dem Dateisystem bereitstellen. Bei Auffälligkeiten wird der Nutzer nach einer Reaktion gefragt. Eine solche Reaktion kann beispielsweise das Blockieren des Zugriffs, das Löschen der Datei oder das Verschieben in die Quarantäne sein.

- **Manuelle Scanner**: Manuelle Scanner bezeichnen Dateiscanner, welche die auf dem System enthaltenen Dateien scannen. Sie müssen entweder manuell oder zeitgesteuert gestartet werden.

- **Online-Scanner**: Hierbei handelt es sich um Scanner, die nicht auf dem System installiert sind, sondern nur im On-Demand-Modus arbeiten. Sie werden oftmals eingesetzt, um einzelne verdächtige Dateien nochmals zu untersuchen.

Anti-Viren-Programme standen in den letzten Jahren verstärkt in der Kritik. Schuld hieran war neben den vergleichsweise schlechten Entdeckungsquoten vor allem die Tatsache, dass Anti-Viren-Softwarelösungen oftmals selbst Schwachstellen enthielten, welche zum Ziel von Cyberattacken wurden. Das BSI veröffentlicht hierzu auf seiner Homepage regelmäßig Warnmeldungen. Zudem veröffentlichen Angreifer regelmäßig falsche Anti-Viren-Programme, die den Programmen seriöser Anbieter nachgebaut sind. Durch diese wird versucht, die Nutzer auszuspähen oder Malware zu installieren.

Trotz der Kritik an Anti-Viren-Programmen empfiehlt das BSI grundsätzlich den Einsatz dieser Programme und hält weiterführende Informationen hierzu vor.[52]

3.5. Backups

Eine der wichtigsten Maßnahmen zur Erreichung der Schutzziele ist der Einsatz von Backups. Selbst die besten technischen Vorkehrungen bieten keinen 100%-igen Schutz vor Cyberattacken. Regelmäßige und schnell verfügbare Backups können die Auswirkungen von Cyberattacken begrenzen, indem Systeme zeitnah wiederhergestellt werden können. Die Bandbreite von möglichen Backups reicht von Magnetbändern im Stahltresor bis hin zu modernen Cloudlösungen.

Damit Backups ihre risikobegrenzende Wirkung entfalten können, müssen sie bestimmte Anforderungen erfüllen. Das Bundesamt für Sicherheit in der Informationstechnik beschreibt in der Veröffentlichung „CON.3: Datensicherungskonzept" spezifische Bedrohungen und Schwachstellen im Hinblick auf die Datensicherung. Diese umfassen:[53]

- **Fehlende Datensicherung**: Die Datensicherung muss regelmäßig erfolgen. Hierbei ist zu beachten, dass ggf. mehr als ein Backup benötigt wird, da eine Cyberattacke ggf. länger nicht bemerkt wurde und deshalb auf einen weiter in der Vergangenheit liegendes Backup zurückgegriffen werden muss. Zudem ist zu prüfen, ob die Datensicherung auch tatsächlich erfolgt, oder ob eventuell Fehler aufgetreten sind.

- **Fehlende Wiederherstellungstests**: Eine regelmäßige Sicherung von Daten gewährleistet nicht automatisch, dass diese Daten auch wiederhergestellt werden können. Deshalb ist regelmäßig zu testen, ob sich die Systeme aus den gesicherten Daten auch wiederherstellen lassen.

- **Ungeeignete Aufbewahrung der Datenträger von Datensicherungen**: Durch eine ungeeignete Aufbewahrung können Backups entweder zerstört werden, oder in die Hände von unberechtigten Personen gelangen. Die daraus gewonnenen Informationen lassen sich ggf. für Cyberattacken und andere kriminelle Handlungen nutzen. Backups sollten deshalb genauso umsichtig geschützt werden wie die Originaldaten.

- **Fehlende oder unzureichende Dokumentation**: Ein wirksames Datensicherungskonzept erfordert eine entsprechende Dokumentation. Ohne diese lassen sich Daten ggf. nicht in der vorgegebenen Zeit einspielen bzw. wiederherstellen.

- **Missachtung gesetzlicher Vorschriften**: Bei Missachtung gesetzlicher Regelungen, bspw. bei Verstößen gegen die Datenschutzgrundverordnung, drohen teils erhebliche Bußgelder.

- **Unsichere Cloud-Anbieter für Online-Datensicherungen**: Cloud-Anbieter für Online-Datensicherungen können ein lohnenswertes Ziel für Cyberkriminelle darstellen. Zudem können die Schnittstellen zwischen Unternehmen und Cloud-Anbieter ein Einfallstor für Cyberkriminelle bieten.

- **Ungenügende Speicherkapazitäten**: Ungenügende Speicherkapazität kann dazu führen, dass Backups nicht durchgeführt werden bzw. noch benötigte Backups überschrieben werden.

- **Unzureichendes Datensicherungskonzept**: Datensicherungskonzepte müssen auf die individuellen Gegebenheiten und Anforderungen abgestimmt werden. Beispielweise ist eine Sicherung auf Magnetbändern für Daten, die schnell verfügbar sein müssen, ungeeignet.

4. STANDORTBESTIMMUNG: WELCHE BEDEUTUNG HABEN CYBERATTACKEN IN DEUTSCHLAND?

Das Thema Cyberrisk ist eines der Top-Themen für Unternehmen weltweit. Im Allianz Risikobarometer 2021 wurden die Risiken aus Cyberattacken auf Platz 3 der wichtigsten weltweiten Unternehmensrisiken genannt.[54] Die Top-Platzierung aus dem Vorjahr wurde nur aufgrund der Auswirkungen der Coronavirus-Pandemie verfehlt.

Auch in Deutschland stellen Cyberattacken für Unternehmen eine komplexe und ernstzunehmende Herausforderung dar. Einen guten Überblick über diese Herausforderungen bietet der jährliche Bericht des BSI zur Lage der IT-Sicherheit in Deutschland.[55] Das BSI beschreibt die Lage in Deutschland hierin als „angespannt bis kritisch".[56] Die Bedrohungslage ist dabei vielschichtig. Angreifer nutzten Schadprogramme für cyberkriminelle Massenangriffe ebenso wie für gezielte Angriffe auf ausgewählte Opfer. Im Berichtsjahr 2021 hat die Bedrohung durch mehrstufige Erpressungsmodelle eine neue Qualität erreicht. Zudem wurden mehrere, teils kritische Schwachstellen in Software-Produkten identifiziert, die Angreifer für Schadprogramm-Angriffe oder Datendiebstahl ausnutzen konnten. Verstärkt nutzten Angreifer auch den Faktor „Mensch" als Einfallstor für Angriffe. Hierbei griffen sie auf Social-Engineering-Methoden zurück. Zu den wichtigsten Trends in 2021 gehören:

- Im Berichtsjahr haben sich Cybererpressungen zur größten Bedrohung entwickelt. Bekannte cyberkriminelle Lösegelderpressungen (Ransomware-Attacken) wurden um Schweigegelderpressungen unter Androhung der Veröffentlichung von Daten sowie Schutzgelderpressungen unter Androhung von DDoS-Angriffen erweitert. Damit ist bei Ransomware-Attacken auch nach Zahlung von Lösegeld oder Schweigegeld grundsätzlich davon auszugehen, dass Daten dauerhaft kompromittiert sind.

- Ransomware-Attacken wurden zudem gezielter und richteten sich vermehrt gegen zahlungskräftige Opfer, um so möglichst hohe Lösegelder zu erpressen (sog. Big Game Hunting).

- Als weitere schwer zu kontrollierende Angriffsart haben sich Software-Supply-Chain-Angriffe herausgestellt. Dabei fügen Angreifer im Netzwerk eines Softwareherstellers Malware in legitime Softwareprodukte ein, welche anschließend über Software-Installationsdateien oder -Updates in die Netzwerke der Kunden des Softwareherstellers gelangt und so eine Vielzahl von Netzwerken und Systemen infizieren kann.

- Auch wenn im Januar 2021 das bisher dominierende Schadprogramm Emotet zerschlagen wurde, ist die Gefahr durch Malware nicht gebannt. Insgesamt wurde ein starker Zuwachs von Malware, insbesondere um den Jahreswechsel verzeichnet (der Tageszuwachs lag im Februar 2021 durchschnittlich bei 553.000 Varianten und markiert damit einen neuen Höchststand).

- Im März 2021 wurde eine kritische Schwachstelle in Microsoft Exchange bekannt. Auf Grund der hohen Verbreitung angreifbarer Server und der leichten Ausnutzbarkeit durch vorgefertigte Exploit-Kits wurde die Lage als „extrem kritisch" eingestuft und die zweithöchste Krisenstufe ausgerufen.

- Phishing-Attacken und Social-Engineering-Angriffe griffen, wie bereits im Vorjahr, zunehmend die Coronavirus-Pandemie auf. Zudem hat sich die Angriffsfläche durch die pandemiebedingte verstärkte Nutzung von Remote-Zugängen, VPN und Videokonferenzsystemen erhöht.

Von übergeordneter Bedeutung für die Cyberrisikosituation in Deutschland waren die Auswirkungen der Coronavirus-Pandemie. Während einerseits im privaten Bereich verstärkt digitale Angebote zur Freizeitgestaltung genutzt und Transaktionen zunehmend online vorgenommen werden, sehen sich andererseits Unternehmen gezwungen, ihre bewährten Arbeitsabläufe neu zu organisieren und zu digitalisieren. Doch Home-Office-Maßnahmen und veränderte Kundenkontaktpunkte schützen ggf. zwar vor Ansteckung, sie bieten aber auch Cyberkriminellen neue Angriffspunkte. Das Bundeskriminalamt hat aufgrund dessen in Zeiten der Corona-Pandemie eine Sonderauswertung zum Thema Cybercrime vorgenommen. Nach den Erkenntnissen des Bundeskriminalamts wurden seit Beginn der Pandemie zunehmend Cyberangriffe festgestellt. Hierbei greifen Cyberkriminelle bei ihren Aktivitä-

ten auf bewährte Modi Operandi und Malware-Familien zurück. Die Coronavirus-Pandemie zeigt dabei einmal mehr auf, dass die Täter sehr rasch gesellschaftliche Entwicklungen aufgreifen und zu kriminellen Zwecken ausnutzen. Der Großteil der Bedrohung geht dabei weiterhin von Phishing und maliziösen Domains aus. Zudem wurden verstärkt Hinweise registriert, dass Kriminelle die Coronavirus-Pandemie zur Verbreitung der Schadsoftware TrickBot ausnutzen. Die thematische Bedrohungslage im Cyberbereich wird als „andauernd hoch" eingestuft.[57]

Diese sehr auf die Angreifer fokussierte Sichtweise wird durch eine Studie des Kriminologischen Forschungsinstituts Niedersachsen e.V. aus dem Jahr 2020 ergänzt, welche u.a. durch das Bundesministerium für Wirtschaft und Energie gefördert wurde. Diese unter dem Titel „Cyberangriffe gegen Unternehmen in Deutschland" veröffentlichte Studie spiegelt die Ergebnisse einer repräsentativen Befragung von 5.000 Unternehmen wider. Im Rahmen der Studie wurde u.a. untersucht, welche IT-Sicherheitsmaßnahmen gegen Cyberangriffe die befragten Unternehmen eingerichtet haben. Hierbei wurde zwischen organisatorischen und technischen Sicherheitsmaßnahmen unterschieden. Während sich bei den organisatorischen Vorkehrungen ein stark heterogenes Bild abzeichnete, wiesen die technischen Vorkehrungen durchweg einen hohen Mindeststandard auf. Defizite bei den organisatorischen Vorkehrungen wurden insbesondere bei kleinen Unternehmen (10–49 Beschäftigte) bzw. branchenabhängig (z.B. im Baugewerbe) bezüglich fehlender schriftlich fixierter Richtlinien zur Informations- bzw. IT-Sicherheit sowie zum Notfallmanagement als auch zu regelmäßigen IT-Sicherheitsschulungen festgestellt. Große Unternehmen (> 500 Beschäftigte) und Unternehmen aus stark regulierten Branchen (z.B. Kreditinstitute) verfügten hingegen mehrheitlich über derartige Regelungen. Bei den technischen Maßnahmen, wie Mindestanforderungen an Passwörter, regelmäßige Back-Ups, Einsatz von Firewalls und Antivirensoftware, regelmäßigen Updates und Patches, sowie der Limitierung von Zugangs- und Nutzungsrechten wurden keine signifikanten größen- bzw. branchenabhängigen Unterschiede festgestellt. Insgesamt kamen 84,9 % der befragen Unternehmen zum Schluss, dass sehr viel für die IT-Sicherheit getan wird.

Die Wichtigkeit von Vorkehrungen gegen Cyberattacken wurde innerhalb der Studie dadurch untermauert, dass 41,1% der befragten Unternehmen in den vorhergehenden zwölf Monaten mindestens einen Cyberangriff erlebt hatten, auf den reagiert werden musste, d.h. Angriffe, die automatisiert vereitelt oder gar nicht erkannt wurden, wurden hierbei nicht mitgezählt. Bei den großen Unternehmen (> 500 Beschäftigten) lag die Jahresprävalenzrate sogar bei 58,2%. Trotz dieser hohen Zahl an Cyberattacken und dem Umstand, dass Unternehmen das Thema Cyberrisk als bedeutende Bedrohung einschätzen, lag die Risikoeinschätzung dafür, in den nächsten Monaten selbst Opfer einer Cyberattacke zu werden, unter den Erfahrungswerten der Vergangenheit. Dies weist auf eine allgemeine Unterschätzung des individuellen Risikos hin.[58]

5. WELCHE ORGANISATIONEN WIDMEN SICH DER VERHINDERUNG VON CYBERRISK?

5.1. Überblick: Internationale Organisation

Eine Vielzahl an Organisationen beschäftigt sich mit der Verhinderung von Cyberrisk. Auch wenn einzelne Institutionen in diesem Bereich führend sind, mangelt es noch an einer internationalen einheitlichen Struktur. Zu den wichtigsten Organisationen weltweit in Bezug auf Cyberrisk gehören die in der Schweiz ansässige Internationale Organisation für Normung (ISO), das in den USA führende National Institute of Standards and Technology (NIST), in Europa die European Union Agency for Cybersecurity (ENISA) und in Bezug auf den Finanzsektor das in Basel ansässige Financial Stability Board (FSB) sowie die EBA.

Abbildung 8: Überblick internationale Organisationen (eigenerstellt)

5.1.1. Internationale Organisation für Normung

Die Internationale Organisation für Normung (ISO) ist eine internationale Nichtregierungsorganisation, zu der 165 nationale Normierungsorganisationen gehören. Sie erarbeitet internationale Normen in allen Bereichen mit Ausnahme der Elektrik und der Elektronik, für welche die Internationale elektrotechnische Kommission (IEC) zuständig ist, und der Telekommunikation, für die die Internationale Fernmeldeunion (ITU) zuständig ist. Gemeinsam bilden diese drei Organisationen die World Standards Cooperation (WSC).

Für den Bereich Informationssicherheitsmanagement gehören die gemeinsamen Standards der ISO und der IEC zu den weitverbreitetsten Standards. Die Standards werden unter dem Nummernkreis „2700x Information technology – Security techniques" zusammengefasst. Sie umfassen:

- **ISO/IEC 27000** – Information security management systems – Overview and vocabulary
- **ISO/IEC 27001** – Information security management systems – Requirements; hervorgegangen aus Teil 2 des British Standard BS 7799[59]
- **ISO/IEC 27002** – Code of practice for information security management; hervorgegangen aus Teil 1 des British Standard BS 7799 und der ISO/IEC 17799[60]
- **ISO/IEC 27003** – Information security management systems – Implementation Guidelines
- **ISO/IEC 27004** – Information security management measurements
- **ISO/IEC 27005** – Information security risk management

5.1.2. National Institute of Standards and Technology

Das National Institute of Standards and Technology (NIST) ist eine US-amerikanische Bundesbehörde und stellt u.a. das Pendant zum Bundesamt für Sicherheit in der Informationstechnik dar. Das NIST wurde 1901 gegründet und ist mittlerweile Teil des U.S. Handelsministeriums. Aufgabe des NIST ist u.a. die Erarbeitung von Normungen und Standards. Sein Mess- und Prüflabor, das vielfältige Bereiche der Informatik, Mathematik, Statistik und Systemtechnik umfasst, ist die Grundlage des Cybersicherheitsprogramms von NIST. Das Cybersicherheitsprogramm von NIST zielt darauf ab, eine bessere Entwicklung und Anwendung praktischer, innovativer Sicherheitstechnologien und -methoden zu ermöglichen, um aktuelle und zukünftige Herausforderungen im Bereich der Computer- und Informationssicherheit zu bewältigen.

Das NIST hat mehrere Datensicherheitsstandards veröffentlicht. Zu nennen sind:

- **NIST 800-53**: Richtlinien für Sicherheitskontrollen und Datenschutzkontrollen in den Bereichen Anwendungssicherheit, Mobiles und Cloud Computing sowie Supply Chain Security
- **NIST 800-53/FI**: Standards für die Implementierung von FISMA[61]
- **NIST 800-30**: Richtlinien für die Durchführung von Risikobewertungen
- **NIST 800-171**: Richtlinien für die physische Sicherheit von Rechenzentren

Zudem hat das NIST im Jahr 2014 ein Cybersecurity Framework für Unternehmen veröffentlicht. Das Cybersecurity Framework gibt einen Überblick über Best-Practices im Bereich Cybersecurity.[62]

5.1.3. European Union Agency for Cybersecurity

Die European Union Agency for Cybersecurity (ENISA) ist eine Behörde der Europäischen Union und widmet sich der Erreichung eines hohen gemeinsamen Cybersicherheitsniveaus in ganz Europa. Die im Jahr 2004 gegründete Behörde gewann durch den im Jahr 2019 verabschiedeten EU Cybersecurity Act[63] enorm an Bedeutung. Ihre Aufgaben umfassen Maßnahmen zur Entwicklung und Umsetzung der Politik der Europäischen Union im Bereich Cybersicherheit, die Stärkung der Vertrauenswürdigkeit von IKT-Produkten, -Diensten und -Prozessen mit Cybersicherheitszertifizierungssystemen und die Zusammenarbeit mit den Mitgliedstaaten und EU-Organen. Ihr Ziel ist es, Europa auf die Cyberherausforderungen von morgen vorzubereiten.[64]

Im Bereich Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen fungiert die ENISA, entsprechend Artikel 8 der Verordnung (EU) 881/2019, als Standardsetter. Sie überwacht fortlaufend aktuelle Entwicklungen bei Normungen in diesem Bereich, evaluiert vorhandene Standards und entwickelt selbst entsprechende Normungen, sofern diese fehlen. Hierzu arbeitet die ENISA mit dem European Committee for Standardization (CEN), dem European Committee for Electrotechnical Standardization (CENELEC) und dem European Telecommunications Standards Institute (ETSI) zusammen. Bei CEN handelt es sich um den Zusammenschluss der Nationalen Normungsgremien von 34 europäischen Ländern. CEN bietet eine Plattform für die Entwicklung europäischer Normen und anderer technischer Dokumente in Bezug auf verschiedene Arten von Produkten, Materialien, Dienstleistungen und Prozessen.[65] CENELEC hingegen ist speziell für die Normung im Bereich elektrotechnische Technik zuständig.[66] ETSI wiederum befasst sich als regionale Normungsorganisation mit Telekommunikations-, Rundfunk- und anderen elektronischen Kommunikationsnetzen und -diensten.[67]

Die Aufgaben von ENISA umfassen aber nicht nur die Überwachung, Evaluierung und Entwicklung von Normungen im Bereich Cybersicherheit, sie ist auch für die Erarbeitung von Leitlinien für Cybersicherheitszertifizierungen zuständig. Zudem fungiert sie als zentraler Wissenspool für Bürger, Organisationen und Unternehmen. Dabei unterstützt sie die strategische Forschung im Bereich Cybersicherheit und fördert die internationale Zusammenarbeit.

5.1.4. Financial Stability Board

Das Financial Stability Board (FSB) ist ein internationales Gremium, welches das globale Finanzsystem überwacht und Empfehlungen ausspricht. Es wurde auf dem Gipfel der zwanzig wichtigsten Industrie- und Schwellenländer (G20) im April 2009 als Nachfolger des Financial Stability Forums eingerichtet. Das FSB hat seinen Sitz bei der Bank für Internationalen Zahlungsausgleich in Basel in der Schweiz. Neben Institutionen aus den G20-Staaten sind internationale Einrichtungen wie die Weltbank, die Europäische Zentralbank und die Europäische Kommission Mitglied.

Aufgaben des FSB sind u.a.:[68]

- Bewertung von Schwachstellen, die das globale Finanzsystem betreffen, und von regulatorischen und aufsichtsrechtlichen Maßnahmen, die zur Behebung dieser Schwachstellen ergriffen wurden.
- Strategische Überprüfungen von internationalen Standardsettern und Koordinierung von politischer Entwicklungsarbeit.
- Festlegung von Leitlinien für die Einrichtung und Unterstützung von Aufsichtsorganen.
- Unterstützung der Notfallplanung für das grenzüberschreitende Krisenmanagement, insbesondere im Hinblick auf systemrelevante Unternehmen.

Das FSB hat das Thema Cyberresilienz als ein Schlüsselelement für die Stabilität des Finanzsystems identifiziert. Im Jahr 2017 hat das FSB eine Bestandsaufnahme der Regulatorik, Leitlinien und der Aufsichtspraxis mit Bezug zu Cybersecurity im Finanzsektor durchgeführt. Ergebnis dieser Bestandsaufnahme war u.a. die Identifikation der Notwendigkeit, den Austausch zwischen den Aufsichtsbehörden und den Unternehmen zu verbessern. Hierfür hat das FSB im Jahr 2018 ein Cyberlexikon entwickelt. Zudem hat das FSB im Jahr 2018 beschlossen, eine Sammlung von Best Practices bezüglich der Reaktion auf Cyberangriffe zu erarbeiten, um die Risiken für die Finanzstabilität, welche von solchen Attacken ausgehen, zu begrenzen. Diese Best Practices wurden im April 2020 unter dem Titel „Effective Practices für Cyber Incident Response and Recovery“ zur Konsultation gestellt und im Oktober 2020 verabschiedet.[69]

5.1.5. Europäische Bankenaufsichtsbehörde

Die Europäische Bankenaufsichtsbehörde (EBA) ist eine unabhängige EU-Behörde, deren Aufgabe es ist, ein wirksames und kohärentes Maß an Regulierung und Beaufsichtigung im europäischen Bankensektor zu gewährleisten. Ihre übergeordneten Ziele bestehen in der Wahrung der Finanzstabilität in der EU und dem Schutz der Integrität, der Effizienz und des ordnungsgemäßen Funktionierens des Bankensektors.

Die EBA ist Bestandteil des Europäischen Systems der Finanzaufsicht (ESFS), dem drei Aufsichtsbehörden angehören: die Europäische Wertpapier- und Marktaufsichtsbehörde (ESMA), die Europäische Bankenaufsichtsbehörde (EBA) und die Europäische Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA). Außerdem zählen der Europäische Ausschuss für Systemrisiken (ESRB) sowie der Gemeinsame Ausschuss der Europäischen Aufsichtsbehörden und die nationalen Aufsichtsbehörden zum ESFS.[70]

Die EBA adressiert das Thema Cyberrisk in ihren EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken vom 28.11.2019. Diese Leitlinien legen Anforderungen an Kreditinstitute, Wertpapierfirmen und Zahlungsdienstleister (PSP) für das Management ihrer Informations- und Kommunikationstechnologie (IKT) und für die Beherrschung bzw. Abschwächung von Sicherheitsrisiken fest und zielen darauf ab, einen kohärenten und robusten Ansatz im gesamten Binnenmarkt zu gewährleisten. Diese Leitlinien traten am 30.06.2020 in Kraft. Die EBA-Leitlinien werden auf nationaler Ebene von den nationalen Aufsichtsbehörden adaptiert. So hat die BaFin die Vorgaben in ihrem Rundschreiben 10/2017 (BA) – Bankaufsichtliche Anforderungen an die IT (BAIT) in der Fassung vom 16.08.2021 berücksichtigt.[71]

5.2. Überblick: Nationale Organisation

Auf nationaler Ebene gestaltet sich die Organisation der Verhinderung von Cyberrisk wie folgt:

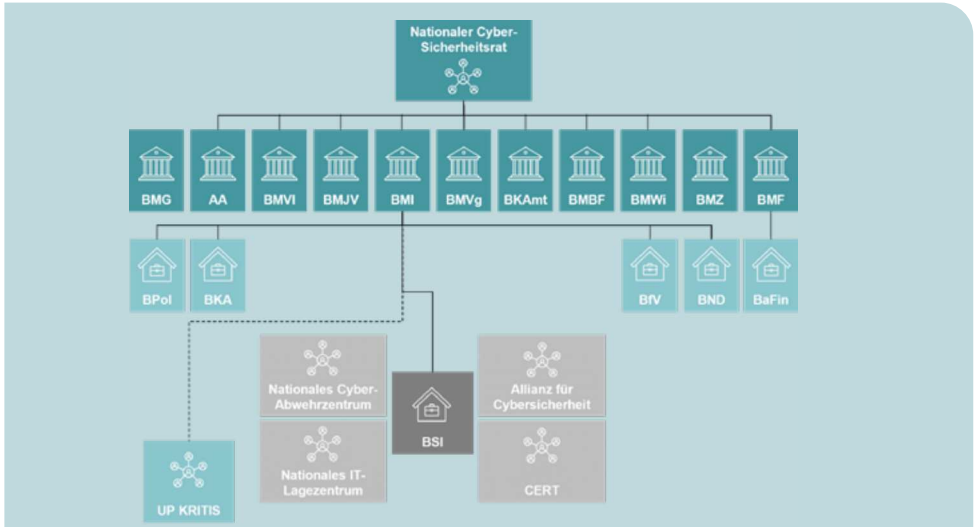

Abbildung 9: Übersicht nationale Organisation (angelehnt an: Zuständigkeiten und Aufgaben in der deutschen Cyber-Sicherheitspolitik (1. Auflage) | Stiftung Neue Verantwortung (SNV) (stiftung-nv.de))

Der Nationale Cybersicherheitsrat bildet das zentrale Steuerungsorgan, wenn es um die Verhinderung von Cyberrisk geht. Beteiligt an der Verhinderung von Cyberrisk sind zudem der Großteil der Ministerien in Deutschland und die ihnen nachfolgenden Ämter. Aus Vereinfachungsgründen ist die Darstellung der Ämter nicht vollständig. Unter den Ämtern wiederum nimmt das BSI bei Fragen rund um Cyberrisk eine hervorgehobene Stellung ein. Hier werden auch verschiedene Foren koordiniert.

5.2.1. Nationaler Cyber-Sicherheitsrat

Der Nationale Cyber-Sicherheitsrat wurde im Jahr 2011 eingerichtet mit dem Ziel, Krisenursachen frühzeitig zu identifizieren und zu beseitigen. Der Nationale Cyber-Sicherheitsrat soll die präventiven Instrumente sowie die Politik für Cybersicherheit zwischen Staat und Wirtschaft koordinieren. Die Schwerpunkte der Arbeit des Nationalen Cyber-Sicherheitsrates ist der Schutz kritischer Infrastrukturen und die Cyberaußenpolitik Deutschlands. Zukünftig soll der Nationale Cyber-Sicherheitsrat zudem:

- auf Basis aktueller technischer Entwicklungen insbesondere Vorschläge zur Weiterentwicklung der nationalen Regelungen für mehr Cybersicherheit machen,
- weitere Felder für die Kooperation von Staat und Wirtschaft für mehr Cybersicherheit und entsprechende Umsetzungsvorschläge aufzeigen,
- die föderale Cybersicherheitsarchitektur in den Blick nehmen und wichtige Impulse in Richtung Bundesregierung und Innenministerkonferenz geben,
- insbesondere den Austausch mit vergleichbaren strategischen Gremien anderer wesentlicher internationaler Partner suchen, um hieraus gegebenenfalls neue Impulse für die nationale Cybersicherheitspolitik zu generieren.

Der Nationale Cyber-Sicherheitsrat tagt dreimal jährlich, sowie anlassbezogen unter dem Vorsitz des Beauftragten der Bundesregierung für Informationstechnik (BfIT). Mitglieder des Cyber-Sicherheitsrats sind:

- Bundeskanzleramt
- Auswärtiges Amt
- Bundesministerium des Innern
- Bundesministerium der Verteidigung
- Bundesministerium für Wirtschaft und Technologie
- Bundesministerium der Justiz und für Verbraucherschutz
- Bundesministerium der Finanzen
- Bundesministerium für Bildung und Forschung
- Vertreter der Länder (Niedersachsen und Hessen)

Die Wirtschaft ist durch den Bundesverband der deutschen Industrie (e.V.) (BDI), den Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), den Deutschen Industrie- und Handelskammertag (DIHK), den Übertragungsnetzbetreiber Amprion sowie durch den UP-KRITIS[72] als assoziierte Mitglieder vertreten. Seit Juli 2017 wird der Nationale Cyber-Sicherheitsrat durch einen Fachbeirat unterstützt.[73]

5.2.2. Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde mit dem BSI-Einrichtungsgesetz vom 17.12.1990 als Bundesbehörde gegründet und dem Bundesministerium des Innern unterstellt.[74] Heutige Grundlage der Arbeit des BSI ist das „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik".

Die Aufgaben des BSI wurden im Laufe der Jahre sukzessive erweitert. Zu Beginn umfasste der Aufgabenbereich den Schutz der Regierungsnetze und die Sicherung zentraler Netzübergänge. Mit der Novellierung des BSI-Gesetzes 2009 kam die Entwicklung von Sicherheitsstandards für die Beschaffung und den Einsatz von IT bei Bundesbehörden hinzu. Das BSI wurde zudem zur zentralen Meldestelle für IT-Sicherheit innerhalb der Bundesverwaltung, um bei IT-Krisen nationaler Bedeutung durch Informationen und Analysen die Handlungsfähigkeit der Bundesregierung sicherzustellen. Zudem nahm das BSI die Rolle als kompetenter Ansprechpartner und Berater für alle Fragen der Informationssicherheit für die Öffentlichkeit ein.

Eine deutliche Erweiterung erfuhren die Aufgaben und Befugnisse des BSI durch das im Juli 2015 in Kraft getretene „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz). Mit verbindlichen Mindestanforderungen an die IT-Sicherheit verbessert es vor allem den Schutz der Kritischen Infrastrukturen (KRITIS) und erhöht die Netzsicherheit in den Bereichen, deren Ausfall oder Beeinträchtigung dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland hätte. Für KRITIS-Betreiber wurde durch das IT-Sicherheitsgesetz zudem eine Verpflichtung zur Meldung von erheblichen IT-Sicherheitsvorfällen an das BSI aufgenommen.

Eine erneute Erweiterung der Aufgaben des BSI ist durch das im Mai 2021 in Kraft getretene Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) erfolgt. Dieses Gesetz ordnet dem BSI u.a. den digitalen Verbraucherschutz zu.[75]

Ein wichtiger Aspekt der Arbeit des BSI ist die Veröffentlichung von Standards, die einen ausreichenden IT-Grundschutz, d.h. ein mittleres, angemessenes und ausreichendes Schutzniveau für IT-Systeme, gewährleisten sollen. Die Standards verfolgen einen ganzheitlichen Ansatz zur Informationssicherheit. Neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet. Sie ermöglichen es, durch ein systematisches Vorgehen notwendige

Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards liefern hierzu bewährte Vorgehensweisen. Ergänzend liefert das IT-Grundschutz-Kompendium konkrete Anforderungen.[76]

Aktuell sind folgende BSI-Standards relevant:[77]

- **BSI-Standard 200-1**: Der BSI-Standard 200-1 definiert allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (ISMS). Er ist weiterhin kompatibel zum ISO-Standard 27001 und berücksichtigt die Empfehlungen der anderen ISO-Standards wie beispielsweise ISO 27002.

- **BSI-Standard 200-2**: Der BSI-Standard 200-2 bildet die Basis der bewährten BSI-Methodik zum Aufbau eines soliden Informationssicherheitsmanagements (ISMS). Er etabliert drei neue Vorgehensweisen bei der Umsetzung des IT-Grundschutzes.

- **BSI-Standard 200-3**: Der BSI-Standard 200-3 beinhaltet gebündelt alle risikobezogenen Arbeitsschritte bei der Umsetzung des IT-Grundschutzes.

- **BSI-Standard 100-4**: Mit dem BSI-Standard 100-4 wird ein systematischer Weg aufgezeigt, ein Notfallmanagement in einer Behörde oder einem Unternehmen aufzubauen, um die Kontinuität des Geschäftsbetriebs sicherzustellen. Der modernisierte BSI-Standard 200-4 befindet sich aktuell in der Community-draft-Phase. Er soll zukünftig eine praxisnahe Anleitung geben, um ein Business Continuity Management System (BCMS) in der eigenen Institution aufzubauen und zu etablieren. Bis zur endgültigen Verabschiedung des BSI-Standards 200-4 bleibt der BSI-Standard 100-4 weiter gültig.

Das BSI hat zudem einen „Leitfaden zur Basis-Absicherung nach IT-Grundschutz: In 3 Schritten zur Informationssicherheit“ veröffentlicht. Dieser Leitfaden liefert einen kompakten und übersichtlichen Einstieg zum Aufbau eines Informationssicherheitsmanagementsystems (ISMS) in einer Institution. Er ist besonders für kleine und mittelständische Unternehmen und Behörden geeignet.

5.2.3. Nationales Cyber-Abwehrzentrum

Das Nationale Cyber-Abwehrzentrum (Cyber-AZ) dient als zentrale Kooperationsplattform der Bundesbehörden im Kampf gegen Cyberattacken. Das Cyber-AZ soll durch einen permanenten Informationsaustausch zwischen allen sicherheitsverantwortlichen Bundesbehörden die Voraussetzungen für eine effektive Gefahrenabwehr und wirksame Prävention schaffen.

Das Cyber-AZ ist ein Kernelement der Cybersicherheitsstrategie aus dem Jahr 2011. Durch die Cybersicherheitsstrategie 2011 wurde das Cyber-AZ unter Federführung des BSI eingerichtet und am 16.06.2011 offiziell eröffnet. Das Cyber-AZ wandelte sich im Laufe der Zeit von einer reinen Informationsdrehscheibe hin zu einer zentralen Kooperationsplattform. Durch das Cyber-AZ wird eine zielgerichtete, hoch integrierte und effiziente Zusammenarbeit zwischen den Beteiligten gewährleistet. Neben einer täglichen Lagebesprechung wird die Arbeit in Arbeitskreisen zu speziellen Themen oder in gemeinsamen Terminen bei Betroffenen eines Cyberangriffs organisiert.

Am 01.09.2019 wurden durch Verabschiedung einer neuen Geschäftsordnung des Cyber-AZ wesentliche Änderungen wirksam. Erstmals haben sich alle beteiligten Behörden dazu verpflichtet, Verbindungspersonen vor Ort ins Cyber-AZ zu entsenden, um die Vor-Ort-Präsenz zu stärken. Gleichzeitig wurde die Struktur des Cyber-AZ an die ähnlicher Kooperationsplattformen angepasst. Nunmehr orientiert sich das Cyber-AZ am Modell des Gemeinsamen Terrorismusabwehrzentrums (GTAZ). Dort kooperieren die Beteiligten ohne Federführung einer einzelnen Behörde allein im Rahmen ihrer gesetzlichen Zuständigkeiten. Die Funktion des Leiters des Cyber-AZ wurde durch die eines Koordinators ersetzt. Diese Aufgabe wird seit dem 16.12.2019 zunächst für zwei Jahre durch das BKA wahrgenommen. Unterstützt wird das BKA dabei durch stellvertretende Koordinatoren des Bundesamtes für Verfassungsschutz (BfV) und der Bundeswehr/Kommando Cyber- und Informationsraum (KdoCIR).

5.2.4. Nationales IT-Lagezentrum, Computer Emergency Response Team und Nationales IT-Krisenreaktionszentrum

Das IT-Lagezentrum ist Teil des BSI und damit betraut, rund um die Uhr ein IT-Lagebild zu erstellen. Gemeinsam mit dem CERT-Bund bildet es das Referat C21 im BSI. Das CERT-Bund ist dabei die zentrale Anlaufstelle zur Lösung von IT-Sicherheitsproblemen in der Bundesverwaltung und bearbeitet primär den technischen Teil. Organisatorisch sammelt das Nationale IT-Lagezentrum die Sicherheitsinformationen aus einer Vielzahl von nationalen und internationalen Quellen (Technik, Sicherheitsbehörden, Polizei, andere Regierungsstellen und Wirtschaft).

Aufgrund des Zusammenwirkens von Informationssammlung und Technik kann ein über normale CERT-Meldungen hinausgehendes Lagebild gewonnen werden, das in einem nationalen IT-Sicherheitslagebild zusammengefasst wird. In dieses Sicherheitslagebild fließen zusätzlich auch Daten eines Sensornetzes zur Erfassung von Unregelmäßigkeiten im Internet mit ein. In IT-Notfällen wird eine Warnmeldung an die Bundesverwaltung herausgegeben, ggf. darüber hinaus als Extraausgabe über das Bürger-CERT. Sofern zusätzlich Kritische Infrastrukturen (KRITIS) betroffen sein könnten, wird unter Hinzuziehung der verantwortlichen KRITIS-Referate im BSI eine Schwachstellenwarnung auch an diese Partner versandt. Bei einem weitergehenden Krisenfall wächst das IT-Langezentrum im Rahmen einer „besonderen Aufbauorganisaion (BAO)“ zum Nationalen IT-Krisenreaktionszentrum auf.[78]

5.2.5. Allianz für Cyber-Sicherheit

Die Allianz für Cyber-Sicherheit (ACS) wurde im Jahr 2012 gegründet. Sie dient als kooperative Plattform für Unternehmen, Verbände, Behörden und Organisationen, um Informationen zu aktuellen Bedrohungslagen und praxisnahe Cybersicherheitsmaßnahmen auszutauschen. Teilnehmer profitieren vom Know-how sowie den zahlreichen engagierten Partnern und können so den Schutz der eigenen IT-Infrastruktur deutlich verbessern.

Der Allianz für Cybersicherheit gehören mehr als 5000 Teilnehmer an. Zu den Teilnehmern gehörten neben IT-Dienstleistungs- und -Beratungsunternehmen sowie IT-Herstellern auch Anwenderunternehmen aller Größen und Branchen.[79]

5.2.6. Bundesanstalt für Finanzdienstleistungsaufsicht

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ist für die Kontrolle von Instituten, Versicherungen und für die Marktaufsicht über den Wertpapierhandel zuständig.[80] Die Hauptaufgabe der BaFin ist die Gewährleistung eines funktionsfähigen, stabilen und integren Finanzsystems. Die herausragende Bedeutung eines solchen Finanzsystems für die Gesellschaft ergibt sich aus dem Versorgungsbeitrag, den dieses Finanzsystem erbringt. Im Rahmen einer Sektorstudie zur Untersuchung kritischer Infrastrukturen wurden drei Versorgungsleistungen von Kreditinstituten (diverse Zahlungsverkehrsgeschäfte) und zwei Versorgungsleistungen von Börsen (Verrechnung, Abwicklung und Verwahrung in Zusammenhang mit dem Wertpapierhandel) als kritische Versorgungsleistungen eingestuft.[81] Der Finanzsektor zählt demnach grundsätzlich zu den Kritischen Infrastrukturen. Soweit ein einzelnes Institut als Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber) zu qualifizieren ist, muss es nach §§ 8a und 8b BSIG verschiedene Anforderungen erfüllen. Diese Institute unterliegen dann neben der Aufsicht der BaFin zusätzlich der Aufsicht des BSI.

Die Bedeutung des Themas Cyberrisk für den Finanzsektor spiegelt sich auch in der aufsichtlichen Praxis der BaFin wider. So bestehen mit den Rundschreiben 10/2021 (BA) – Mindestanforderungen an das Risikomanagement – MaRisk[82] und 10/2017 (BA) – Bankaufsichtliche Anforderungen an die IT (BAIT)[83] umfangreiche Anforderungen an den Einsatz von Informationstechnik in den Instituten. Mit den Rundschreiben verfolgt die BaFin das Ziel, einen flexiblen und praxisnahen Rahmen für die technisch-organisatorische Ausstattung der Institute – insbesondere für das Management der IT-Ressourcen, das Informationsrisikomanagement und das Informationssicherheitsmanagement – vorzugeben. Ferner werden die Anforderungen des § 25b KWG (Auslagerung von Aktivitäten und Prozessen) näher präzisiert. Den durch die Aufsicht gesetzten Rahmen haben die Institute mit konkreten organisatorischen Vorgaben zu füllen. Hierbei können sie grundsätzlich auf gängige Standards abstellen. Zu diesen zählen beispielsweise der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik und die internationalen Sicherheitsstandards ISO/IEC 270XX der International Organization for Standardization.[84]

Neben diesen allgemein auf die IT bezogenen Anforderungen veröffentlichte die BaFin mehrere Beiträge zum Thema Cyberrisk im Jahr 2020 und legte hierin auch ihre Erwartungshaltung an die Kreditinstitute dar.[85] Anfang Mai 2021 erklärte die BaFin das Thema IT- und Cyberrisiken zum Aufsichtsschwerpunkt für das Jahr 2021. Die BaFin begründet den aufsichtlichen Schwerpunkt wie folgt: „Der technische Wandel im Finanzsektor nimmt weiter an Fahrt auf. Zum einen gewinnen wegen der COVID-19-Pandemie digitale Geschäftsmodelle mit Online-Vertrieb und rund um die Uhr verfügbaren Servicekanälen mehr und mehr Marktanteile. Zum anderen durchdringen Innovationen wie Künstliche Intelligenz und die Distributed-Ledger-Technologie (DLT) sowie die darauf basierenden Kryptowerte die Branche zusehends. Dieser technische Wandel eröffnet den Marktteilnehmern viele Chancen. Unternehmen und Aufsicht kommen aber nicht umhin, sich zugleich auf vermehrte IT-Risiken einzustellen, etwa aus Pannen in den IT-Systemen der Unternehmen und Angriffen von Hackern. IT-Pannen und Cyberkriminalität können nicht nur zu signifikanten finanziellen Verlusten führen oder zumindest die Reputation der betroffenen Unternehmen schädigen. Auch systemische Auswirkungen sind möglich. IT- und Cyberrisiken sind daher – wie bereits 2020 – ein BaFin-weiter Aufsichtsschwerpunkt."

Mit der Festlegung als Aufsichtsschwerpunkt für das Jahr 2021 geht einher, dass die BaFin ein besonderes Augenmerk im Rahmen der risikoorientierten Aufsicht auf Kritische Infrastrukturen legen will und das Thema der zunehmenden Auslagerung bzw. Ausgliederung von IT-Dienstleistungen näher beleuchtet. Die BaFin will 2021 systematisch bei den auslagernden Unternehmen abfragen, welche Maßnahmen sie ergriffen haben, um IT- und Cyberrisiken zu begrenzen oder zu reduzieren. Auch bei Sonderprüfungen will die BaFin einen Schwerpunkt auf IT- und Cybersicherheit legen. IT- und Cyberrisiken sollen auch ein Thema im Rahmen der Fokusaufsicht sein, die im Zuge der Neuausrichtung der Behörde eingerichtet werden soll.[86]

6. WELCHE STRATEGIEN WERDEN ZUR VERHINDERUNG VON CYBERATTACKEN VERFOLGT?

6.1. Europäische Ebene

Auf europäischer Ebene orientiert sich die Verhinderung von Cyberrisk an der im Dezember 2020 vorgestellten EU-Cybersicherheitsstrategie. Die EU-Cybersicherheitsstrategie soll als zentrales Element der Gestaltung der digitalen Zukunft Europas, des Aufbauplans für Europa und der EU-Strategie für eine Sicherheitsunion die kollektive Abwehrfähigkeit gegen Cyberbedrohungen stärken und dazu beitragen, dass alle Bürgerinnen und Bürger und Unternehmen die Vorzüge vertrauenswürdiger und zuverlässiger Dienste und digitaler Instrumente uneingeschränkt nutzen können.[87] Die Strategie umfasst die folgenden drei Handlungsfelder:[88]

- **Widerstandsfähigkeit, technologische Unabhängigkeit und Führungsrolle**: Auf diesem Feld schlägt die Kommission vor, die Vorschriften über die Sicherheit von Netz- und Informationssystemen durch eine Richtlinie über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union (überarbeitete NIS-Richtlinie oder „NIS 2“) neu zu gestalten, um die Abwehrfähigkeit kritischer öffentlicher und privater Sektoren zu verbessern. Darüber hinaus schlägt die Kommission vor, ein Netz von Sicherheitseinsatzzentren in der gesamten EU mithilfe Künstlicher Intelligenz (KI) aufzubauen, das für die EU ein echter „Cybersicherheitsschutzschild“ mit der Fähigkeit sein wird, frühzeitige Signale für drohende Cyberangriffe zu erkennen und Maßnahmen zu ermöglichen, bevor Schäden verursacht werden. Weitere Maßnahmen umfassen die gezielte Unterstützung kleiner und mittlerer Unternehmen (KMU) im Rahmen der digitalen Innovationszentren sowie verstärkte Bemühungen, um Fachkräfte auszubilden und zu schulen, die besten Talente auf dem Gebiet der Cybersicherheit anzuziehen und zu binden sowie in eine offene wettbewerbsfähige Forschung und Innovation von Weltrang zu investieren.

- **Aufbau operativer Kapazitäten zur Prävention, Abschreckung und Reaktion**: Die Kommission bereitet derzeit mit den Mitgliedstaaten in einem offenen und integrativen Verfahren eine neue gemeinsame Cyberstelle vor, um die Zusammenarbeit zwischen den EU-Einrichtungen und den Behörden der Mitgliedstaaten, die für die Prävention, Abschreckung und Reaktion im Hinblick auf Cyberangriffe zuständig sind (einschließlich ziviler und diplomatischer Gemeinschaften sowie der Strafverfolgungs- und Verteidigungskreise im Bereich der Cybersicherheit), zu stärken. Die EU will sich auch dafür einsetzen, die Zusammenarbeit im Bereich der Cyberabwehr weiter zu verbessern und modernste Fähigkeiten auf diesem Gebiet zu entwickeln. Sie will sich dabei auf die Arbeiten der Europäischen Verteidigungsagentur stützen und die Mitgliedstaaten auffordern, die Ständige Strukturierte Zusammenarbeit und den Europäischen Verteidigungsfonds in vollem Umfang zu nutzen.

- **Förderung eines globalen offenen Cyberraums durch verstärkte Zusammenarbeit**: Die EU will ihre Zusammenarbeit mit internationalen Partnern intensivieren, um die regelbasierte Weltordnung zu stärken, die internationale Sicherheit und Stabilität im Cyberraum zu fördern sowie die Menschenrechte und Grundfreiheiten im Internet zu schützen. Sie will internationale Normen und Standards voranbringen, die diese Grundwerte der EU widerspiegeln, indem sie mit ihren internationalen Partnern in den Vereinten Nationen und anderen einschlägigen Foren zusammenarbeitet. Die EU beabsichtigt ihr Instrumentarium für die Cyberdiplomatie weiter zu stärken. Außerdem will sie durch eine EU-Agenda für den Aufbau externer Cyberkapazitäten die Bemühungen um den Aufbau solcher Kapazitäten in Drittländern verstärken. Die Cyberdialoge mit Drittländern, regionalen und internationalen Organisationen und der Multi-Stakeholder-Gemeinschaft werden intensiviert. Die EU will ferner ein weltumspannendes EU-Netz für Cyberdiplomatie errichten, um für ihre Vision des Cyberraums zu werben.

Erste Schritte bei der Umsetzung der EU-Strategie sind bereits erfolgt. So gab der Rat im April 2021 grünes Licht für die Einrichtung eines Europäischen Kompetenzzentrums zur Bündelung von Investitionen in Forschung, Technologie und industrielle Entwicklung im Bereich der Cybersicherheit. Die neue Stelle, die ihren Sitz in Bukarest (Rumänien) haben soll, wird insbesondere Mittel für den Bereich der Cybersicherheit aus den Programmen „Horizont Europa“ und „Digitales Europa“ koordinieren. Das Europäische Kompetenzzentrum für Industrie, Technologie und Forschung im Bereich der Cybersicherheit wird mit einem Netz nationaler Koordinierungszentren zusammenarbeiten, die von den Mitgliedstaaten benannt werden. Das Zentrum wird auch die

wichtigsten europäischen Akteure, darunter die Industrie, Hochschul- und Forschungseinrichtungen und andere einschlägige Organisationen der Zivilgesellschaft, zusammenbringen, um eine Kompetenzgemeinschaft für Cybersicherheit zu bilden und so das Fachwissen im Bereich der Cybersicherheit EU-weit zu steigern und zu verbreiten. Es soll zudem eng mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) zusammenarbeiten.[89]

6.2. Nationale Ebene

Das Thema Cyberrisk beschäftigt nicht nur internationale Institutionen, sondern nimmt auch auf nationaler Ebene eine wichtige Stellung ein. Fixpunkt für die Organisation der Cybersicherheit auf nationaler Ebene ist die im Jahr 2011[90] entwickelte und in den Jahren 2016[91] sowie 2021[92] fortgeschriebene „Cybersicherheitsstrategie für Deutschland". Aus dieser Strategie ergibt sich auch die Organisation für die Abwehr von Cyberrisk (siehe Grafik im Abschn. 5.2.).

Die im Jahr 2011 veröffentlichte Strategie definierte die folgenden zehn strategischen Bereiche:
- Schutz Kritischer Infrastrukturen[93]
- Sichere IT in Deutschland
- Stärkung der IT-Sicherheit in der öffentlichen Verwaltung
- Einrichtung eines Nationalen Cyberabwehrzentrums
- Einrichtung eines Nationalen Cybersicherheitsrats
- Wirksame Kriminalitätsbekämpfung im Cyberaraum
- Effektives Zusammenwirken für Cybersicherheit in Europa und weltweit
- Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie
- Personalentwicklung der Bundesbehörden
- Instrumentarium zur Abwehr von Cyberangriffen

Eine der wichtigsten organisatorischen Weichenstellungen war die Einrichtung eines Nationalen Cybersicherheitsrates und eines Nationalen Cyberabwehrzentrums.

Die zehn strategischen Bereiche aus 2011 wurden in der im Jahr 2016 fortgeschriebenen Strategie unter dem Leitbild, dass die Handlungsfähigkeit und Souveränität Deutschlands auch im Zeitalter der Digitalisierung gewährleistet sein muss, zu folgenden vier Handlungsfeldern zusammengefasst:[94]

- **Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung**: Ziel ist es, die Menschen, Unternehmen und sonstigen Akteure in Deutschland in die Lage zu versetzen, die Chancen und Risiken beim Einsatz von Informationstechnik zu erfassen, zu bewerten und ihr Handeln daran auszurichten. Als Grundlage hierfür wurde eine gezielte digitale Bildung für alle Alters- und Anwendergruppen identifiziert. Cybersicherheit muss fest im Bewusstsein der Gesellschaft verankert werden, um digitaler Sorglosigkeit entgegenzuwirken. Zudem müssen die Voraussetzungen für eine sichere elektronische Kommunikation und sichere Webangebote geschaffen werden. Weitere wichtige Aspekte stellen die Schaffung sicherer elektronischer Identitäten und die Einführung von Gütesiegeln für IT-Sicherheit dar.

- **Gemeinsamer Auftrag Cybersicherheit von Staat und Wirtschaft**: Ziel ist es, die Unternehmen in Deutschland in die Lage zu versetzen, sich selbst und ihre Kunden wirksam vor Cyberangriffen zu schützen. Besonderes Augenmerk gilt dabei den Betreibern Kritischer Infrastrukturen. Es gilt im Wege des mit dem IT-Sicherheitsgesetz etablierten kooperativen Ansatzes die erforderlichen Rahmenbedingungen fortzuentwickeln und bei Bedarf auf andere Bereiche der Wirtschaft zu erweitern. Bei der Entwicklung und Durchsetzung wirksamer und bedarfsgerechter IT-Sicherheitsstandards müssen Staat und Wirtschaft vertrauensvoll und eng zusammenarbeiten. Das Fundament hierfür ist eine starke deutsche IT-Wirtschaft, die durch eine moderne Wirtschaftspolitik zu fördern ist. Zudem sollen Maßnahmen erarbeitet werden, um die im internationalen Vergleich schwächer ausgeprägte Gründungskultur für Startups im Bereich IT-/Cybersicherheit in Deutschland zu verbessern. Der Einbeziehung von Providern und nationalen IT-Sicherheitsdienstleistern kommt bei der Erkennung und Abwehr von Cyberangriffen eine Schlüsselrolle zu.

- **Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur**: Die fortschreitende Digitalisierung führt dazu, dass heute eine Vielzahl von staatlichen Stellen in Bund und Ländern mit Fragen der Cybersicherheit befasst ist. Das Aufgabenfeld reicht von der Prävention, der Gefahrenabwehr und der Strafverfolgung über die Spionageabwehr und nachrichtendienstliche Aufklärung bis zur Cyberverteidigung. Dabei sind sowohl innere wie äußere Sicherheit im Cyberraum gleichermaßen betroffen. Der Staat muss seine Institutionen so aufstellen, dass der Schutzauftrag für die Gesellschaft auch im Zeitalter der Digitalisierung wahrgenommen wird.

  Eine moderne Cybersicherheitsarchitektur begreift Cybersicherheit vor diesem Hintergrund als permanente gesamtstaatliche Aufgabe, die gemeinsam zu bewältigen ist. Wesentlich ist, dass im Bedarfsfall Informationen verteilt werden und die Aufgabenwahrnehmung effizient koordiniert wird. Föderalen, ressort- und behörden- sowie grenzübergreifenden Synergien kommt besondere Bedeutung zu. Das Nationale Cyberabwehrzentrum bietet auf Bundesebene bereits die entsprechende Struktur, unter deren Dach die einzelnen Akteure im Rahmen ihrer jeweiligen Zuständigkeiten zusammenarbeiten. Es gilt, diese Zusammenarbeit zu intensivieren und die Länder künftig stärker einzubinden.

- **Aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik**: Sicherheit muss insbesondere im Zeitalter der Digitalisierung auch global gedacht werden. Deutschland wird sich bei Maßnahmen zur Stärkung nationaler bzw. regionaler Cybersicherheitsfähigkeiten auch für interoperable Cybersicherheitsarchitekturen und -standards ein-

setzen. Auf europäischer Ebene ist für einen sicheren europäischen Cyberraum der digitale Binnenmarkt mit Schwerpunkt auf dem Austausch sicherer und interoperabler Daten von entscheidender Bedeutung. Entsprechendes gilt – im Rahmen bestehender Unionskompetenzen – in Bezug auf die polizeiliche und justizielle Zusammenarbeit sowie eine entsprechend gestaltete Gemeinsame Außen- und Sicherheitspolitik und die Vernetzung der europäischen IT-Sicherheitsforschung. Zusätzlich setzt Deutschland sich in internationalen Foren (z.B. bei der NATO) für mehr Cybersicherheit ein.

Die vier Handlungsfelder wurden in der am 08.09.2021 beschlossenen Cybersicherheitsstrategie 2021 beibehalten[95] und durch strategische Ziele und operative Maßnahmen konkretisiert. Diese sollen vor dem Hintergrund von Leitlinien, welche aus den die Handlungsfelder übergreifenden Interessen und Belangen abgeleitet wurden, betrachtet, geprüft und umgesetzt werden. Die Leitlinien wurden wie folgt gefasst[96]:

- **Cybersicherheit als eine gemeinsame Aufgabe von Staat, Wirtschaft, Wissenschaft und Gesellschaft etablieren**: Cyberbedrohungen und -angriffe betreffen nicht nur den Staat, sondern auch Unternehmen, wissenschaftliche Einrichtungen, Vereine sowie Privatpersonen. Cybersicherheit wird daher als gemeinsame Aufgabe aller Akteure verstanden. Da Cyberbedrohungen nicht an Ländergrenzen halt machen, wird zudem die Bedeutung europäischer und internationaler Zusammenarbeit betont.

- **Digitale Souveränität von Staat, Wirtschaft, Wissenschaft und Gesellschaft stärken**: Die Bundesregierung versteht unter digitaler Souveränität „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können". Wesentliche Voraussetzungen hierfür sind zum einen sichere Technologien und Lösungen und zum anderen die Fähigkeit, die Chancen und potenziellen Risiken digitaler Technologien erkennen und bewerten zu können.

- **Digitalisierung sicher gestalten**: Grundvoraussetzung für das Gelingen der Digitalisierung in Deutschland ist die Cyber- und Informationssicherheit. Nur ein hohes Sicherheitsniveau ermöglicht es, die Potenziale der Digitalisierung voll auszuschöpfen.

- **Ziele messbar und transparent ausgestalten**: Wesentliche Neuerung der Strategie 2021 ist die regelmäßige Evaluierung der Nachhaltigkeit und Effektivität der Strategie. Hierzu sind alle in der Cybersicherheitsstrategie 2021 formulierten Ziele mit definierten Indikatoren hinterlegt, die den Erfolg der Strategie nachvollziehbar und überprüfbar machen sollen. Die Zielerreichung soll sowohl zum Ende der Laufzeit als auch während der Laufzeit regelmäßig überprüft werden.

7. AUSBLICK

Cyberrisk und Cybersecurity stehen zu Recht im Fokus von Politik, Wirtschaft, Öffentlichkeit, Aufsicht und Wirtschaftsprüfern. Die Gefährdungslage ist auch in Deutschland angespannt bis kritisch. Die konkreten Angriffe sind vielschichtig. Sie können sowohl Kritische Infrastrukturen als auch allgemein Unternehmen, öffentliche Verwaltungen, aber auch Privatpersonen betreffen. Dieser Teil 1 einer Serie von IDW Knowledge Papers zum Thema Cyberrisk beschäftigte sich vorrangig mit der Darstellung von Grundlagen zum Umgang mit Cyberrisk.

In Teil 2 dieser Reihe, der voraussichtlich noch 2021 erscheint, wird der Fokus auf Möglichkeiten gelegt, wie Cybersecurityprüfungen dazu beitragen können, Cyberrisk effektiv zu bekämpfen.

QUELLENVERZEICHNIS

[1] Als Angriffsvektoren werden Kombinationen von Angriffswegen und -techniken bezeichnet, mit denen sich Angreifer unerlaubt Zugang zu IT-Systemen verschaffen.

[2] Unter einem Scriptkiddie werden Computernutzer verstanden, die trotz mangelnder Grundlagenkenntnisse versuchen in fremde Computersysteme einzudringen oder sonstigen Schaden anzurichten. Diese bedienen sich meist Gebrauchsanweisungen für ihre Attacken.

[3] Vgl. Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2020, S. 29 und Crowdstrike, Global Threat Report 2021, S. 25.

[4] Vgl. BKA „Cybercrime – Bundeslagebild 2020", S. 12 f.

[5] Vgl. Crowdstrike: Global Threat Report 2021, S. 7.

[6] Vgl. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond.

[7] Vgl. 2020 Phishing and Fraud Report (f5.com), S. 3.

[8] Unter Social Engineering wird die zwischenmenschliche Beeinflussung verstanden, mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen zu verleiten.

[9] Vgl. Die 10 gängigsten Phishing Attacken | Kaspersky.

[10] Vgl. Was ist Malware, und wie können Sie sich davor schützen? | Kaspersky.

[11] Vgl. Broad/Markoff/Sanger: Israeli Test on Worm Called Crucial in Iran Nuclear Delay in: The New York Times: Stuxnet Worm Used Against Iran Was Tested in Israel – The New York Times (nytimes.com).

[12] Vgl. Albright/Brannan/Walrond: Stuxnet Malware und Natanz: stuxnet_update_15Feb2011.pdf (stanford.edu).

[13] Vgl. Stuxnet – SecuPedia.

[14] Vgl. Computerwurm – Wikipedia.

[15] Vgl. Internet: Mydoom richtet Milliardenschäden an – Netzwirtschaft – FAZ.

[16] Nicht immer lassen sich Viren eindeutig einer bestimmten Art zuordnen. Mithin existieren auch Mischformen.

[17] Beim Einschalten eines Computers muss zuerst das Betriebssystem geladen werden. Hierfür ist der sog. Urlader zuständig. Hierzu wird auf Speichermedien in einer festen Reihenfolge nach Betriebssystemen gesucht. Auf fast allen Speichermedien gibt es eine fest vorgegebene Stelle, an der ein Betriebssystem-Ladeprogramm stehen kann. Auf einer Festplatte nennt man diese Stelle Master-Boot-Record (MBR). Das Ladeprogramm aus dem MBR startet das auf der Festplatte gespeicherte Betriebssystem.

[18] Unter einem Makro wird eine zusammengefasste Folge von Anweisungen oder Deklarationen verstanden, die anstelle von mehreren Einzelanweisungen im Programm mit nur einem einfachen Aufruf ausgeführt werden kann.

[19] Vgl. Emotet: So schützen Sie sich und erkennen den Trojaner | Kaspersky.

[20] Vgl. Managementabstrakt Fortschrittliche Angriffe – Neue Qualität aktueller Angriffe und Prognose (bund.de).

[21] Vgl. Emotet: So schützen Sie sich und erkennen den Trojaner | Kaspersky.

[22] Vgl. BSI – Presse – Emotet-Infrastruktur zerschlagen – BSI informiert Betroffene (bund.de).

[23] Vgl. Was sind Trojaner? | Trojaner entfernen | Kaspersky.

[24] Vgl. Attacke mit dem Krypto-Trojaner WannaCry – Taktik und Folgen | Compliance | Haufe.

[25] Vgl. Ransomware: Cyberattacke trifft 800 Filialen einer schwedischen Supermarktkette | ZEIT ONLINE.

[26] Vgl. BSI – Bundesamt für Sicherheit in der Informationstechnik – Newsletter SICHER • INFORMIERT vom 12.08.2021.

[27] Vgl. Anhalt-Bitterfeld: Hacker stellen persönliche Daten von Abgeordneten ins Darknet – DER SPIEGEL.

[28] Vgl. Hacker-Angriff über IT-Dienstleister Kaseya hat weltweite Folgen | Compliance | Haufe.

[29] Vgl. Bundesamt für Sicherheit in der Informationstechnik: Ransomware – Bedrohungslage, Prävention & Reaktion 2019, S. 5.

[30] Vgl. Bundesamt für Sicherheit in der Informationstechnik: Ransomware – Bedrohungslage, Prävention & Reaktion 2019, S. 7.

[31] Als Exploit wird die systematische Möglichkeit bezeichnet Schwachstellen in Programmen auszunutzen. Exploit Kits sind eine bestimmte Art von Schadprogrammen. Diese Programme enthalten Daten oder ausführbaren Code, die eine oder mehrere Sicherheitslücken in den Programmen, die auf einem Computer laufen, ausnutzen können. Exploit Kits können über das Darknet käuflich erworben werden.

[32] Vgl. Angriff im Hotel-Netz | heise online.

[33] Vgl. Wird das IT-Debakel der DKB zur Nemesis für die Sparkassen-IT? (finanz-szene.de).

[34] Vgl. DKB und Sparkassen-IT von 16-jährigem Script-Kiddie genarrt? (finanz-szene.de).

[35] Vgl. Mirai-Botnet gefährdet IoT-Geräte mit neuen Varianten | Avira Blog.

[36] Grafik angelehnt an Darstellung in Mirai DDoS Attack Explained (imperva.com).

[37] Vgl. Was sind DDoS-Attacken, und wie lassen sie sich verhindern? | Kaspersky.

[38] Vgl. BSI – APT (bund.de).

[39] Vgl. Das müssen Sie über Advanced Persistent Threats wissen | Offizieller Blog von Kaspersky.

[40] Vgl. [Report] M-Trends 2020 (fireeye.com).

[41] Vgl. Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland, S. 28.

[42] Ein Router ist ein dedizierter Computer für den Zusammenschluss von Netzen. Er kann Netze unterschiedlicher Technologien mit verschiedenen Medien, Adressschemata oder Rahmenformaten verbinden. Er wird am häufigsten zur Internetanbindung verwendet.

[43] Vgl. Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland, S. 28.

[44] Vgl. 5 Warning Signs of Advanced Persistent Threat | Tips to Prevent APT | Kaspersky.

[45] Vgl. 5 Warning Signs of Advanced Persistent Threat | Tips to Prevent APT | Kaspersky.

[46] Vgl. IDW: *IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1)*, Tz. 23.

[47] Das ISO Open Systems Interconnection model ist ein Referenzmodell für Netzwerkprotokolle als Schichtenarchitektur.

[48] Als Applikation wird Anwendungssoftware bezeichnet, d.h. ein Computerprogramm, das eine für den Anwender nützliche Funktion ausführt.

[49] Vgl. Was ist eine Firewall? – Cisco.

[50] Unter Payload wird die Nutzlast der übermittelten Daten verstanden.

[51] Vgl. Proxy-Firewall :: proxy firewall :: ITWissen.info.

[52] Vgl. BSI – Virenschutz und falsche Antivirensoftware (bund.de).

[53] CON.3: Datensicherungskonzept (bund.de).

[54] Vgl. Allianz-Risk-Barometer-2021.pdf; Die Studie stützt sich auf Antworten von 2.769 Unternehmen.

[55] Vgl. Die Lage der IT-Sicherheit in Deutschland 2021 (bund.de).

[56] Vgl. Die Lage der IT-Sicherheit in Deutschland 2021 (bund.de), S. 9.

[57] Vgl. BKA – Lagebilder – Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie, S. 21.

[58] Vgl. Cyber-attacks against companies (kfn.de), S. 155 ff.

[59] Der British Standard BS 7799 stellt Spezifikation für ein Informations-Sicherheits-Management-System (ISMS) dar.

[60] Der British Standard BS 7799-1 ist ein „Code of practice" für Informationssicherheit. Die Norm ist gedacht für interne Audits.

[61] Der Federal Information Security Management Act (FISMA) ist ein US-amerikanisches Bundesgesetz, das Bundesbehörden verpflichtet, ein Informationssicherheits- und -schutzprogramm zu implementieren.

[62] Vgl. Framework for Improving Critical Infrastructure Cybersecurity (nist.gov).

[63] Als EU Cybersecurity Act wird die am 27 Juni 2019 in Kraft getretene Verordnung (EU) 881/2019 bezeichnet, die die Verordnung (EU) Nr. 526/2013 ersetzte. Mit dem EU Cybersecurity Act wurde zum einen das Mandat der ENISA gestärkt und zum anderen ein EU-weit geltendes Rahmenwerk für die IT-Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen etabliert.

[64] Vgl. About ENISA – The European Union Agency for Cybersecurity – ENISA (europa.eu).

[65] Vgl. What we do? (cen.eu).

[66] Vgl. CENELEC – About CENELEC – Who we are.

[67] Vgl. ETSI – Standards, mission, vision, direct member participation.

[68] Vgl. About the FSB – Financial Stability Board.

[69] Abrufbar unter: Effective Practices for Cyber Incident Response and Recovery: Final Report – Financial Stability Board (fsb.org).

[70] Vgl. Deutsch | European Banking Authority (europa.eu).

[71] Vgl. BaFin – Aktuelles – Rundschreiben 10/2017 (BA) – Bankaufsichtliche Anforderungen an die IT ... in der Fassung vom 16.08.2021.

[72] Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen.

[73] Vgl. Cyber-Sicherheitsrat (bmvg.de).

[74] Vgl. Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik.

[75] Vgl. https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.htm.

[76] Vgl. BSI – IT-Grundschutz (bund.de).

[77] Vgl. BSI – BSI-Standard 100-4: Notfallmanagement (bund.de).

[78] Vgl. BSI-Lagezentrum und CERT-Bund – SecuPedia.

[79] Vgl. ACS – Allianz für Cyber-Sicherheit – ACS (allianz-fuer-cybersicherheit.de).

[80] Vgl. BaFin – Aufgaben & Geschichte.

[81] Vgl. Sektorstudie_Finanzen_Versicherungen.pdf (bund.de).

[82] Vgl. BaFin – Aktuelles – Rundschreiben 10/2021 (BA) – MaRisk BA.

[83] Vgl. BaFin – Aktuelles – Rundschreiben 10/2017 (BA) – Bankaufsichtliche Anforderungen an die IT ... in der Fassung vom 16.08.2021.

[84] Vgl. BaFin – Aktuelles – Rundschreiben 10/2017 (BA) – Bankaufsichtliche Anforderungen an die IT ... in der Fassung vom 16.08.2021, Tz. 2 f.

[85] Vgl. BaFin – Alle Ausgaben der BaFinPerspektiven – BaFinPerspektiven Ausgabe 1 | 2020.

[86] Vgl. BaFin Broschüre.

[87] Vgl. Die neue Cybersicherheitsstrategie der EU (europa.eu).

[88] Vgl. The EU's Cybersecurity Strategy in the Digital Decade | Shaping Europe's digital future (europa.eu).

[89] Vgl. Cybersicherheit: Wie die EU Cyberbedrohungen begegnet – Consilium (europa.eu).

[90] Vgl. Cyber-Sicherheitsstrategie für Deutschland (bund.de).

[91] Vgl. Cyber-Sicherheitsstrategie für Deutschland (bund.de).

[92] Vgl. Cybersicherheitsstrategie für Deutschland 2021 (bund.de).

[93] Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

[94] Vgl. Cyber-Sicherheitsstrategie für Deutschland (bund.de), S. 13 ff.

[95] Vgl. Cybersicherheitsstrategie für Deutschland 2021 (bund.de), S. 28 ff.

[96] Vgl. Cybersicherheitsstrategie für Deutschland 2021 (bund.de), S. 22 ff.

Ihre Notizen:

Dieses Knowledge Paper wurde vom IDW Arbeitskreis „IT-Prüfungen bei Instituten“ entwickelt.

Wir freuen uns über Ihre Anmerkungen. Sie können diese direkt an Herrn Dr. Daniel P. Siegel oder an Herrn Andreas Pöhlmann, Institut der Wirtschaftsprüfer in Deutschland e.V., Postfach 320580, 40420 Düsseldorf oder an siegel@idw.de bzw. poehlmann@idw.de senden.

INSTITUT DER WIRTSCHAFTSPRÜFER IN DEUTSCHLAND E.V.
WIRTSCHAFTSPRÜFERHAUS

Tersteegenstr. 14
40474 Düsseldorf

Postfach 32 05 80
40420 Düsseldorf

Telefon: +49 (0) 211/4561-0
Telefax: +49 (0) 211/4561097

E-Mail: info@idw.de
Web: www.idw.de

IDW
INSTITUT DER WIRTSCHAFTSPRÜFER