Cybersicherheit wird zur Chefsache

Dr. Manfred Rack

Rechtsanwalt

RACK
RECHTSANWÄLTE

Vorwort

Cyberangriffe und die verursachten Schäden steigen dramatisch. Im letzten Jahr 2023 wurden Schäden in Höhe von 206 Milliarden durch Hackerangriffe verursacht. Die Gesetzgeber von EU und dem Bund reagieren mit neuen gesetzlichen Vorschriften zur Abwendung oder mindestens zur Reduzierung von IT- und Cyberrisiken. Die vorliegenden Referentenentwürfe zum KRITIS-DachG und zum neuen BSIG liegen seit 7.5.2024 vor. Die EU-Richtlinien sind bis zum 17. Oktober 2024 umzusetzen. Neu ist die harte und nicht delegierbare Geschäftsleiterverantwortung für das Risikomanagement im Bereich der Cybersicherheit, auf die sich die Organe von Unternehmen einstellen müssen. Die Letztverantwortung tragen die Geschäftsleiter, auch wenn ihnen die Kompetenz dazu fehlt und sie fachkundige Hilfspersonen und Berater einsetzen. Durch die Verpflichtung der Geschäftsleiter wollen die Gesetzgeber der Cybersicherheit höchste Priorität verschaffen, um die Motivation zur Cybersicherheit zu steigern. Neben den rechtlichen Organisationsfragen stellen sich Fragen aus der Informatik zur IT- und Cybersicherheit. Mit dem folgenden Beitrag sollen Geschäftsleiter in die Lage versetzt werden, die richtigen Fragen an Berater zu stellen und Schutzmaßnahmen zu veranlassen, auch wenn sie weder auf eigene rechtliche noch IT-Kompetenzen zurückgreifen können. Sie müssen in der Lage sein, Risikomanagementmaßnahmen im Bereich der Cybersicherheit umzusetzen und zu überwachen. Der Verantwortungsbereich erfordert zur Überwindung der Komplexität, die eigene Sprache und Begrifflichkeit der IT Experten zu durchdringen. Im Beitrag werden konsequent deshalb die Fachbegriffe erläutert und auch einfache Zusammenhänge mit Fallbeispielen erklärt. Eingehend behandelt werden unter anderem das Schwachstellenmanagement, die Risiken und die Kontrolle der Softwarelieferketten – SBOMs, Maßnahmen der Cyberhygiene, und vor allem die Organisation dieser Schutzmaßnahmen, um den Vorwurf des Organisationsverschuldens gegen Geschäftsleiter zu vermeiden. Der zu verantwortende Bereich der Cybersicherheit lässt sich nur durch die Kombination von Rechts- und IT-Beratung bewältigen.

Inhaltsverzeichnis

Cybersicherheit wird zur Chefsache

1. Das ständig steigende Risiko von Cyberangriffen

Cyberangriffe können erheblichen **Schaden** verursachen. Laut einer Studie des Verbands der deutschen Informations- und Telekommunikationsbranche (Bitkom) pendeln sich die jährlichen Schäden bei über 200 Milliarden ein,[1] was etwa einem Viertel des Bundeshaushalts entspricht. Nach dem Allianz Risk Barometer zählen Cyberangriffe mit 40 % neben Betriebsunterbrechungen mit 46 % zu den häufigsten Geschäftsrisiken weltweit.[2] Mehr als jedes dritte Unternehmen war in den letzten zwei Jahren Ziel einer Hackerattacke.[3] Die Täter kommen öfter aus der organisierten Kriminalität. Drei Viertel der Schäden werden durch Cyberattacken verursacht. Erstmals fühlen sich 52 % der Unternehmen in ihrer Existenz bedroht, durch **Datenklau**, **Spionage** oder **Sabotage**, durch den A**usfall von Informations- und Produktionssystemen** sowie die **Störung von Betriebsabläufen**. Häufige Schäden entstehen durch Phishing, Passwortklau und Malware. Sie sind meist eine unmittelbare Folge von sogenannten **Ransomware-Angriffen**, bei denen Computer und andere Systeme blockiert werden und die Betreiber anschließend erpresst werden. Presse und Internet berichten fast täglich über neue Cyberangriffe auf Unternehmen und sonstige Einrichtungen, auf Parlament, Kliniken und sogar auf politische Parteien.

Die FAZ berichtet am 11.5.2024 in ihrem Leitartikel „Im digitalen Dauerfeuer“ über die hohe Zahl von 70 neuen Schwachstellen, die täglich

[1] Pressemitteilung Bitkom, Wirtschaftsschutz 2023, vom 1.9.2023, S. 4,7,9,12,13.

[2] Allianz Risk Barometer 2023.

[3] KPMG Lünendonk-Studie 2023, Von Cyber Security zu Cyber Resilience, Wie Unternehmen auf die steigende Bedrohungslage realgieren; FAZ vom 28.Mai,2024, Cyberangriffe nehmen zu.

erkannt werden.[4] Das Bundeskriminalamt hat am 13. Mai 2024 das Bundeslagebild Cybercrime von 2023 vorgestellt und den Gesamtjahresschaden mit 206 Milliarden angegeben. An Lösegeld für die Daten von Geschädigten wurden 16,1 Milliarden gezahlt. Das Bundeskriminalamt -BKA- weist daraufhin, dass die Dunkelziffer besonders hoch ist, weil viele Angriffe nicht angezeigt werden. Von einem Angriff wurden aktuell der Verbund von Krankenhäusern und eine Gruppe von 72 Kommunen blockiert.[5]

Aufsehen erregte der Angriff der Hackergruppe Storm-0558 im Juni 2023 auf 21 Organisationen und 503 Accounts unter anderem auf E-Mail-Konten des US-Außenministeriums. Abgeschöpft haben die Hacker mit Verbindungen zu China u.a. 60.000 E-Mails des US-Außenministeriums, worauf vom Präsidenten der Cyber Safety Review Board eingerichtet wurde. Sicherheitslücken bei Microsoft waren die Ursache. Ein Sicherheitscode wurde erbeutet und ermöglichte das Einloggen in beliebige E-Mail-Konten. Hacker hatten sich Befugnisse in der Microsoft-Cloud verschafft, was von Microsoft zugegeben wurde. Die fehlende Sicherheitskultur bei Microsoft wurde kritisiert. Schon im April 2021 wurde ein Signaturschlüssel beim Absturz eines Verbrauchersignatursystem erbeutet. Die Sicherheit der Cloudlösungen von Microsoft werden seitdem ernsthaft in Frage gestellt, wenn der Generalschlüssel erschlichen und die Zugriffserlaubnis auf die meisten Cloudanwendungen von Microsoft verschafft werden kann. Der innenpolitische Sprecher der FDP-Fraktion wird mit der politischen Feststellung und Forderung zitiert, der Microsoft-Vorfall zeige, dass selbst die beste Verschlüsselung nichts bringe, wenn die Angreifer den Schlüssel haben und nicht geklärt sei, wie die Angreifer an den Schlüssel gelangen konnten und schließlich warum der Angriff von 2021 nicht früher aufgefallen sei.

Ermittlern aus Hessen ist es aktuell in der „Operation Endgame“ gelungen, das bisher größte Netzwerk Schadsoftware auszuschalten. Über Dropper[6] konnte die Strafverfolgungsbehörde die Kontrolle über das kriminelle System mit dem Zugriff auf hunderttausende Opfersystem übernehmen. Die Ermittler haben die Cyberkriminellen mit deren eigenen Mitteln geschlagen, indem sie nach Schwachstellen im kriminellen System suchten und ausmachen konnten und schließlich mit Droppern ausnutzten.[7]

Mit dem Ruf nach dem Gesetzgeber reagiert die Politik auf die steigenden Risiken durch Cyberangiffe. Gefordert wurde durch gesetzliche Regelungen zum Schutz der kritischen Infrastruktur, IT-Sicherheitslücken konsequent zu schließen, Unabhängigkeit von US-Konzernen anzustreben und auf freie selbst verwaltete Technik umzusteigen.[8]

[4] FAZ vom 11.5.2024, S.17, Im digitalen Dauerfeuer.

[5] FAZ vom 14.5.2024 S. 5, Die Bedrohung durch Cyberangriffe wächst.

[6] Ein Dropper oder Viren-Dropper ist ein eigenständig ausführbares Computerprogramm, das zur Freisetzung eines Computervirus dient. Dropper werden meist für eine Erstinfektion von Cyberkriminellen verwendet.

[7] FAZ vom 31.Mai 2024 Seite 1 im Lokalteil.

[8] Tagesschau vom 8.9.2023.

2. Die neue Geschäftsleiter-verantwortung für IT-Sicherheit als Reaktion des Gesetzgebers

Dieses steigende Risiko soll durch die neuen Regelungen der EU und des Bundes zur Cybersicherheit abgewendet werden. Wegen der Bedeutung des Risikos werden vor allem die Geschäftsleiter ausdrücklich verpflichtet. Sie haften in Zukunft persönlich, wenn sie ihre Pflichten verletzen gemäß § 38 BSIG[9] des Referentenentwurfs vom 7.5.2024 für Schadensersatzforderungen, die aus eigenem Vermögen zu leisten sind.[10] Die Aufmerksamkeit der Geschäftsleiter soll deshalb auf diese neue Rechtslage und ihre Pflichten für die IT-Sicherheit gelenkt werden.

Art. 17 der NIS-2-RL-E verpflichtet die leitenden Organe wesentlicher und wichtiger Einrichtungen zur Umsetzung der konkreten Sicherheitsanforderung, die in Art. 18 NIS-2-RL-E der Unternehmensführung vorgegeben sind, um einen angemessenen Sicherheitsstandard der von ihnen genutzten Netzwerk- und Informationssystemen zu erreichen.

Nach § 14 KRITIS-DachG (KRITIS-Dachgesetz) des Entwurfs eines Gesetzes zur Umsetzung der Richtlinie EU 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen, sind Geschäftsleiter von Betreibern kritischer Anlagen verpflichtet, die von diesen Betreibern zur Einhaltung von § 10 KRITIS-DachG ergriffenen Maßnahmen zu billigen und zu überwachen. Ausdrücklich geregelt ist die Unwirksamkeit von Vereinbarungen mit den Betreibern, auf solche Ersatzansprüche zu verzichten. Die Geschäftsleiter von Betreibern kritischer Anlagen müssen nach § 14 II KRITIS-DachG regelmäßig an Schulungen teilnehmen, worüber die Aufsichtsbehörden Nachweise verlangen können. Bei der Einschaltung von Hilfspersonen bleiben die Leitungsorgane letztverantwortlich. Die Bedeutung dieser Pflicht wird durch die ausdrückliche Haftungsregelung unterstrichen.

Die gleiche Regelung zur Geschäftsleiterverantwortung findet sich in § 38 BSIG im Referentenentwurf des NIS-2-UmsuCG–NIS2 Umsetzungs- und Cybersicherheitsstärkungsgesetz. Nach § 39 Abs.1 BSIG haben die Betreiber kritischer Anlagen die Erfüllung der Anforderungen nach §§ 30,31 BSIG zum Risikomanagement „besonders wichtiger“ und „wichtiger“ Einrichtungen und zu den besonderen Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen nachzuweisen.

3. Das Organisationsrisiko der Verantwortungsdiffusion

Der Gesetzgeber hat offensichtlich das allgemeine Risiko der Verantwortungsdiffusion erkannt und eine für Geschäftsleiter ungewöhnlich scharfe Verantwortungs- und Haftungsregelung formuliert, die sich alle Organe von Unternehmen bewusst machen sollten, um durch organisatorische Vorkehrungen im Compliance-Management-System ihr Haftungsrisiko zu vermeiden. Diese harte Regelung für Geschäftsleiter soll im Folgenden mit Hintergrundinformationen näher erläutert werden.

[9] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen. BSIG, BSI-Gesetz.

[10] Plate, NIS2 – und jetzt?, in iX 2024 S. 53.

Der BGH hat in seinem Schubstreben-Urteil entschieden, dass Pflichten an namentlich benannte Mitarbeiter und an ebenfalls mit Namen benannte Vertreter zu delegieren sind.[11] Entsprechend dieser Rechtsprechung schreibt das Gesetz vor, die Verantwortung für die Cybersicherheit eindeutig und nicht weiterdelegierbar an die Geschäftsleiter zu delegieren, die namentlich bekannt und im Handelsregister veröffentlicht sind. Entgegen dieser gesetzlichen Anforderung wird in der Unternehmenspraxis nämlich regelmäßig der Wunsch geäußert, die Pflichten mit Funktionen und nicht mit Namen zu verlinken. Dadurch wird die Verantwortung diffus verteilt und namenlos. Der BGH verpflichtet deshalb zur Delegation an namentlich benannte Pflichtenträger, weil nur so wirksame Kontrollen möglich sind. Die Verhaltensforschung erklärt diesen regelmäßig geäußerten Vorbehalt gegen die Namensnennung mit dem Begriff der „Verantwortungsdiffusion“. Erwiesen ist in der Verhaltensforschung, dass die Bereitschaft, gegen Missstände oder Notfälle einzugreifen, höher ist, wenn ein Mitwisser oder Zuschauer allein ist, als wenn er in Gesellschaft anderer die Notsituation erlebt. Wenn mehrere Zeugen eines Missstands sind, ist sich jeder einzelne der Tatsache bewusst, dass andere eingreifen könnten. Der Prozess der Verantwortungsdiffusion wird verstärkt, wenn die Anzahl der Mitwisser zunimmt. So erklärt sich, dass Rechtsverstöße in Unternehmen bekannt sind, aber keiner einschreitet und sich einer auf den andern verlässt. Hinweisgebersysteme und namentliche Delegationen von Pflichten an Einzelpersonen können abhelfen.[12]

Die Verantwortung von Vorständen und Geschäftsführern für die Einhaltung der Legalitätspflicht ist vom BGH in ständiger Rechtsprechung entschieden. Danach kann das Organ einer Gesellschaft die Oberaufsicht über die Einhaltung aller einschlägigen Rechtsvorschriften nicht delegieren und nicht abbedingen.[13]

Bei § 14 KRITIS-DachG und § 38 BSIG handelt es sich also um nichts Neues, sondern um eine ständige, schon lang bekannte und nunmehr auch gesetzlich geregelte kodifizierte Rechtsprechung. An der Verantwortung der Geschäftsleiter bestehen keine Zweifel. Die ausdrückliche und scharfe Regelung im Gesetz hat offenbar einen besonderen Grund, der sich aus der Stellungnahme und den Erfahrungen des BSI ergibt.

Das Bundesamt für Sicherheit in der Informationstechnik – BSI – äußert sich skeptisch zur bisherigen Delegation der Verantwortung für

---

[11] BGH vom 17.10.1967, NJW 1968,247 – Schubstreben Urteil.

[12] Jonas/Stroebe/Hewstone, Sozialpsychologie, 5.Aufl., S.302 unter Hinweis auf den verfilmten Fall, bei dem 38 Augenzeugen gegen den Mord an Kitty Genovese auf offener Straße in New York nicht eingeschritten sind und die weltweite Forschung über Verantwortungslosigkeit ausgelöst hat, S. 298.

[13] RG, 14.12.1911 – VI 75/11, RGZ 78, 107 (Kutscher-Urteil); RG, 12.1.1938 – VI. 172/37, RGJW 1938, 1651 (Kleinbahn-Urteil); RG, 25.2.1915 – VI 526/14, RGZ 87 (1916), 1 (Heilsalz-Urteil); BGH, 25.10.1951 – III ZR 95/50, BGHZ 4, 1 (Benzinfahrt-Urteil); BGH, 9.2.1960 – VIII ZR 51/59, BGHZ 32 (1960), 53 (Besitzdiener-Urteil).

Informationssicherheit.[14] Die Informationssicherheit werde häufig vernachlässigt und falle hinter dem Tagesgeschäft zurück. Durch die unklare Aufteilung von Zuständigkeiten werde die Verantwortung für Informationssicherheit zum „Problem anderer Leute“. Sie werde so lange hin- und hergeschoben, bis keiner sie mehr zu haben glaubt. Weil die Priorisierung der Cybersicherheit oft fehlt, komme es zu den Cyberattacken gegen Unternehmen und andere Einrichtungen, Schäden in Höhe von über zweihundert Milliarden im letzten Jahr 2023.

Nach dem Erkennen des Risikos der Verantwortungsdiffusion hat das BSI offenbar den Gesetzgeber von der Notwendigkeit einer neuen ausdrücklichen gesetzlichen Regelung der Delegation der Verantwortung an Geschäftsleiter überzeugt. Die rechtliche Verbindlichkeit durch eine gesetzliche Regelung ist deutlicher als die einer höchstrichterlichen BGH-Rechtsprechung aus Einzelfallentscheidungen, die nur juristischen Experten bekannt sind und nicht zum Allgemeingut gezählt werden können.

Es fehlte bisher an IT-Governance und der klaren Delegation der Pflichten zur Cybersicherheit. Es reicht offenbar nicht aus, sich auf IT-Abteilungen zu verlassen.

In der Unternehmenswirklichkeit wird die IT-Infrastruktur von vielen verschiedenen Teams betrieben, jeweils getrennt für den Betrieb des Servers und des Betriebssystems, für die darauf laufende Datenbank und für die Anwendung. Hinzu kommt die IT-Security. Alle Teams sind an dem IT-Change-Management beteiligt, wodurch die Entscheidungsverfahren erschwert und verzögert und die Verantwortungsdiffusion gefördert wird, weil die IT-Sicherheit zwischen alle Stühle gerät.[15] Nach den Umfragen der Lünendonk Studie in Zusammenarbeit mit KPMG sind nur 14 % des T0P-Managements an der Entwicklung einer Cyberstrategie beteiligt. In neun von zehn Unternehmen ist die IT-Abteilung für die Entwicklung der Cyberstrategie verantwortlich, in jedem vierten Unternehmen ist sie sogar ausschließlich zuständig.[16] Cybersicherheit wird vernachlässigt.

Cybersicherheit muss deshalb zu Recht zur Chefsache gemacht werden. Ein Cybervorstand muss mit der Bereitschaft zum Managementsystem für Informationssicherheit – ISMS - eingesetzt werden.

Die meisten Hacker kommen über interne Türen in IT-System, indem unbesorgt auf nicht erkannte Phishing-Mails geklickt wird. Auch das bewusste Öffnen digitaler Türen durch illoyale Mitarbeiter kann Hackerangriffe begünstigen. Aus der Statistik des BSI ergibt sich, dass in 13 % der Angriffsfälle Softwareprodukte ohne funktionierende Zugangskontrollen das Eindringen und den Missbrauch ermöglichten.[17]

Dem Cybervorstand ist zu raten, sich am BSI Grundschutzkompendium zu orientieren. Es umfasst Hinweise zur Umsetzung eines Managementsystems für Informationssicherheit. Benannt werden die unterschiedlichen Risiken

[14] Standard 200-2 zur IT Grundschutz-Methodik.

[15] Frank und Casper, iX 12/2023, unter der Überschrift, „Zwischen allen Stühlen“.

[16] KPMG Lünendonk-Studie 2023, Von Cyber Security zu Cyber Resilience, Wie Unternehmen auf die steigende Bedrohungslage reagieren, S.28.

[17] BSI, Die Lage der IT- Sicherheit in Deutschland 2023, S. 34.

und die Handlungsempfehlungen zur Abwendung dieser Risiken. Ebenfalls ergeben sich Handlungsempfehlungen aus der ISO-Norm 27001, nach der auch Zertifizierungen möglich sind.

Zum ISMS gehören - ohne Anspruch auf Vollständigkeit - folgende Maßnahmen, die Geschäftsleiter zur Erfüllung ihrer neuen Aufgabe berücksichtigen müssen:

Erstens gehört zum ISMS ein Überwachungssystem, mit dem Angriffe zu erkennen sind, was auch von externen Dienstleistern angeboten wird.

Zweitens zählt zum ISMS ein Notfallplan für den Fall des Cyberangriffs mit Ablaufdiagramm. Für den Ernstfall ist ein Maßnahmenkatalog zu erstellen, aus dem sich ergibt, wer, was und wann zu tun hat. Pflichten müssen für den Hackerangriffsfall klar delegiert sein. Zunächst ist die Wiederherstellung der IT-Systeme zu sichern. Die Delegation der Pflichten gehört als zweite von sechs Organisationspflichten nach der Rechtsprechung des BGH zum Organisationsverschulden zum unverzichtbaren Teil eines Compliance-Management-System. Zum Notfallplan zählen auch das Sichern der Daten und der schnelle Shut-Down aller Systeme.

Drittens sind die Behörden und die Betroffenen zu informieren. Diese Meldungen sind die Grundlagen für eventuelle Bußgeld- und Schadensersatzrisken.

Viertens hat der Cybervorstand durch Schulungen und fachliche Unterstützungen Grundkenntnisse und Kompetenz zur Cybersicherheit zu erwerben, was sich aus § 38 BSIG und § 14 KRITIS-DachG ergibt.

Fünftens ist die Cybersicherheit als permanente Dauerpflicht zu verstehen, die eine ständige Verbesserung und Nachbesserung des Cyberschutzes verlangt. Die Cybersicherheit ist ständig zu aktualisieren und zwar nicht nur zur Rechtslage, sondern auch zur technischen Sachlage im Rahmen eines Schwachstellenmanagements. Neue Techniken zum Erkennen von Risiken und zu ihrer Abwehr sind in das ISMS aufzunehmen.[18]

4. Die Informationsbeschaffungs-pflicht des Cybervorstands

Geschäftsleitern fehlt in der Regel die fachliche IT- Kompetenz, Cyberrisiken und die Möglichkeiten der Abwehr einzuschätzen. Der IT- Laie erkennt seine IT-technische Inkompetenz nicht, weil ihm dazu schon die Kompetenz fehlt. Dies hat zur Folge, dass er nicht in der Lage ist, Cyberrisiken und IT-Schwachstellen zur erkennen und zu erfragen. Diesen Zusammenhang und das dadurch offengelegte Organisationsrisiko erklärt die Verhaltensökonomie und Psychologie mit dem Dunning-Kruger-Effekt.[19] Die zur Organisation verpflich-

[18] Deutscher Anwaltsspiegel, CyberSecurity ist C-Level Aufgabe, Verschärfte Haftung für Leitungsorgane in Unternehmen: Kommt der Cybervorstand, 24. Mai 2023, von Dr. Kristina Schreiber und Dr. Eren Basar.

[19] Rack, Compliance Berater 6/2017 S. 206 Das Rechtsrisiko des Dunning-Kruger-Effekts- eine psychologische Erklärung für Rechtsver-

teten Geschäftsleiter müssen sich dieser Risikolage in Form einer bekannten menschlichen Schwäche bewusst sein, und deshalb routinemäßig sich in allen IT-Sicherheitsfragen beraten lassen. Die sicherste Organisation der Cybersicherheit wäre die Schaffung eines Cybervorstands mit ausgewiesener eigener IT-Kompetenz, was inzwischen schon gefordert wird.[20] Geschäftsleiter ohne eigene IT-Kompetenz sind von den im Folgenden thematisierten Anforderungen an ein Schwachstellenmanagement überfordert.

Die einschlägige Organisationspflicht des Vorstands zum Informationsmanagement im Unternehmen ist einzuhalten. Daraus ergeben sich erhebliche Konsequenzen für das IT-Sicherheits-Management. Gewollte Unkenntnis oder auch Willful Blindness entlastet den Vorstand nicht. Im Wissensaufspaltungsurteil hat der BGH entschieden, nicht das persönliche präsente Wissen von Angestellten zählt, sondern das typischerweise aktenmäßig festgehaltene Wissen, zu dem alles gehört, was der Rechtsverkehr von einem Unternehmen als dokumentiertes Aktenwissen erwarten und was später einmal rechtserheblich werden kann, dessen Verfügbarkeit zu organisieren ist. Erfüllt der Vorstand diese Organisationspflicht nicht, müsse die juristische Person, das Unternehmen als AG oder GmbH, sich materiell rechtlich so behandeln lassen, als habe sie von der Information Kenntnis. In späteren gerichtlichen Verfahren spielt es eine Rolle, was einmal vorhersehbar, vermeidbar und zu verantworten war. Rechtserhebliche Informationen müssen im Unternehmen deshalb verfügbar gehalten und weitergeleitet werden, es muss nachgefragt und genutzt werden und es wird bei Unkenntnis unterstellt. In seiner ISION Entscheidung verlangt der BGH vom Geschäftseiter bei eigener Inkompetenz – in diesem Fall seiner rechtlichen Inkompetenz - , sich seine eigene fachlichen Unzulänglichkeit bewusst zu machen und sich beraten zu lassen.[21] Die häufige Neigung zur Beratungsresistenz ist zu vermeiden. Besonders das Wissen in der IT-Sicherheit zu organisieren, wird wegen der grenzenlosen Vielzahl von Schwachstellen und deren Abwendungsmöglichkeit zu einer kaum zu bewältigenden Organisationsaufgabe im Rahmen eines Managementsystem für Informationssicherheit (ISMS). Nur mit digitalen Datenbanken ist die Aufgabe zu bewältigen.

Der Geschäftsleiter muss zu seiner Beratung in allen Cyber- und IT Sicherheitsfragen sich von nachweislich kompetenten Angestellten mit Stabsfunktion oder von Dienstleistern beraten lassen und diese verpflichten, ihm alle einschlägigen Rechtspflichten zur Einhaltung nachzuweisen. Vor allem sind die Berater von Geschäftsleitern zu verpflichten, über Schwachstellen in der IT des Unternehmens aufzuklären. Die Risikolage kann sich durch die täglich steigende Anzahl von Schwachstellen und die Anzahl der Patches verändern, so dass eine systematische Aktualisierung der

---

stöße wegen unterlassener präventiver Rechtsprüfung.

[20] Wie Fn.11, Schreiber und Basar.

[21] BGHZ 132,30,36, BB 1996, 924 Wissensaufspaltungs-Urteil; Rack, Compliance Berater, 2/2013, Informationsmanagement als Organisationspflicht, mit weiteren Nachweisen aus der BGH-Rspr.

BGH, 20.9.2011 – II ZR 234/09 (OLG Hamburg), NJW – RR 2011, 1670 (ISION Urteil).

Risiko- und Pflichtenlage erforderlich ist. Die für das Unternehmen einschlägigen Cyber- und IT-Risiken sind fortlaufend zu erfassen und in einer jeweils aktuellen Übersicht dem für die IT-Sicherheit verantwortlichen Geschäftsleiter vorzustellen und als Beweise zu sichern, da von den Aufsichtsbehörden jederzeit der Nachweis gefordert werden kann.

5. Die Organisation der Cyber- und IT-Sicherheit mit dem Compliance-Management-System RECHT IM BETRIEB

5.1 Die Organisationspflichten

Wie jedes Risiko eines Rechtsverstoßes ist auch das Risiko des Verstoßes gegen Rechtsvorschriften zu Vermeidung und Verringerung des Cyberrisikos zu organisieren, was mit dem Compliance-Management-System RECHT IM BETRIEB bewältigt werden kann, dem das folgende Schema zugrunde liegt. Danach ist zu unterscheiden einerseits zwischen den sechs Organisationspflichten und andererseits den zu organisierenden Pflichten, die den Schutz vor Cyber- und IT-Risiken bezwecken.
Die sechs Organisationspflichten ergeben sich aus der einschlägigen und faktisch bindenden Rechtsprechung des BGH zum Organisationsverschulden[22] und der DIN ISO 373001 zur guten Unternehmensführung durch Geschäftsleiter. Rechtspflichten zum Schutz vor Risiken sind erstens zu ermitteln, zweitens zu delegieren, drittens zu aktualisieren, viertens zu erfüllen, fünftens zu kontrollieren und sechstens zu dokumentieren. Die nach diesen sechs Organisationspflichten zu organisierenden Rechtspflichten ergeben sich zum Schutz und zur Abwehr von Cyber- und IT-Risiken aus den Entwürfen zum KRITIS-DachG und dem NIS-2-UmsuCG sowie dem neuen BSIG. In RECHT IM BETRIEB sind die einzuhaltenden Rechtspflichten ermittelt und markiert und sind an Mitarbeiter zu delegieren, zu aktualisieren, einzuhalten, auf ihre Einhaltung zu kontrollieren und zur Beweissicherung und zum Nachweis gegenüber Aufsichtsbehörden zu dokumentieren.
Im Folgenden werden die Einzelvorschriften zu den Organisationspflichten aus den neuen Gesetzen zur IT- und Cybersicherheit nach den einschlägigen Paragraphen benannt.

Erstens sind die Risikosachverhalte und die Rechtspflichten zur präventiven Abwehr der Risiken zu ermitteln[23] und zu identifizieren. Die Organisationspflicht zur Ermittlung von Cyberrisiken und von Schutzmaßnahmen zu deren präventiver Abwehr ergeben sich aus §§ 30 Abs.1,2 und 31 Abs.2 BSIG. Damit umgesetzt wird Art.21 der NIS2 Richtlinie. Die Ermittlung, Analyse und Bewertung der Risiken der Betreiber kritischer Anlagen ist in § 9 KRITIS-DachG und die Ermittlung der Pflichten zur Risikoabwehr ist in § 10 KRITIS-DachG geregelt.

[22] Rack, Compliance Berater. 8/2014, Die rechtlichen Voraussetzungen für ein Compliance-Management-System, Seite 279 mit allen Urteilen von RG und BGH.

[23] Rack, Compliance Berater, 5/2013, S. 191, Die Organisationspflicht nach der höchstrichterlichen Rechtsprechung mit Einzelnachweisen zur Risikoanalyse.

Zweitens sind die einschlägigen Rechtspflichten zu delegieren.[24] In 21 Einzelentscheidungen haben RG und BGH die Pflicht zu Delegation konkretisiert. Neu gesetzlich und erstmalig geregelt ist die Geschäftsleiterverantwortung nahezu wortgleich in § 38 BSIG sowie in § 14 KRITIS-DachG. Die Verantwortung der Cyber- und IT-Sicherheit wird an den jeweiligen Geschäftsleiter, an das Organ des Unternehmens, delegiert. Es handelt sich um eine Organisationspflicht. Sie hat ein Geschäftsleiter schon aufgrund seiner Organstellung zu erfüllen. Delegiert werden müssen vom Geschäftsleiter an verantwortliche Mitarbeiter oder Dritte die zu organisierenden Pflichten, z.B. unter anderem die Pflichten zum Management für Schwachstellen, für die Softwarelieferketten, für Cyberhygiene, für Risikoanalyse, für Zugriffskontrollen, für Back-up und Wiederherstellung nach Notfällen und Krisen. Damit ist das Risiko der Verantwortungsdiffusion abzuwenden.

Drittens sind die Pflichten zu aktualisieren.[25] Vor allem sind auch die Verkehrssicherungspflichten zu aktualisieren, was sich aus dem Kupolofen Urteil des BGH ergibt. Der Gesetzgeber und die Verwaltung können nicht sämtliche Schadensrisiken eines Unternehmens erfassen. Deshalb sind Unternehmen zur Selbstregulierung in Form von Verkehrssicherungspflichten dazu verpflichtet, Risiken aus der Unternehmenstätigkeit zu ermitteln und im Unternehmen abzuwenden.[26] Diese Rechtslage gilt ganz besonders für die Cybersicherheit und die IT-Sicherheit für Betreiber kritischer Anlagen, da sich die Schwachstellen und damit die Risikolage täglich ändern kann und die Schutzmaßnahmen im gleich schnellen Rhythmus wie die Verkehrssicherungspflichten aktualisiert werden müssen. Zu erinnern ist, dass monatlich 2.500 Schwachstellen dazukommen und die passenden Patchs nicht im gleichen Tempo nicht entwickelt und offenbar auch erst gar nicht gezählt werden können. Die Abwehr der Cyberisiken ist zu Priorisieren. Die gleiche Aktualisierungspflicht zur Anpassung an den jeweils technischen Fortschritt ergibt sich aus dem Hühnerpest Urteil des BGH, in dem einem Tierarzneimittelhersteller vorgeworfen wurde, nicht die neueste Abfülltechnik verwendet zu haben, was seine Pflicht gewesen wäre.[27]

Viertens sind die Pflichten zu erfüllen[28]. Gesetzlich geregelt ist die Erfüllung in § 39 BSIG sowie in §§ 10 und 11 KRITIS-DachG.

Fünftens ist die Einhaltung der Pflichten zu kontrollieren. Gesetzlich geregelt ist die Kontrollpflicht in § 14 Abs.1 KRITIS-DachG und § 38 Abs.1 BSIG.

---

[24] Rack, Compliance Berater, 6/2013, S.231, Die Organisationspflicht zur Delegation.

[25] Rack, Compliance Berater 7/2013, Die Aktualisierung von Unternehmenspflichten, S. 275.

[26] Kupolofen Urteil BGHZ 92, S. 143.

[27] BGH, 26.11.1989 – VI ZR 212/66; BGHZ 51, 91 – Hühnerpestentscheidung.

[28] Rack, Compliance Berater 8/2014 S. 110,115, Die rechtlichen Voraussetzungen eines Compliance-Management-Systems, mit Einzelnachweisen aus Urteilen zu jeder Organisationspflicht.

Sechstens ist die Einhaltung der Rechtspflichten eines Unternehmens zu dokumentieren.[29] Gesetzlich geregelt ist die Pflicht zur Dokumentation in §§ 30 Abs. 1, 39 BSIG. Vor allem lässt sich der Nachweis von den Geschäftsleitern mit der Organoberaufsichtsmaske führen. Ob und welche Rechtspflichten ermittelt, delegiert, eingehalten, kontrolliert und schließlich zur Beweissicherung auch dokumentiert sind, erschließt sich für die Geschäftsleiter und allen Dritten auf einen Blick. Mit der Oberaufsichtsmaske wird im Compliance-Management-System RECHT IM BETRIEB dokumentiert, dass der jeweilige Geschäftsleiter seine Pflicht nach § 14 KRITIS-DachG und nach § 38 BSIG eingehalten hat, die Umsetzung der Schutzmaßnahmen zu überwachen. Das Bundesamt kann nach § 39 BSIG und die Aufsichtsbehörden nach § 14 Abs.2 und § 11 Abs.1 und Abs. 5 KRITIS-DachG geeignete Nachweise verlangen. Die Oberaufsichtsmaske eignet sich als Nachweis zur Erfüllung seiner Überwachungspflichten als Geschäftsleiter über die Einhaltung aller Rechtspflichten zur IT- und Cybersicherheit.

5.2 Die zu organisierenden Rechtspflichten

Die Schutzmaßnahmen gegen Cyberangriffe, die von den Geschäftsleitern zu billigen und zu überwachen sind, und für die er auch bei Einschaltung von Hilfspersonen die Letztverantwortung trägt,[30] ergeben sich aus § 30 BSIG, mit dem Art.21 der europäischen Cybersicherheits- und Resilienzrichtlinie NIS2 umgesetzt wird.

Nach § 30 Abs.2 BSIG sind Maßnahmen nach § 30 Absatz 1 BSIG sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informations-technik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risiko-

[29] Rack, Compliance Berater, 8/2014, Die rechtlichen Voraussetzungen für ein Compliance-Management-System, Die Organisationspflichten zur Dokumentation nach der Rechtsprechung. S.289.

[30] Referentenentwurf zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, Stand 7.5.2024, Seite 155 zu § 38 Abs.1 BSIG.

managementmaß-nahmen im Bereich der Sicherheit in der Informationstechnik,

7. Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Welche konkreten Schutzmaßnahmen in der Praxis umgesetzt werden können, um Cyberangriffe zu verhindern und die Cybersicherheit zu erhöhen, soll im Folgenden dargestellt werden. Geschäftsleiter sind verpflichtet, den Stand der Technik einzuhalten und internationale Vorschriften zu berücksichtigen. Um seine umfassende Verantwortung für Cybersicherheit wahrnehmen und seine Organisationspflicht erfüllen sowie seine Haftung vermeiden zu können, muss ein Geschäftsleiter sich mit den folgenden Themen beschäftigen, um zumindest seinen Beratungsbedarf zu erkennen und die weiterführenden Fragen stellen zu können.

6. Besondere Anforderungen an Risikomanagement Maßnahmen

Nach § 30 Abs. 2 Nr. 1 BSIG sind Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik zu erstellen. Die Risikoabwehrmaßnahmen sollen im Verhältnis zum drohenden Risiko stehen.[31]

Von Betreibern kritischer Anlagen nach § 31 BSIG sind Systeme zur Angriffserkennung einzusetzen, Bedrohungen sind zu identifizieren und zu vermeiden sowie Beseitigungsmaßnahmen vorzusehen. Der Stand der Technik ist zu beachten.

Das Risiko ist allgemein als eine Beziehung zwischen der Schadensursache und dem Schaden als Wirkung sowie einem Erfahrungssatz zu verstehen, nachdem auf eine Schadensursache mit Wahrscheinlichkeit ein Schaden eintritt, wenn er nicht durch ein Schutzmaßnehme verhindert wird, wobei die Schutzmaßnahme eine Rechtspflicht darstellt, Diese allgemein geltende Dreiteilung eines Risikos in erstens die Ursache, zweitens die Wirkung und drittens den Erfahrungssatz als Aussage über das Verhältnis von Ursache und Wirkung , wonach auf eine bestimmte Ursache nach geltenden Erfahrungssätzen mit hoher Wahrscheinlichkeit eine Schaden als Wirkung folgt, ergibt sich vor allem aus der Rechtsprechung des BGH im IKB Urteil.[32]

---

[31] Referentenentwurf zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, Stand 7.5.2024, Seite 147 zu § 30 Abs.1 BSIG.

[32] IKB Urteil BGH, 2.2.1996 – V ZR 239/94, BGHZ 132,30, BB 1996, 924.

Auf dem speziellen Risikogebiet der Cyber- und IT-Sicherheit sind unter anderem folgende Schadensursachen zu beachten,

- die Schwachstellen der IT im Unternehmen von Betreibern kritischer Anlagen ohne Schutzmaßnahmen,
- unsichere Softwarelieferketten,
- fehlende Notfallpläne zur Bewältigung von Sicherheitsvorfällen,
- fehlendes Back-up-Management,
- lückenhafte Cyberhygiene,
- unzulängliche Zugriffskontrollen,
- fehlende Verschlüsselung,

und die daraus folgenden Cyberangriffe mit Vorfällen und Schäden als Wirkung zu verstehen. Die Erfahrungen über das Verhalten von Hackern beim Ausnutzen von Schwachstellen ohne ausreichendes Schwachstellenmanagement mit effektiven Schutzmaßnahmen begründen die Wahrscheinlichkeit eines Vorfalls für einen drohenden Angriff.

Der Stand der Technik dient dem Erfassen der jeweils aktuellen Erfahrungen beim Erkennen und Vermeiden von Cyberattacken und deren Folgen. Schon jetzt ist festzuhalten, dass die Technik von Cyberangriffen und Cyberschutzmaßnahmen sich ständig ändern und ein hoher Aktualisierungsbedarf entsteht. Wenn monatlich 2.500 Schwachstellen neu erfasst werden, müssten die Abwehr- und Schutzmaßnahmen durch Patches im gleichen Rhythmus aktualisiert werden. Da die Bewältigung als unrealistisch anzusehen ist, muss priorisiert werden, was später noch vertieft wird.

7. Das Schwachstellen Management als Cyber-Risikovorsorge

Nach § 38 Abs.1 i.V.m. § 30 Abs.2 Nr. 5 BSIG ist der Geschäftsleiter zum Schwachstellen Management und zu deren Offenlegung verpflichtet, sie zu billigen und ihre Umsetzung zu überwachen.

Eine Sicherheitslücke oder eine Schwachstelle ist auf dem Gebiet der Informationssicherheit ein Fehler in einer Software oder einer Hardware, durch den ein Programm mit Schadwirkung (Exploit) oder ein Angreifer in ein Computersystem eindringen kann.

Schwachstellen in IT-Systemen ermöglichen das Eindringen von Hackern zur Erpressung, Datenklau, Sabotage, Werkspionage, Abschöpfen von Geschäftsgeheimnissen, Störung der Produktionsabläufe und zum Ausfall von Informationssystemen. Die wichtigste Quelle für Schwachstelleninformationen ist die National Vulnerability Database (NVD), die vom US National Institute of Standards an Technology (NIST) betrieben wird. Sie veröffentlicht fortlaufend neue Schwachstellen. Bis 2016 wurden jeden Monat etwa 10 Jahre lang etwa 500 neue Schwachstellen in Softwareprodukten gefunden. Ab 2017 wurden dreimal mehr Schwachstellen gefunden, in den drei Quartalen 2023 waren es mehr neue als in 2014 bis 2016 zusammen. Aktuell liegt die Anzahl neuer Schwachstellen im Durchschnitt beim fünffachen von 2016 also bei 2.500 im Monat, was die steigende Tendenz zeigt. Der Anspruch, sie alle zu beheben, gilt als unrealistisch.[33]

Zu erwägen wäre bei dieser Einschätzung die rechtliche Unmöglichkeit einer solchen Pflichterfüllung für den Geschäftsleiter nach § 275 BGB.

[33] Frank und Casper, iX 12/2023, Schwachstellenmanagement: mehr als Scannen und Finden, Seite 50 mit aufschlussreicher Abbildung 2 zum Stand von 19.10.2023.

Der Gesetzgeber hat jedoch in Kenntnis der kaum zu bewältigenden Aufgabe die Pflichten der Geschäftsleiter im Gesetz vorsorglich unter den Vorbehalt der Verhältnismäßigkeit gestellt. Das Gesetz verlangt deshalb in § 30 Abs.1 BSIG verhältnismäßige technische und organisatorische Maßnahmen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. In § 10 KRITIS-DachG werden die Betreiber kritischer Anlagen verpflichtet, geeignete und verhältnismäßige, technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu ergreifen. Nach § 31 Abs.2 BSIG soll der erforderliche Aufwand zum Identifizieren von Bedrohungen den geeigneten Beseitigungsmaßnahmen nicht außer Verhältnis zu den Folgen des Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen. Der Umgang mit Schwachstellen besteht darin, Schwachstellen regelmäßig und kontinuierlich zu identifizieren, sie für die Umgebung im Unternehmen zu bewerten, um sie zu priorisieren, d.h. zu entscheiden, was zuerst und vorrangig zu veranlassen ist, mit angemessenen Maßnahmen zu behandeln und um schließlich damit Schäden zu verhindern oder zu verringern. Die drei Kernaufgaben sind

- das Identifizieren,
- das Priorisieren und
- das Behandeln.

Die wichtigste Aufgabe ist das Priorisieren.[34] Rechtlich wird damit das Verhältnismäßigkeitsprinzip angewandt[35]. Wenn nicht alle Schwachstellen wegen der großen Zahl verhindert werden können, müssen sie soweit wie möglich behandelt werden. Zur Einhaltung des Verhältnismäßigkeitsprinzips müssen Schwachstellen bewertet werden, um eine Rangfolge zu ermitteln, nach der sie zu bearbeiten sind.

8. Bewertung, Auswahl und Vorrangsbehandlung von Schwachstelle

Zur Bewertung von Schwachstellen wird auf den offenen Standard verwiesen, den Common Vulnerability Scoring System (CVSS), der von der US National Infrastructure Advisory Council (NIAC) erstellt und veröffentlicht wird. Aktuell betrieben wird dieser Standard von dem Forum of Incident Response und Security Teams (FIRST). Der CVSS-Score repräsentiert die Relevanz von Schwachstellen und setzt sich aus verschiedenen Eigenschaften der Schwachstelle, aus Metriken[36], zusammen. Er

[34] Frank und Casper, iX, 12/2023 Schwachstellenmanagement: mehr als Scannen und Finden, S. 50 f. Abbildung 1.

[35] Referentenentwurf zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, Stand 7.5.2024, Seite 147 zu § 30 Abs.1 BSIG.

[36] Eine **Softwaremetrik**, oder kurz **Metrik**, ist eine (meist mathematische) Funktion, die eine Eigenschaft von Software in einen Zahlenwert, auch **Maßzahl** genannt, abbildet. Hierdurch

berechnet sich aus komplexen Formeln und gibt einen Maßstab darüber ab, wie die Schutzziele der Vertraulichkeit, der Integrität und der Verfügbarkeit betroffen sind.

Vor allem kann er den verantwortlichen Geschäftsleitern eine Hilfe für die Entscheidung darüber bieten, welche der vielen Schwachstellen vorrangig zu behandeln sind.[37] Zu berücksichtigen sind außerdem, der Schutzbedarf der bedrohten Systeme, die Verfügbarkeit von Patches[38] als Gegenmaßnahmen und Nachbesserungen, die Wahrscheinlichkeit der Ausnutzung der Schwachstelle, die das Exploit Prediction Scoring System (EPSS) von FIRST bietet, das für alle veröffentlichten Schwachstellen tagesaktuell und kostenfrei zur Verfügung gestellt wird.[39] Die Schutzbedürftigkeit und damit die Entscheidung über den Vorrang einer Schutzmaßnahme kann vom jeweiligen Unternehmen abhängen. Forschungsergebnisse, Medizindaten oder Produktionsdaten können unterschiedlich je nach Unternehmenszweck bewertet werden. Dringend zu empfehlen ist die Dokumentation des Schwachstellenmanagements, um die Beweise für die Entlastung des Geschäftsleiters zu sichern, da dieser die Beweislast für die Erfüllung seiner Pflichten nach § 38 i.V.m.§ 30 BSIG trägt. Nach § 93 Abs. 2 S. 2 AktG gilt der Grundsatz der Beweislastumkehr, wonach die Geschäftsleiter die Beweislast trifft, wenn streitig ist, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben. In der Rechtsprechung gilt für Unternehmen der Grundsatz der Beweislastumkehr und begründet damit die Pflicht zur ständigen Dokumentation, weil vorher nicht klar ist, wann der Schaden eintreten wird.

Eine Marktübersicht zu Anbietern von Werkzeugen für die Behandlung von Schwachstellen bietet der zitierte Aufsatz.[40]

9. Der Wettlauf um die Schwachstellen zwischen Hackern mit Vorsprung und Entwicklern im Rückstand

Schwachstellen werden mit unterschiedlichen Zielen und Absichten behandelt. Hacker spüren Schwachstellen auf, um sie zum eigenen Vorteil und zum Nachteil von IT-Nutzern, Entwicklern und sonstigen Berechtigten zu missbrauchen. Hacker verheimlichen erspähte Schwachstellen oder betreiben Handel mit anderen Hackern.

Die Entwickler dagegen ermitteln Schwachstellen, um sie zu beheben und offenzulegen.[41] Über diese Szenarien müssen sich Geschäftsleiter in Zukunft im Rahmen ihrer Organisati-

---

werden formale Vergleichs- und Bewertungsmöglichkeiten geschaffen.

[37] Frank und Casper, iX, 12/2923 Schwachstellenmanagement: mehr als Scannen und Finden, S. 50 f. Abbildung 4.

[38] Ein Patch ist eine Nachbesserung oder Korrekturauslieferung für Software oder Daten aus Endanwendersicht, um Fehler zu beheben, bekannt gewordene Sicherheitslücken zu schließen sowie bislang nicht vorhandene Funktionen nachzurüsten.

[39] Frank und Casper, iX, 12/2023 Schwachstellenmanagement: mehr als Scannen und Finden, S. 50 f. Abbildung 4.

[40] Frank und Casper, iX,12/2023, Werkzeuge für das Schwachstellenmanagement, S.58 f.

[41] BSI, Die Lage der IT- Sicherheit in Deutschland 2023, S. 34.

onspflicht zum Schwachstellen Management informieren.

9.1 Bug-Bounty-Programme zur systematischen Behebung von Schwachstellen durch Entwickler und Sicherheitsforscher

Übersetzt werden diese Programme sinngemäß mit „Kopfgeld Programme für Programmfehler“. Es sind Initiativen zur Identifizierung, Behebung und Bekanntmachung von Fehlern in Software unter Auslobung von Sach- und Geldpreisen für die Entdecker von Schwachstellen. Microsoft organisiert Bug-Bounty-Programme für Internetdienste und getrennt davon für Computer-Betriebssysteme. Prämien werden für unterschiedliche Schwachstellen von 500 bis 250.000 Dollar ausgelobt, je nachdem welche Angriffsszenarien oder Lücken von Entdeckern oder Sicherheitsforschern angezeigt werden.[42]

Die Sicherheit von freier und quelloffener Software wird gestärkt durch das EU-Fossa-2-Projekt, bei dem unabhängige Forscher und Entwickler von Deloitte aufgerufen sind, Sicherheitslücken in jeweils ausgeschriebenen Open-Source-Lösungen zu identifizieren.[43]

Bei einer **Full Disclosure**[44] werden von IT-Sicherheitsforschern die betroffenen Entwicklungsunternehmen und die Öffentlichkeit über die entdeckte Lücke offen informiert, so dass auch Hacker die Lücke nutzen können bevor sie behoben ist, was als Nachteil zu verstehen ist. Dieses Vorgehen wird als unverantwortlich kritisiert.

Als verantwortungsvolle Enthüllung und heute **als Standard gilt deshalb** eine **Responsible Disclosure**, wonach die betroffenen Unternehmen zuerst informiert werden und ein Zeitfenster von üblicherweise 60 Tagen eingeräumt wird, um die Schwachstelle zu beheben. Erst dann macht der Sicherheitsforscher die Sicherheitslücke öffentlich, nachdem das betroffene System mit Lücke gesichert oder deaktiviert wurde.[45] Dann beginnt das Risiko, dass Hacker die veröffentlichte Schwachstelle ausnutzen. Sofort nach der Schwachstellen Information ist den Betreibern zu empfehlen, den Zeitvorsprung von 60 Tagen für Schutzmaßnahmen zu nutzen.

9.2 Exploits als systematischer Missbrauch von Schwachstellen durch Hacker

Mit Hilfe von Programmcodes[46] werden Sicherheitslücken und Fehlfunktionen von Programmen ausgenutzt, um sich Zugang zu

---

[42] Wikipedia zu Bug-Bounty-Programmen, mit weiteren Nachweisen zu unterschiedlichen Programmen, u.a. Microsoft, Online Services Bug Bounty Terms.

[43] Wikipedia mit Einzelnachweisen zur Literatur.

[44] Offenlegung oder Enthüllung.

[45] Biermann, Kai, Bug Bounty, Kopfgeldjagd im Internet, in Zeit online, 3.Sept. 2013.

[46] Als **Programmcode** werden die Anweisungen bezeichnet, die im Rahmen der Softwareentwicklung für ein bestimmtes Computerprogramm oder einen Teil davon entstehen und die dessen Funktionalität in einer bestimmten Programmiersprache beschreiben bzw. repräsentieren.

Ressourcen zu verschaffen und in Computersysteme einzudringen und sie zu beeinträchtigen. Ein Exploit ist selbst eine Entwicklung, die Sicherheitslücken anzeigt und dokumentiert, womit Softwarehersteller eine Schwachstelle schneller erkennen und beheben können.

Die Sicherheitslücken und Schwachstellen bei Software sind offenbar nur bei der Entwicklung zu vermeiden und vor dem Einsatz zu testen.

Exploits werden in verschiedene Arten eingeteilt. Bei **Lokalen Exploits** werden Sicherheitslücken in den Programmen ausgenutzt, mit denen die Datei eingelesen wird**.** Bei **Remote Exploits** werden über Angriffe aus dem Internet mit Hilfe manipulierter Datenpaketen auf Schwachstellen in der Netzwerksoftware Sicherheitslücken ausgespäht. **SQL-Injection-Exploits** stellen eine Gefahr dar, weil sie bei Webanwendungen eingesetzt werden, die eine SQL-Datenbank nutzen, und über das Internet sehr leicht zugänglich sind oder auch grundsätzlich für jede Anwendung gefährlich sind, die auf eine SQL-Datenbank zugreifen.[47]

Zero-Day-Exploits werden eingesetzt, bevor es einen Patch, eine Lösung zur Schwachstelle, gibt und dadurch Entwickler keine Zeit zur Nachbesserung haben, der Hacker sie nicht dem Entwickler meldet, sie geheim hält und als offene Schwachstelle für längere Zeit ausnutzt. Sie werden unter Hackern gehandelt oder gegen hohe Summen dem Hersteller angeboten.[48]

Als einzige Lösung erscheint das Vermeiden der Sicherheitslücken schon beim Entwickeln und beim Testen, was bei der Komplexität der Softwaresysteme als praktisch unmöglich gehalten werden muss, wenn schon der führende Softwarehersteller Microsoft durch Sicherheitslücken auffällig wird und seinen Generalschlüssel selbst vor Hackerangriffen nicht sichern kann. Die Hacker zeigen ihre Überlegenheit durch die erfolgreichen Angriffe und der Ausbeute. Die Schäden in Höhe von 206 Milliarden im Jahr 2023 durch Cyberattacken sind so hoch, dass die aktuelle gesetzgeberische Initiative zum BSIG und KRITIS-DachG dringend geboten erscheint. Auf jeden Fall ist der Cyber- und IT- Sicherheit eine höhere Priorität einzuräumen als bisher. Obwohl die Folgen der neuen Regelungen für Unternehmen erhebliche finanzielle und organisatorische erheblich sind, formiert sich kein Widerstand. Die Betroffenen können aufgrund der Bedrohungslage[49] darauf verweisen, dass zu Recht Priorität der Cybersicherheit einzuräumen ist, und alle Unternehmen gleich vom Mehraufwand und den Mehrkosten betroffen sind.

Der Bikom Präsident Wintergerst stellt detailliert die Risikolage und die ermittelte Einschätzung durch die Wirtschaft dar, wonach erstmals die Mehrheit der Unternehmen sich in ihrer Existenz bedroht fühlt, deutliche Zunahme von Cyberattacken und schließlich eine steigende Investitionsbereitschaft in die Cybersicherheit erwartet.

Die neue gesetzliche Regelung der Delegation der Organisationsverantwortung an die Geschäftsleiter erscheint deshalb als sinnvoller

[47] Heise Security, „Deutlicher Anstieg der SQL-Injection-Angriffe, und Giftspritze“ aus Wikipedia Fn. 5 und 6.

[48] Miller, Charles, The Legitimate Vulnerability Market: The Secret World of 0-day Exploit Sales; Patrick Beuth, Der perfekte iPhone-Hack kostet zwei Millionen Dollar.

[49] Wintergerst, Bitkom-Präsident, Wirtschaftsschutz 2023, mit detaillierter Darstellung der Risikolage auf Seiten 12,14,15.

und erster angemessener Schritt verbunden mit der Erwartung, dass die IT-Sicherheit höhere Beachtung durch erweiterte Budgets und verstärkte Unterstützung durch die Geschäftsleitung erfahren wird.[50] Die neue Organisationspflicht zur Cybersicherheit mit der gesetzlich geregelten persönlichen Haftung verspricht die ausreichende Motivation bei Geschäftsleitern zu bewirken.

Allerdings reicht die Delegation der Verantwortung nicht aus. Vielmehr ist das Entscheidungsverfahren zum Schwachstellenmanagement näher zu regeln.

9.3 Die SolarWinds cyberattack als Lehrbeispiel für kriminelle Exploits

Die neuen organisatorischen Anforderungen an Geschäftsleiter werden zum Erkennen und Abwehren von Cyberattacken am Beispiel des Angriffs auf das US-Unternehmen SolarWinds deutlich.[51] Hackerangriffe erkennen und davor zu schützen gehört noch nicht zum Allgemeinwissen von Geschäftsleitern. Expertenwissen wird notwendig, um die neue Organisationspflicht erfüllen zu können. Vor allem sind Lehren und Konsequenzen aus dem SolarWinds Fall für die zu organisierenden Schutzmaßnahmen zu ziehen, die von den neuerdings verantwortlichen Geschäftsleitern zu beachten sind.

Angegriffen wurde mit Solarwinds ein Anbieter einer Überwachungs- und Managementplattform für die gesamt IT-Infrastruktur eines Unternehmens mit weltweit 300 000 namhaften Großkunden und fast allen Fortune-500 Unternehmen, das auf Netzmanagement-Software spezialisiert ist und eine vermeintlich sichere Software vertreibt.

Angegriffen wurde Solarwinds unbemerkt schon 2019. Erst Ende 2020 wurden Cyberangriffe bei US Sicherheitsfirmen und Regierungsstellen auffällig. Deren Gemeinsamkeit war der Einsatz der Orionsoftware von SolarWinds, die sich als gemeinsame Quelle herausstellte. Die anonymen Hacker hatten unbemerkt einen Trojaner in die SolarWinds Software eingeschleust und auf deren Software-Kunden weiterverteilt. Über vier Monate blieb der Trojaner unauffällig. Das Besondere an dem Angriff war, dass die SolarWinds Software so manipuliert wurde, dass zehntausende Kunden von Solarwinds mit Sicherheitsverletzungen betroffen waren und erst bei den Anwendern der SolarWinds Software die Manipulationen bemerkt wurden. Gehackt wurde u.a. die US-Firma FireEye, die Software zum Testen der Sicherheit ihrer Kunden vertreibt und selbst wiederum Kunde von SolarWinds war. Auch das US- Handels- und Finanzministerium war betroffen. Durch den weltweit großen Kundenkreis von SolarWinds wurde die schädliche Wirkung des Angriffs auf eine einzige Software Quelle über die Lieferkette auf alle Kunden von SolarWind multipliziert. Vor allem SolarWinds Kunden, die selbst Software entwickeln und vertreiben, wurden als Multiplikatoren des Trojaners missbraucht. Dazu gehörten die namhaften Software Entwickler Microsoft, Nvidia, Belkin, Intel und Cisco.[52]

Die bis heute unbekannten Hacker waren in den Erstellungsprozess der SolarWinds Soft-

[50] Plogsties, NIS2 – und jetzt? iX 3/2024.

[51] Weidenhammer, in: All About Security, Angriff auf die Supply Chain-Solarwinds.

[52] Weidhammer, in: All About Security, Angriff auf die Supply Chain-SolarWinds.

ware eingedrungen und hatten manipulativ den Trojaner installiert, mit einer gültigen SolarWinds Signatur versehen, auf den Update-Server geschleust, von dort auf die Zielsysteme der SolarWinds Kunden ausgeliefert, von wo aus der Trojaner befehlen konnte, Daten auszulesen, das Netzwerk zu analysieren oder andere Schadcodes zu laden. Mit der Schadsoftware wurde der Erstellungsprozess manipuliert, Informationen über das zu infizierende Netzwerk zu sammeln, an den steuernden Server zu senden, und durch Downloads für Fernzugriffe Hintertüren einzubauen, um die Zugriffssicherungen zu umgehen. Angegriffen wurden ausgewählte Kunden von SolarWinds darunter Unternehmen wie Microsoft, US-Behörden und deutsche Ministerien und 16 Bundesbehörden, das Bundeskriminalamt, und der zentrale IT-Dienstleister des Bundes, ITZ Bund. Viren-Dropper[53] wurden bei ausgewählten Kunden eingeschleust, um die Reichweite der Hacker zu erweitern.

Mit der Schadsoftware wurde bei Microsoft Teile des Quellcodes eingesehen, bei Azure der Code für Sicherheits- und Identitätsfunktionen, außerdem Sourcecode-Repositories[54]. Kopien der Microsoft Codes waren möglich, um Schwachstellen auszuspähen. Erbeutet wurden bei der Sicherheitsfirma FireEye Instrumente, mit denen die Sicherheit ihrer Kunden getestet werden. Deren Konzept besteht nämlich darin, die Angriffs-Tools von kriminellen Hackern zu imitieren. Dadurch vermehrten die Hacker ihre Werkzeuge, um selbst anzugreifen, vor allem auch die gehackten Sicherheitsfirmen mit den eigenen Programmen.

Über die Hacker ist nichts bekannt. Sie werden in Russland vermutet.

9.4 Konsequenzen aus der SolarWinds cyberattack

Der Fall zeigt überdeutlich die Anfälligkeit der Software Branche. Wenn selbst Firmen wie Microsoft ihre Quellcodes vor dem Auslesen und Sicherheitsfirmen ihre Testinstrumente nicht vor dem Kopieren schützen können, wenn SolarWinds mit weltweit 300 000 Unternehmen ihre Netzwerke vor Manipulationen und vor dem Einschleusen von Trojanern nicht schützen können und schließlich die gesamte Lieferkette einer großen Softwarefirma mit Schadsoftware infiziert werden kann, wird die Sicherheit der IT Branche zum Organisationsproblem. Es wurde von den Gesetzgebern von Bund und EU erkannt und an die Geschäftsleiter als Organisationspflicht delegiert. Die folgenden Hinweise zu den Konsequenzen sind nicht abschließend und mit fortlaufenden Erfahrungen zu ergänzen.

9.4.1 Informationsbeschaffung durch Geschäftsleiter über alle eingesetzten Softwareprogramme im Unternehmen

Erstens sollten die neu nach § 30 Abs.2 Nr.5 i.V.m. § 38 Abs.1 BSIG verantwortlichen Cybervorstände und Geschäftsleiter für jede im Unternehmen eingesetzte Software systematisch erfragen, welche Informationen über die im Unternehmen verwendete Software vorlie-

[53] Ein Viren-Dropper ist ein eigenständig ausführbares Computerprogramm, das zur Freisetzung eines Computervirus dient. Dropper werden meist für eine Erstinfektion verwendet, da sich der virale Code anschließend automatisiert weiterverbreiten kann.

[54] Ein Repository ist ein verwaltetes Verzeichnis zur Speicherung und Beschreibung digitaler Objekte für ein digitales Archiv.

gen, wozu **die Bug-Bounty-Programme und eventuelle bekannt gewordene Exploits** gehören. Im Rahmen des Compliance-Management-Systems lassen sich Meldesysteme organisieren, die systematisch alle Angestellten dazu verpflichten, IT Informationen zu melden, die die IT Sicherheit betreffen. Vor allem auch alle Hinweise Dritter außerhalb des Unternehmens sollten nicht ignoriert, sondern aufgegriffen und zum Schutz des Unternehmens geprüft werden.

Im SolarWind Fall lagen Informationen des Sicherheitsforschers Vinoth Kumar vor, dass ein Datenleck besteht und unter Verwendung eines Passworts eine Datei auf den Server des Unternehmens geladen werden kann und als Beweis für die Anfälligkeit von SolarWind Software gelten muss. Diese warnenden Hinweise auf ein öffentliches GitHub, einen Onlinedienst für Softwareentwickler, per E-Mail an SolarWind wurde nachweislich ignoriert.[55]

Diese Pflicht der Geschäftsleiter ergibt sich § 30 Abs.2 Nr. 5 i.V.m. § 38 Abs.1 BSIG. Danach sind Sicherheitsmaßnahmen beim Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen einschließlich Management und Offenlegung von Schwachstellen umzusetzen.

9.4.2 Die technische und rechtliche Prüfung von Software auf Sicherheitslücken

Zweitens ist jedem Geschäftsleiter im Hinblick auf seine neue zu beachtende Verantwortung für die Cybersicherheit zu empfehlen, die von seinem Unternehmen eingesetzte Software EDV-technisch auf Mängel und auf Sicherheitslücken und auf eventuelle zivilrechtliche Mängelansprüche nach den neuen Regelungen gemäß § 327 BGB ff. prüfen zu lassen. Seit Januar 2022 gelten neue zivilrechtliche Regelungen für Verträge über digitale Inhalte und Dienstleistungen. Sie gelten für Vertragsgegenstände mit digitalen Elementen. Bei Software ist von einem sehr weitgehenden Mangelbegriff auszugehen, was aus der Komplexität der Software folgt.[56] Eine Software ist auch dann mangelhaft, wenn sie vermeidbare Sicherheitslücken enthält, die einen Angriff durch Viren, Trojaner oder andere Schadsoftware ermöglichen.[57]

Es gilt das „**Gesetz zur Umsetzung der Richtlinien über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen**". Mit § 327 BGB wird eine neue Vertragsart eingeführt, zu Verträgen mit Verbrauchern über die Bereitstellung digitaler Inhalte oder digitaler Dienstleistungen durch den Unternehmer gegen Zahlung eines Entgelts. Die neuen §§ 327 bis 327 u BGB enthalten Regelungen zu Mängelgewährleistungen, Aktualisierungspflichten, Änderungsverboten, Informationspflichten und Haftungsausschlüssen jeweils für digitale Produkte.[58] Produktmängel sind in § 327 e BGB geregelt. Die gesetzlichen Neuregelungen über digitale Produkte gelten auch für Verträge zwi-

[55] Weidhammer, in All About Security, unter: Leichtes Spiel für Angreifer.

[56] Redeker, IT-Recht, Rn.349.

[57] Redeker, IT-Recht, Rn.343; Schimmer DuD 2006,616; Paulus/Tegge DuD 2006,623; Klett/Gehrmann.

[58] Haar, iX 2/2022, Neues Vertragsrecht zu digitalen Produkten, Zum Schutze der Kunden, Seite 99.

schen den Unternehmen, allerdings nach § 327t BGB nur „ergänzend“. Kaufleute können untereinander von den Regelungen abweichen. Im Rahmen der Grenzen der AGB-Kontrolle kann dann auch eine vom BGB abweichende Vertragsgestaltung durch allgemeine Geschäftsbedingungen vereinbart werden. Ohne diese abweichenden Geschäftsbedingungen gelten die §§ 327 ff. vollumgänglich auch im Geschäftsverkehr.[59] Geschäftsleiter sind zur Prüfung verpflichtet, ob die eingesetzte Software mängelfrei ist. Nach der aktuellen Fassung der Produkthaftungsrichtlinie der EU im Entwurf gilt nach Art.4 Software als Produkt und nach Art.6 Abs.1 f Prod-HaftRL-E gilt die Software als fehlerhaft, wenn die Sicherheitsanforderungen einschließlich der sicherheitsrelevanten Cybersicherheitsanforderungen nicht berücksichtigt sind.[60] Der Richtlinien Entwurf ist noch nicht umgesetzt.

10. Die Cloud als Risiko und Schwachstelle

Software Anwendungen, die direkt aus dem Internet erreichbar sind, werden häufig Ziele von Angriffen, die aus den Logs erkennbar sind. Eine Logdatei enthält das automatisch geführte Protokoll aller Aktionen von Prozessen auf einem Computersystem. Auf Logs sind alle angewiesen, die eine Software Anwendung betreiben. Das Log muss die nötigen Informationen enthalten, wenn man herausfinden will, welche Browserversionen einen bestimmten Fehler verursachten.[61] Browser dienen als Computerprogramme der Darstellung von Webseiten oder allgemein von Dokumenten und Daten. Das Log mit seiner Funktion als Protokoll muss die Informationen enthalten, die Hinweise geben, welche Browser einen bestimmten Fehler verursacht haben. Auf dem Log muss unter anderem der Benutzername protokolliert sein, bei denen die Log-in-Versuche erfasst wurden, die fehlgeschlagen sind und auf einen Fehler in einer Browserversion schließen lassen.

Bei der Cloud-Nutzung spielen Sicherheitsanforderungen eine besonders große Rolle, um den Schutz von Daten, Anwendungen und Infrastrukturen zu gewährleisten und potenzielle Sicherheitsrisiken zu minimieren. Während die klassischen und meist in sich geschlossenen IT-Infrastrukturen in der Regel gut geschützt sind, ergeben sich mit der Nutzung von IT-Leistungen aus der Cloud neue Angriffsvektoren und damit ein hohes Risiko der Kompromittierung der IT-Systeme.[62]

Das BSI stellt zum Angriffsrisiko fest: „Nicht jede Schwachstelle ist für Angreifer einfach ausnutzbar. Eine Schwachstelle in einer lokalen Anwendung ohne Verbindung zum Internet kann beispielsweise nur durch einen lokalen Angreifer ausgenutzt werden. Sind dagegen Schwachstellen in Softwareprodukten direkt

[59] Haar, iX 2/2022, Neues Vertragsrecht zu digitalen Produkten, Zum Schutze der Kunden, Seite 107

[60] Adelberg, Perspektiven der Haftung für Fehler von Software und softwaregestützten Produkten nach dem Änderungsentwurf zur EU-Produkthaftungsrichtlinie, ZfPC 2023,59.

[61] Frank und Casper, iX 12/2023, Schwachstellenmanagement: mehr als Scannen und Finden, S.51

[62] KPMG Lünendonk-Studie 2023, Von Cyber Security zu Cyber Resilience, Wie Unternehmen auf die steigende Bedrohungslage reagieren, S.21.

aus dem Internet erreichbar, können sie von einer höheren Anzahl von Cyberkriminellen für Angriffe missbraucht werden.“[63]

11. Log4Shell als Anlass für das Schwachstellen-Management

Im Dezember 2021 wurde die Schwachstelle in Log4j entdeckt und als Log4Shell benannt. Bei Log4j handelt es sich um eine Programmbibliothek, die in Java-Anwendungen eingesetzt wird, um Logs zu erzeugen. Die Programmbibliothek enthält auch eine Funktion, um Logzeilen aufzulösen und zu interpretieren. Diese Lookups können von Hackern missbraucht werden, ohne dass sie als Logeinträge erkannt werden, die von Angreifern eingetragen wurden. Die Programmbibliothek erwies sich als einfach und leicht von Angreifern auszunutzen und zu missbrauchen. Angreifer konnten die Kontrolle über das System erlangen und sensible Daten ausschleusen, eigene Java-Codes an das Opfersystem schicken, ausführen lassen, um im Ergebnis das angegriffene System zu kontrollieren.

Danach hat sich das Schwachstellen Managment grundlegend verändert.

Erstens erwies sich die Schwachstelle Log4Shell als durch Hacker leicht ausnutzbar. Angreifer kamen leicht an Informationen, die sie in ein Eingabefeld auf einer Webseite einfügten, um das System hinter der Webseite kontrollieren zu können. Angreifer konnten sich frei bedienen, weil Informationen unverschlüsselt in Logdateien geschrieben wurden. [64]

Zweitens war die Schwachstelle sehr verbreitet, weil Java eine der verbreitetsten Programmiersprachen ist und Log4Shell auch eine der verbreitetsten Logging- Bibliotheken ist, schätzten Analysten 34.000 betroffene Projekte.

Drittens war sie schließlich nur schwer erkennbar. Log4j ist eine Bibliothek, die immer nur als versteckte Komponente in einer anderen Software vorkommt. Sie war Teil einer Software Lieferkette. Bis heute wächst die Zahl der betroffenen Anwendungen wegen erstens der leichten Ausnutzbarkeit, zweitens der hohen Verbreitung und drittens wegen ihrer schweren Erkennbarkeit.

Der Fall Log4Shell zeigt, dass die Verantwortlichen Schwachstellen nur sehr schwer zu erkennen und zu beheben können. Ein systematisches Vorgehen war deshalb zu fordern, nämlich ein Schwachstellen Management.[65] Dies gilt umso mehr, als der Gesetzgeber die Verantwortung zur Cybersicherheit ausdrücklich den Geschäftsleitern übertragen hat. Wenn Geschäftsleiter diese neue Organisationspflicht erfüllen sollen, muss ein allgemein geltendes Schwachstellen Management konzipiert werden, was als Maßstab und Handlungsempfehlung für Geschäftsleiter tauglich ist.

[63] BSI, Die Lage der IT- Sicherheit in Deutschland 2023, S. 34.

[64] Frank und Casper, Im Detail beschrieben sind die Einzelheiten des Angriffs in iX 12/2023 S.51, Schwachstellenmanagement: mehr als Scannen und Finden, S. 51 – 53.

[65] Haar, iX 2/2022, Neues Vertragsrecht zu digitalen Produkten, Zum Schutze der Kunden, S.54.

Schwachstellen sind systematisch erstens zu identifizieren, mit dem Ziel, sie zweitens wegen der hohen Zahl zu priorisieren, drittens zu behandeln und viertens präventiv zu vermeiden. Die Pflicht zum Schwachstellenmanagement ergibt sich aus § 30 Abs.2 Nr. 6 BSIG.

12. Schwachstellen identifizieren

Identifizieren lassen sich Schwachstellen **durch authentifizierte Scans**, bei denen authentifizierte Benutzer mit legitimen Anmeldedaten nach Schwachstellen suchen und eine Innensicht des Systems nutzen, mehr Schwachstellen erkennen und sich einen vollständigen Eindruck verschaffen können. Bug-Bounty Programme für Entwickler und Sicherheitsexperten sind authentifizierte Scans. Zu unterscheiden sind Scans, bei denen Agenten auf den Systemen installiert werden oder bei denen von einem zentralen netzwerkbasierten Scanner das zu prüfende Zielsystem angesteuert wird, um Schwachstellen zu suchen.

Nicht authentifizierte Scans verwenden keine Anmeldedaten. Es handelt sich um Oberflächen-Scans, mit denen Hintertüren, nicht gepatchte Software und sonstige Sicherheitslücken gesucht werden können. Schwachstellen, die bei nicht authentifizierten Scans gefunden werden, sollten vorrangig behandelt werden, weil sie von Hackern ohne Anmeldedaten leicht gefunden und missbraucht werden können.[66]

Eine Sicherheitslücke oder eine Schwachstelle ist auf dem Gebiet der **Informationssicherheit** ein Fehler in einer Software oder einer Hardware, durch den ein Programm mit Schadwirkung (Exploit) oder ein Angreifer in ein Computersystem eindringen kann.

Schwachstellen in IT-Systemen ermöglichen das Eindringen von Hackern zur Erpressung, Datenklau, Sabotage, Werkspionage, Abschöpfen von Geschäftsgeheimnissen, Störung der Produktionsabläufe und zum Ausfall von Informationssystemen.

Die wichtigste Quelle für Schwachstelleninformationen ist die National Vulnerability Database (NVD), die vom US National Institute of Standards an Technology (NIST) betrieben wird. Sie veröffentlicht fortlaufend neue Schwachstellen. Bis 2016 wurden jeden Monat etwa 10 Jahre lang etwa 500 neue Schwachstellen in Softwareprodukten gefunden. Ab 2017 wurden dreimal mehr Schwachstellen gefunden, in den drei Quartalen 2023 waren es mehr neue als in 2014 bis 2016 zusammen. Aktuell liegt die Anzahl neuer Schwachstellen im Durchschnitt beim Fünffachen von 2016 also bei 2.500 im Monat.[67] Der Anspruch, sie alle zu beheben, gilt als unrealistisch. Schwachstellen müssen deshalb priorisiert werden.

13. Schwachstellen Priorisieren

13.1 Die Anwendung des Verhältnismäßigkeitsprinzips

Rechtlich zu erwägen wäre bei der hohen Zahl der monatlich identifizierten Schwachstellen

[66] Frank und Casper, iX 12/2023 S.51, Schwachstellenmanagement: mehr als Scannen und Finden, S. 54.

[67] Frank und Casper, iX 12/2023, Schwachstellenmanagement: mehr als Scannen und Finden, Seite 50 mit aufschlussreicher Abbildung 2 zum Stand von 19.10.2023.

die rechtliche Unmöglichkeit der Pflicht des Geschäftsleiters zur Behebung der Schwachstellen nach § 275 BGB.

Der Gesetzgeber hat jedoch in Kenntnis der kaum zu bewältigenden Aufgabe die Pflichten der Geschäftsleiter im Gesetz vorsorglich unter den Vorbehalt der Verhältnismäßigkeit gestellt. Die Behandlung der Schwachstellen ist deshalb zu priorisieren. Mit den begrenzten Ressourcen sind die größten Sicherheitsgewinne anzustreben.[68]

Das Gesetz verlangt deshalb in § 30 Abs.1 BSIG v**erhältnismäßige** technische und organisatorische Maßnahmen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. In § 10 KRITIS-DachG werden die Betreiber kritischer Anlagen verpflichtet, geeignete **und verhältnismäßige**, technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz zu ergreifen.

Nach § 31 Abs.2 BSIG soll der erforderliche Aufwand zum Identifizieren von Bedrohungen den geeigneten Beseitigungsmaßnahmen nicht außer Verhältnis zu den Folgen des Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen. Der Umgang mit Schwachstellen besteht darin, Schwachstellen regelmäßig und kontinuierlich zu identifizieren, sie für die Umgebung im Unternehmen zu bewerten, um sie zu priorisieren, d.h. zu entscheiden, was zuerst und vorrangig zu veranlassen ist, mit angemessenen Maßnahmen zu behandeln und um schließlich damit Schäden zu verhindern oder zu verringern.

13.2 Die Bewertung von Schwachstellen zur Rangfolgenbildung und als Entscheidungshilfen für Geschäftsleiter

13.2.1 Der Base Score

Die technischen Aspekte einer Schwachstelle werden mit dem Base Score[69] bewertet.

Zur Bewertung von Schwachstellen wird auf den offenen Standard verwiesen, den Common Vulnerability Scoring System (CVSS)[70], der von der US National Infrastructure Advisory Council (NIAC) erstellt und veröffentlicht wird. Aktuell betrieben wird dieser Standard von dem Forum of Incident Response und Security Teams (FIRST). Der CVSS-Score repräsentiert die Relevanz von Schwachstellen und setzt sich aus verschiedenen Eigenschaften der Schwachstelle, aus den Metriken, zu-

[68] Frank und Casper, iX 12/2023, Schwachstellenmanagement: mehr als Scannen und Finden, S. 56

[69] **Score** in Bezug auf Schwachstellen ist eine Bewertung oder ein Punktwert, der die Schwere oder das Risiko einer Sicherheitslücke quantifiziert. Es gibt verschiedene Score-Systeme, die von Sicherheitsexperten verwendet werden, um die Bedrohlichkeit von Schwachstellen zu bewerten.

[70] **CVSS (Common Vulnerability Scoring System)**: Dieses System bewertet Schwachstellen auf einer Skala von 0 bis 10. Ein höherer CVSS-Score bedeutet eine größere Bedrohung.Die Bewertung basiert auf Faktoren wie Ausnutzbarkeit, Auswirkungen und Komplexität.

sammen. Er berechnet sich aus komplexen Formeln und gibt einen Maßstab darüber ab, wie die Schutzziele der Vertraulichkeit, der Integrität und der Verfügbarkeit betroffen sind. Vor allem kann er den verantwortlichen Geschäftsleitern eine erste Hilfe für die Entscheidung darüber bieten, welche der vielen Schwachstellen vorrangig zu behandeln sind.[71] Wenn die Zahl der Schwachstellen nach der Bewertung mit dem Base Score zu hoch wird, sind weitere andere Bewertungsmaßstäbe anzulegen.

13.2.2 Der Temporal Score

Der Temporal Score bezieht eine aktuelle Momentaufnahme der verfügbaren Exploits und der Schutzmaßnahmen, der Patchs sowie der Zuverlässigkeit der Berichte zu der Schwachstelle mit ein. Der Temporal Score ist ständig zu aktualisieren. Die Wahrscheinlichkeit der Ausnutzung der Schwachstelle bietet das Exploit Prediction Scoring System (EPSS) von FIRST, das für alle veröffentlichten Schwachstellen tagesaktuell und kostenfrei zur Verfügung gestellt wird.[72] Insgesamt flossen 1164 Verschiedene Variablen in das mathematische Modell ein, um eine bessere Priorisierung zu ermöglichen.[73]

13.2.3 Der Environmental Score

Der Environmental Score berücksichtigt den jeweiligen Schutzbedarf der betroffenen Systeme. Die Schutzbedürftigkeit und damit die Entscheidung über den Vorrang einer Schutzmaßnahme kann vom jeweiligen Unternehmen abhängen. Forschungsergebnisse, Medizindaten oder Produktionsdaten können unterschiedlich je nach Unternehmen bewertet werden. Der Unternehmenskontext ist miteinzubeziehen. Die Frage, welchen Schaden in einem Unternehmen eine Schwachstelle verursachen kann, lässt sich nur und erst beantworten, wenn die Bedeutung des Systems für das Unternehmen berücksichtigt wird. Ob eine Schwachstelle kritisch ist, muss für jedes Unternehmen individuell beantwortet werden. Die bessere Priorisierung hängt vom Unternehmenszweck ab, der unterschiedliche Prioritäten verfolgen kann.

14. Die Behandlung identifizierter und priorisierter Schwachstellen

Nachdem in § 38 BSIG die Geschäftsleiter von Unternehmen die Verantwortung für die Cybersicherheit tragen, stellt sich für sie die Frage, wie die priorisierten Schwachstellen zu behandeln sind. Sie zu kennen und zu priorisieren, wendet noch nicht das Risiko aus der Schwachstelle für die Cybersicherheit ab. Die Schwachstelle kann durch das Einspielen eines Patchs behoben werden. Steht noch kein Patch als Lösung zur Verfügung und kann die Schwachstelle nicht behoben werden, kann man versuchen, um das Risiko der Ausnutzung zu senken, etwa durch die Einrichtung von Fire Wall Regeln zur Verhinderung des Zugriffs auf eine verwundbare Schnittstelle. Eine Möglichkeit wäre auch, die angreifbare

[71] Frank und Casper, iX, 12/2923, Schwachstellenmanagement: mehr als Scannen und Finden, S. 59 f. Abbildung 4.

[72] Frank und Casper, iX, 12/2023 Schwachstellenmanagement: mehr als Scannen und Finden, S. 50 f. Abbildung4.

[73] Frank und Casper, iX, 12/2023 Schwachstellenmanagement: mehr als Scannen und Finden, S. 60.

Funktion auszutauschen. Schlimmstenfalls müsste sogar ein Risiko getragen werden. Das Inkaufnehmen des Risikos müsste als einzige Alternative beschrieben und vor allem auch so dokumentiert werden. [74]

Eine Marktübersicht zu Anbietern von Werkzeugen für die Behandlung von Schwachstellen mit weiteren Details bietet der zitierte Aufsatz.[75]

15. Die Dokumentation des Schwachstellen Managements zur Beweissicherung

Dringend zu empfehlen ist die Dokumentation des Schwachstellenmanagements bei Vorgang der Priorisierung, um die Beweise für die Entlastung des Geschäftsleiters zu sichern, da dieser die Beweislast für die Erfüllung seiner Pflichten nach § 38 i.V.m.§ 30 BSIG trägt. Nach § 93 Abs. 2 S. 2 AktG gilt der Grundsatz der Beweislastumkehr, wonach die Geschäftsleiter die Beweislast trifft, wenn streitig ist, ob sie die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters angewandt haben. Weil vorher nicht klar ist, wann der Schaden eintreten wird, gilt die Dokumentationspflicht als Dauerpflicht.

16. Die Softwarelieferkette (SBOM) als Schwachstelle

Nach § 30 Abs.2 Nr.4 BSIG sind Geschäftsleiter zur Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehung zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstanbietern.

Software besteht aus einer Vielzahl von Einzelkomponenten, die eine Lieferkette bilden und jede für sich eine Schwachstelle sein kann[76]. Als Paradebeispiel für die Verwundbarkeit der Softwarelieferkette gilt die unscheinbare Java Bibliothek Log4Shell, von der viele Anwender nicht wussten, dass sie zu den einzelnen Komponenten ihrer verwendeten Software gehörten. Mit ihr konnten interne Daten erspäht und gestohlen, Hintertüren verbreitet, Code-Ausführungen ferngesteuert, Schadprogramme und unerwünschte Befehle ausgeführt werden. Drei Tage nach der Veröffentlichung der Lücke wurden schon 830.000 Angriffe gezählt. Die leichte Missbrauchsmöglichkeit, die hohe Verbreitung, die schädliche Wirkung und vor allem die Unkenntnis der Wirkung und die fehlende Transparenz machten das Risiko von Log4Shell aus.[77]

Abgewendet werden soll dieses Risiko auf Grund der Unkenntnis über die Komponenten in der Softwarelieferkette mit der SBOM-Richtlinie des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Eine SBOM (Software Bill of Materials) ist eine Stückliste, die alle Einzelbestandteile einer Softwarelösung enthält. Die SBOM Richtlinie ist eine Empfehlung des BSI, wie diese Stückliste für Software konkret aussehen soll. Die SBOM

[74] Frank und Casper, iX, 12/2023 Schwachstellenmanagement: mehr als Scannen und Finden, S. 63.

[75] Frank und Casper, iX, 12/2023, Werkzeuge für das Schwachstellenmanagement, S. 58 f.

[76] Schneider, Udo, iX10/2022. SOFTWARE BILLS OF MATERIALS, SBOMs – Stücklisten für Software S. 55.

[77] Schneider, Udo, iX10/2022. SOFTWARE BILLS OF MATERIALS, SBOMs – Stücklisten für Software S. 55.

soll einen Überblick über alle Einzelkomponenten den Anwendern bieten, um von Attacken oder Sicherheitsproblemen betroffene Softwarekomponenten schnell identifizieren und abwehren zu können. Sichern soll die SBOM den betroffenen Softwareanwendern eine schnelle Reaktionsfähigkeit, die Sicherheit ihrer IT, die Kontrolle über geschäftskritische Anwendungen, die Wiederherstellung der Arbeitsfähigkeit und die Resilienz.

Die EU will mit dem Cyber Resilience Act (CRA) zur Abwendung des Softwarelieferkettenrisikos die Hersteller von Software zur Einhaltung gemeinsamer Sicherheitsstandards verpflichten. Die SBOM Richtlinie des BSI soll auf diese Pflichten vorbereiten. Die SBOM ist ständig zu aktualisieren, weil Software weiterentwickelt und damit auch die Risiken und Abwehrinstrumente sich weiterentwickeln. Das manuelle Erstellen von SBOMs ist aufwändig. Angestrebt wird deshalb das automatisiert und standardisierte Erstellen.[78]

Zur Abbildung von SBOMs haben sich zwei Standards entwickelt.

Erstens lassen sich SBOMs im Format Software Package Data Exchange (**SPDX**) erstellen, das ursprünglich für mehr Transparenz bei der Verwendung von Open-Source-Lizenzen und bei der Abhängigkeiten von Software entwickelt wurde. Es ist seit 2021 als ISO Standard (ISO/IEC 5962:20213) spezifiziert.

Zweitens lassen sich SBOMs im Format **CycloneDX** vom OWASP (Open Web Application Security Project) erstellen, was explicit zur Abbildung von SBOMs entwickelt wurde. Beide Formate umfassen u.a. die exakte Bezeichnung der Software, die Abhängigkeit zu anderer Software, Bibliotheken oder Dienste, Dateibezeichnungen, Lizenzen, Anmerkungen. An den SBOM können vor allem die wechselseitigen Abhängigkeiten abgelesen und in Baumstrukturen graphisch dargestellt werden. Nicht nur die IT Sicherheit wird durch die SBOMs angestrebt.

Auch die Abhängigkeit von Lizenzen kann ebenfalls aus der SBOM ermittelt werden. Nachverfolgen lässt sich auch, welchen Lizenzen die Software unterliegt. In Audits oder durch illoyale und ehemalige Mitarbeiter können Lizenzverletzungen bekannt werden. Die Abhängigkeit von Lizenzen und von technischen Änderungen sind regelmäßig zu aktualisieren.[79]

17. Die neue Pflicht zu Standards bei der automatischen Erstellung und Pflege von SBOMs

Die Information in SBOMs lassen sich automatisch während des Entwicklungsverfahren erstellen. Die wechselseitigen Abhängigkeiten der Einzelkomponenten einer Software sind im Entwicklungsverfahren sichtbar und können in Protokollen erfasst werden. **Eine Pflicht zur Vorlage von SBOMs durch den jeweiligen Zulieferer besteht noch nicht.** In den USA gilt allerdings schon seit 12.5.2021 eine „Executive Order on Improving the Nation´s Cybersecurity“ (RO 140281), mit der die Mitteilung von Informationen über Schwachstellen entlang der Software Lieferkette von staatlichen

[78] Plogsties, iX 3/2024, Was die SBOM für die Cloud bedeutet, S. 78 mit Hinweis auf iX. de/z39u.

[79] Schneider, Udo, iX10/2022. SOFTWARE BILLS OF MATERIALS S. 61, 62.

Käufern gefordert wird. Erfasst sind technische und organisatorische Standards zur Softwarelieferkettensicherheit von der NIST[80] in der NIST SP 800-161 unter dem Titel **„Cybersecurity Supply Chain Risk Management Practices for System and Organisations“.** Das NIST Cybersecurity Framework (NIST CSF) besteht aus Standards, Richtlinien und Best Practices zur Verbesserung des Managements von Cybersicherheitsrisiken.

Das BSI wirbt ebenfalls für transparentes und effizientes Schwachstellen- und Patchmanagement auf Basis von Software Bills of Materials.

Festzuhalten bleibt, dass die Erstellung von SBOMs eine wichtige Aufgabe darstellt, um die Softwarelieferkette gegen Angriffe zu sichern. Sie war bisher keine Pflicht sondern eine Empfehlung, um die Cybersicherheit zu fördern.

Durch § 30 Abs.1 und Abs. 2 Nr. 4 BSIG zählt die Sicherheit der Softwarelieferkette zu den Pflichten der besonders wichtigen oder wichtigen Einrichtungen, deren Geschäftsleiter neu nach § 38 Abs. 1 BSIG verpflichtet sind, die zu ergreifenden Risikomaßnahmen nach § 30 BSIG zu billigen und ihre Umsetzung zu überwachen. Durch §§ 30, 38 BSIG wird der Stand der Technik nunmehr zur Pflicht, sobald das Gesetzgebungsverfahren abgeschlossen wird.

18. Die Identifizierung von einzelnen Komponenten aus der SBOM

Mit den zwei beschriebenen Standards für SBOMs **– SPDX und CycloneDX** – soll sichergestellt sein, dass jeder Empfänger einer SBOM diese auch lesen, auswerten und weiterverarbeiten kann. Dazu wiederum ist es erforderlich, die einzelnen Komponenten der SBOM zu identifizieren, was in der Praxis nicht immer der Fall ist.[81] Die Standards SPDX und CycloneDX standardisieren nur das Schema der SBOM, nicht aber die Identifikation der Einzelkomponenten. Sie können Schwachstellen enthalten, was das Beispiel Log4Shell gezeigt hat. Sie können auch von einzelnen Lizenzen abhängen und müssen auch deshalb identifiziert werden können, ohne mit anderen Komponenten verwechselt zu werden. Die verwendeten Standards sind nicht bindend und erschweren die Vergleichbarkeit von SBOMs.[82]

19. Standardisierte Sicherheitsinformation für IT-Produkte

Vom amerikanischen Nist[83] wurde die Common Platform Enumeration (CPE) als Teil des Security Content Automation Protocol (SCAP) erstellt. Sie wurde besonders zur Identifikation von schon installierten IT- Produkten entworfen. Mit ihr können Administratoren eine Datenbank mit allen IT-Einrichtungen eines Un-

[80] NIST ist das National Institute of Standards and Technology, eine nichtregulatorische Behörde, die Innovationen durch Förderung der Wissenschaft von Standards und Technologie fördert.

[81] Braun Gunnar, Wie viel Standard steckt in SBOMs, in iX 9/2023 Seite 107.

[82] Braun Gunnar, Wie viel Standard steckt in SBOMs, in iX 9/2023 Seite 108.

[83] Wie Fn. 58.

ternehmens erstellen und verwalten. Bei SCAB handelt es sich um eine Sammlung von Beschreibungen zur Vereinheitlichung und Erleichterung von Sicherheitsinformationen für IT- Produkte. Außerdem gibt es noch als Teil von SCAP die Common Vulnerability Enumeration (CVE) und das Common Vulnerability Scoring System (CVSS). Alle Spezifikationen zusammen genommen bilden die National Vulnrability Database (NVD).[84]

Mit diesen Datenbanken können mit Hilfe der vereinheitlichten CPE Bezeichnungen nach jeweils neu veröffentlichte Schwachstellen die Betroffenheit von Software im Unternehmen geprüft werden. Die CPE enthält aktuell 1,1 Millionen Einträge. Die Einträge enthalten die Version von CPE, den Typ des Produkts, Betriebssysteme und Hardware.[85]

Neben der Schwachstellenermittlung sind Softwarekomponenten auch nach rechtlichen Merkmalen zu identifizieren, wie dem Urheber und Lizenzberechtigten. Darüber geben Software Identification Tags[86] (SWID-Tags) in formalisierter Form Auskunft. SWID-Tags sind seit 2007 als ISO/IEC 19770-2 standardisiert werden aber nur selten außer von Microsoft verwendet.[87]

Ein weiteres Format zur Standardisierung von Sicherheitsinformationen ist PURL oder auch Package URL, dessen Ziel es ist, Namenskonventionen zu vereinheitlichen. Softwarekomponenten werden bei PURL von den Autoren selbst mit Namen und Version verantwortlich bezeichnet, wodurch die Bezeichnungen präziser sind als bei einer Bezeichnung durch eine zentrale Stelle wie die CPE. Dieselbe Softwarekomponente kann auch aus unterschiedlichen Bezugsquellen stammen, was zu unterschiedlichen Lizenzen führen kann. PURL gilt inzwischen als der meist genutzte Komponentenbezeichner. [88]

20. Schwachstellendatenbanken

Wer neue Schwachstellen in den Komponenten suchen muss, die in den SBOMs, den Softwarelieferketten angeben sind, kann in Schwachstellendatenbanken, SBOM Vulnerability Databases recherchieren. Format und Einträge sind nicht einheitlich.

Erstens wird die National Vulnerability Database (NVD) genannt, die CVE – Einträge speichert, von der NIST-Behörde zentral verwaltet wird und als Standardquelle gilt.

Zweitens wird die Open Source Vulnerability Database (OSV) genannt, die von Google gestützt wird und Open Source Software anzeigt, enthält GitHub Security Advisories (GHSA), die von jedem Besitzer eines GitHub Repositorys erstellt werden kann, ohne einen formalen Genehmigungsprozess wie bei der NVD und ohne Validierung auskommt.

---

[84] Braun Gunnar, Wie viel Standard steckt in SBOMs, in iX 9/2023 Seite 109.

[84] Braun Gunnar, Wie viel Standard steckt in SBOMs, in iX 9/2023 Seite 109.

[85] Braun Gunnar, Wie viel Standard steckt in SBOMs, in iX 9/2023 Seite 109.

[86] Tag (Etikett, Mal, [Ab-]Zeichen, Auszeichner, Anhänger oder Schildchen) ist eine Auszeichnung eines Datenbestandes mit zusätzlichen Informationen.

[87] Braun Gunnar, Wie viel Standard steckt in SBOMs, in iX 9/2023 Seite 110 mit Beispielen.

[88] Braun Gunnar, Wie viel Standard steckt in SBOMs, in iX 9/2023 Seite 111-112 mit Vergleichsbeispielen für die Log4shell Komponente.

Drittens betreiben die Toolhersteller eine Datenbank, die durch eigene Teams neue Schwachstellen untersuchen und auch neu entdecken und ihren Kunden zur Verfügung stellen. Diese Informationen gelten als qualitativ besser und liefern genauere Details zu betroffenen Versionen.[89]

Zum Schwachstellenmanagement gehört die ständige Beobachtung der Komponenten einer Software, weil aus Erfahrung ständig neue Schwachstellen gefunden werden, zuletzt 2.500 pro Monat mit steigender Tendenz. Dadurch ändert sich die Sicherheit einer Software, obwohl die Software selbst gleich bleibt. Software verrottet (Software Rot) mit jeder neu gefundenen Schwachstelle. Deshalb müssen Schwachstellendatenbank ständig abgefragt werden.

Hinzu kommt ein weiterer Grund für die ständige Beobachtung. Von der Verwendung einer Komponente hängt es ab, ob eine Software von einer Komponentenschwachstelle betroffen wird.

Erst aus der Verwendung der Komponente ergibt sich das Risiko einer Schwachstelle. Die Softwarehersteller sollen deshalb die Schwachstellen in Verbindung mit dem Produkt dokumentieren und weitergeben. Dazu gibt es das Format Vulnerability Exploitability Exchange (VEX). Den Softwareherstellern ermöglichen VEX Dokumente, ihren Kunden einerseits anzuzeigen, welche Schwachstellen seiner Software ihm bewusst sind und erleichtert diesem andererseits, sein Risiko beim Einsatz der Software einzuschätzen. VEX Dokumente sind maschinenlesbar und zeigen an, ob ein Produkt von der Schwachstelle betroffen ist und welche Schutzmaßnahmen zu empfehlen sind. Schwachstelleninformationen können sich ständig ändern, so dass zu empfehlen ist, VEX Dokumente getrennt von SBOMs – Softwarelieferketten Stücklisten – zu halten. Empfohlen wird den Softwareherstellern, die Kunden über neue Schwachstelleninformationen laufend mit VEX-Dokumenten zu unterrichten. Anwender können mit den standardisierten VEX Dokumenten feststellen, ob sie eine Schwachstelle in einer der von ihnen verwendeten Komponenten wirklich betrifft und über Änderungen der Sicherheitslage aktuell informiert bleiben. VEX existiert in zwei Varianten, erstens als Profil des Common Security Advisory Framework (CSAF), was inzwischen Standard ist, und zweitens als Teil des SBOM-Formats CycloneDX.[90]

21. Die unverzichtbare permanente Kontrolle der Softwarelieferkette nach Schwachstellen

Im Verlauf des Erstellungsprozesses von Software ist die Kontrolle nach Schwachstellen einfacher als nach der Fertigstellung, nach der die verschiedenen Versionen der SBOMs auf Verwundbarkeiten zu prüfen sind. Sourcecode Plattformen wie Github[91] enthalten eingebaute

[89] Braun Gunnar, Wie viel Standard steckt in SBOMs, in iX 9/2023 Seite 114.

[90] Braun Gunnar, Wie viel Standard steckt in SBOMs, in iX 9/2023 Seite 115,116,117 mit VEX Dokumenten als Beispiel.

[91] Github ist ein Onlinedienst zur Softwareentwicklung und Versionsverwaltung für Softwareprojekte auf Git-Basis. Das Unternehmen GitHub, Inc. hat seinen Sitz in San Fancisco und gehört zu Microsoft.

Abhängigkeitskontrollen (Dependency Checks), die auf verwundbare Komponenten prüfen. Die Verzeichnisse zur Speicherung und Beschreibung digitaler Objekte sind laufend nach oder bei Änderungen der Komponenten auf angreifbare Abhängigkeiten zu prüfen. Vor allem müssen auch die später erkannten Schwachstellen je nach den Versionen festgehalten werden.

Die Möglichkeit einer kontinuierlichen Überwachung, der Analyse von SBOMs und zur Benachrichtigung über Sicherheitslücken bietet OWASP[92] mit einem Dependency Track.[93]

Während die Informationstechnik zur Softwarelieferkettensicherheit als fortgeschritten eingeschätzt wird, werden Lücken bei der Organisation kritisiert. Informationen zur SBOMs von Zulieferern werden nicht gepflegt und den Kunden nicht zur Verfügung gestellt[94].

Möglicherweise fehlten zur Organisation der Cybersicherheit bisher die rechtlichen Vorgaben. Sie sind mit den §§ 30,38 BSIG neu formuliert. Die Geschäftsleiterverantwortung nach § 38 BSIG macht die Organisation von Risikomanagementmaßnahmen, den Stand der Technik, sowie die Berücksichtigung europäischer und internationaler Normen zur Pflicht. Die Haftung für die Verletzung dieser Pflicht können Geschäftsleiter nicht abbedingen.

22. Veröffentlichte SBOMs – Software Lieferkette - in Registrierdiensten

Registrierdienste helfen bei der Veröffentlichung von SBOMs, die für spezifische Container- Images[95] erstellt wurden und von Unternehmen heruntergeladen oder auch angeboten werden.[96] Zu Recht wird ein vertraulicher Umgang mit dem Austausch von SBOMs empfohlen. Zu rechnen ist nämlich damit, dass Hacker das Angebot an SBOMs ausspähen und direkt nach möglichen Angriffsvektoren suchen können.

---

[92] Die Open Web Application Security Project - **OWASP-** ist eine Non-Profit-Organisation mit dem Ziel, die Sicherheit von Anwendungen, Diensten und Software im Allgemeinen zu verbessern. Durch Schaffung von Transparenz sollen Endanwender und Organisationen fundierte Entscheidungen über wirkliche Sicherheitsrisiken in Software treffen können. Innerhalb dieser Gemeinschaft aus Firmen und sonstigen Einrichtungen aus aller Welt werden frei verfügbare Informationsmaterialien, Methoden, Werkzeuge und Technologien erarbeitet.

[93] Schneider, Udo, iX10/2022. SOFTWARE BILLS OF MATERIALS S. 68; Ein **Dependency Track** ist ein Instrument, um Risiken in Softwarelieferketten zu identifizieren und zu reduzieren.

[94] Schneider, Udo, iX10/2022. SOFTWARE BILLS OF MATERIALS S.71.

[95] Ein **Container Image** ist ein relativ isoliertes und unveränderliches Paket aus einer Software und den zur Laufzeit benötigten Werkzeugen und Dateien. Ein Image ist folglich für sich genommen lauffähig und äußerst robust.

[96] Plattformen zur Veröffentlichung von SBOMs bieten an z.B.: Red Hat Quay.io /ECR Public/Docker Hub/JFROG Artifactory/ aus Plogsties, iX 3/2024 Was die SBOM-Richtlinie für die Cloud bedeutet S.79 mit weiteren Hinweisen auf die gängigsten SBOM-Tools im Überblick.

23. Die Vorteile des SBOM Konzepts

SBOMs bieten Transparenz und machen die Einzelkomponenten einer Software sichtbar und nachvollziehbar. Die Anwender einer Software können durch die SBOM erkennen, welche Softwarekomponenten in ihren Anwendungen und Containern laufen und welche davon angreifbare Versionen enthalten und für sich allein ein Risiko darstellen können.
Log4Shell zum Beispiel würde als Einzelkomponente aufgeführt und könnte auf ein Risiko beurteilt werden. Mögliche Sicherheitsrisiken können schneller und sicherer identifiziert werden. Erkannte Sicherheitslücken können mit einem Patch geschlossen werden. Für das Lizenzmanagement können die Anwender die Nutzungsbedingungen leichter erkennen und damit rechtliche Risiken durch Lizenzverstöße verringern. Im Notfallmanagement kann bei einer Störung oder einem Ausfall durch eine Einzelkomponente diese leichter ausgetauscht werden, um die unterbrochene Arbeitsfähigkeit wiederherzustellen.[97]

Nachdem die Schutzmaßnahmen gegen das Risiko der Softwarelieferkette als Schwachstelle dargestellt wurde, sollen die Schutzmaßnahmen der Cyberhygiene nach der aktuellen Rechtslage beschrieben werden.

24. Maßnahmen zur Cyberhygiene als Stand der Technik

In § 30 Abs. 2 Nr.7 BSIG ist der Geschäftsleiter nach § 38 Abs.1 BSIG zu Maßnahmen zur Cybersicherheit nach dem Stand der Technik verpflichtet, wozu grundlegende Verfahren im Bereich der Cyberhygiene gehören. Eine Definition der „Cyberhygiene“ im Sinne der umzusetzenden NIS-2 Richtlinie bietet die Gesetzesbegründung. Dazu zählen mehrere Verfahren zur Verbesserung der Cybersicherheit, zum Beispiel

- Die Einschränkung von Zugriffskonten auf Administratorenebene
- Netzwerksegmentierungen,
- Backup- und Sicherungskonzepte für Daten,
- Regelung für sichere Passwörter,
- Patchmanagement.
- Berücksichtigung der Empfehlungen des Bundesamtes,
- Vertragliche Vereinbarungen mit Dienstleistern und Zulieferern zu Risikomanagementmaßnahmen.
- Schulungen- und Informationsmaßnahmen zum Schärfen des allgemeinen Bewusstseins der Mitarbeiter über Risiken mit IKT-Produkten.[98]

Die wichtigsten Grundsätze zur Cyberhygiene des Referentenentwurfs finden sich auch schon vorher in der Literatur mit Beschreibung des jeweiligen Schutzzwecks, der Anwendung und vor allem mit Fallbeispielen von Sicherheitsvorfällen, die bei der Beachtung des jeweiligen Grundprinzips hätten verhindert werden können.[99] Die folgende Kurzdarstellung

[97] Plogsties, iX 3/2024, Was die SBOM für die Cloud bedeutet, S. 80.

[98] Referentenentwurf zur Umsetzung der NIS-2-Richtlinie zu § 30 Abs.2 BSIG, Seite 148 Bearbeitungsstand 7.5.2024.Li.

[99] VMWARE White Paper: DIE WICHTIGSTEN GRUNDSÄTZE DER CYBER-HYGIENE

der Grundprinzipien soll den Begriff der Cyberhygiene zu konkretisieren helfen.

1. **Das Prinzip der minimalen Zugriffsrechte** soll verhindern, dass Anwender mit mehr Rechen ausgestattet sind, als sie eigentlich benötigen und dass Angreifer Benutzernamen und Kennwörter als Anmeldedaten sich unrechtmäßig beschaffen und auf die Systeme zugreifen können. Sicherheitsvorfälle bei den Firmen Target und Sony haben diese Schwachstelle ausgenutzt.
2. Ohne die Anwendung des **Prinzips der Mikrosegmentierung**, auch Netzwerksegmentierung, können Angreifer von einem Bereich, zu dem sie sich Zugang verschafft haben, problemlos in andere Segmente der Software gelangen. Im Falle von Target konnten die Angreifer nach dem Eindringen auf das Lüftungssystem bis in das Zahlungsnetzwerk vordringen. Bei dem Angriff auf das OPM (United States Office of Personnel Management) verschafften sich Angreifer über das LAN-Netzwerk zum Rechenzentrum des Innenministeriums. Im Vorfall Sony bewegten sich die Angreifer ebenfalls frei im Netzwerk. Segmentierung können Angreifer beim Vordringen von einem zum anderen Bereich behindern. Die gesamte IT-Umgebung soll in kleine Abschnitte unterteilt werden. Die einzelnen Anwendungen sind mit Grenzen zu umgeben.
3. Ohne wirksame **Verschlüsselung** können Hacker Daten in lesbarer Form abgreifen. Bei einem Vorfall bei Royal & Sun Alliance Insurance PLC stellte die Untersuchungskommission der Regierung fest, dass die Daten nicht ausreichend verschlüsselt waren. Im Falle einer Datenverletzung müssen die Daten unlesbar sein.
4. **Ohne das Prinzip der Mehrfach-Authentifizierung – auch Multi-Factor Authentication – MFA -** können Hacker sich Kennwörter und damit Zugriff auf Systeme verschaffen. Im Vorfall bei Linkedin wurden unzureichend geschützte Kennwörter von 100 Millionen Anwendern offengelegt. Das Risiko bestand darin, dass Anwender häufig dasselbe Kennwort für mehrere Websites verwenden, Durch MFA hätte dieses Risiko abgewendet werden können. Im Vorfall von OPM konnten die gestohlenen Anmeldedaten von Hackern uneingeschränkt missbraucht werden, weil keine MFA Schranke eingesetzt war.
5. **Das Prinzip des effektiven Patchings verhindert** das Missbrauchen von Schwachstellen durch Hacker. Vorhandene Patchs[100] sollten auf jeden Fall eingesetzt werden, um identifizierte Schwachstel-

RUND UM CLOUD UND MOBILITÄT, Seite 5 ff.

[100] Patches sind Nachbesserungen von erkannten Schwachstellen.

len zu schließen. Im Vorfall WannaCry ist es dem Erpressungstrojaner gelungen, eine schon bekannte Softwareschwachstelle auszunutzen, für die ein Patch vorhanden war, aber nicht eingesetzt wurde, um die Lücke zu schließen.[101]

25. Die weiterentwickelte IT-Sicherheits- Regelung in zwei Richtlinien nach EU-Recht

Der Schutz der IT-Sicherheit Kritischer Infrastrukturen ist bisher im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) vom 14.8.2009 geregelt.

Seit 16.Januar 2023 sind zwei Richtlinien der EU in Kraft, die Cybersicherheits- und Resilienzrichtlinien **NIS2** (Network an Information Security) und **CER** (Critical Entities Resilience Directive).

Die CER regelt den physischen Schutz vor Sabotagen und Angriffen. Die NIS2 regelt die Sicherheit der Informations- und Kommunikationstechnik.

Beide Richtlinien sollen sicherstellen, dass die Bevölkerung der EU mit lebenswichtigen Gütern und Diensten von den als kritisch eingestuften Einrichtungen versorgt werden können.

26. Der erweiterte Anwendungs-bereich der Richtlinien

Anzuwenden sind die Richtlinien auf **achtzehn Industriesektoren** mit Vorgaben an das Risikomanagement und die Cyber-sicherheit. Mit der Richtlinie 2022/2557 wurde ein einheitlicher europäischer Rechtsrahmen für die Stärkung der Resilienz kritischer Einrichtungen in mindestens elf Sektoren gegen Gefahren auch außerhalb des Schutzes der IT-Sicherheit im Binnenmarkt geschaffen.[102] Die Richtlinie schafft einen übergreifenden Rahmen, der als „DACH“ illustriert wird, einen All-Gefahren-Ansatz verfolgt, und damit auch Naturkatastrophen oder vom Menschen verursachte, unbeabsichtigt oder sogar vorsätzliche Gefährdungen berücksichtigt. Zur Abgrenzung von der IT-Sicherheit wird das Ziel als „physischer Schutz“ bezeichnet. Mit dem KRITIS-DachG werden erstmals eigenständige sektorenübergreifende abstrakte Regelungen getroffen. Das KRITIS-DachG soll einen Prozess aufsetzen, der nationale und betreiberseitige Risikobewertungen in allen Sektoren, das Erstellen von Resilienzplänen durch die Betreiber, und branchenspezifische Schutzstandards fördert.[103]

Nach **Schätzungen des statistischen Bundesamtes werden zehnmal** mehr Unternehmen als bisher gesetzlich zur Einhaltung der Rechtsvorschriften aus den Richtlinien verpflichtet sein.[104] Bisher sind beim BSI 800 Betreiber kritischer Infrastrukturen registriert. Dazu kommen noch etwa zwei- bis dreitau-

[101] VMWARE White Paper: DIE WICHTIGSTEN GRUNDSÄTZE DER CYBER-HYGIENE RUND UM CLOUD UND MOBILITÄT, Seite 12.

[102] Referentenentwurf vom 21.12.2023, S. 1.

[103] Referentenentwurf vom 21.12.2023, S. 1 und 2 unter Problem und Ziel.

[104] Plate, NIS2 – und jetzt?, in iX 2024 S. 53.

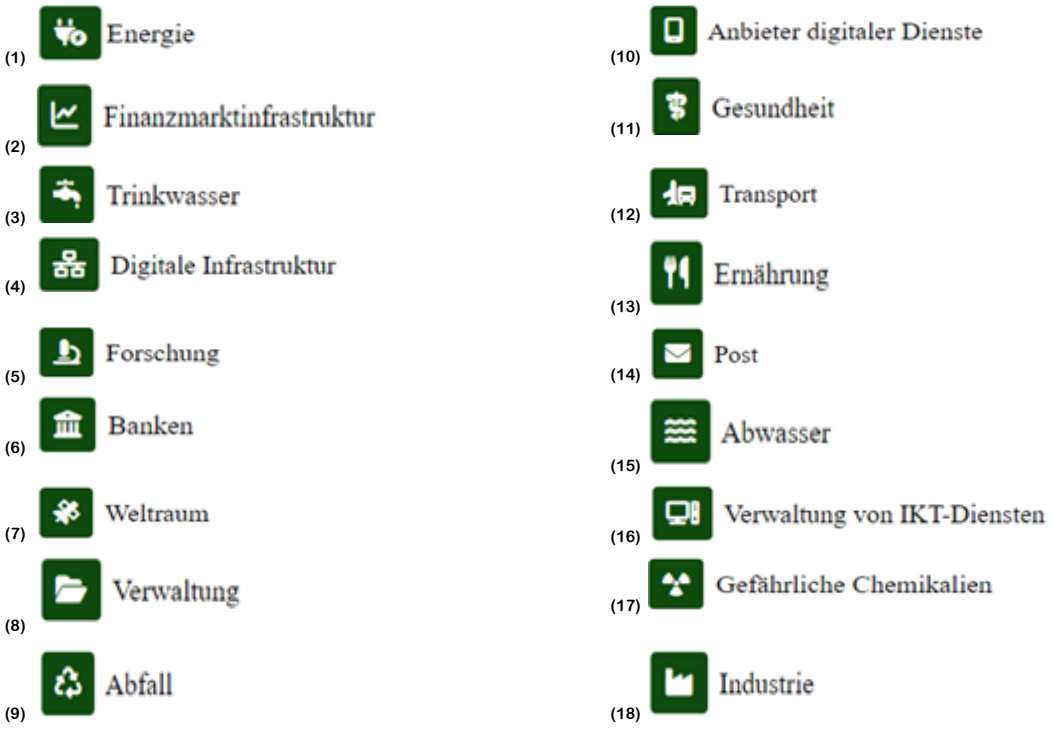
send Unternehmen im besonderen öffentlichen Interesse aus dem Chemie- und Rüstungssektor. **Nach der Umsetzung von NIS2 und CER in Deutschland betrifft die Regulierung rund 30 000 Einrichtungen. Doppelt so viele Sektoren als bisher werden als kritisch eingestuft.** Die Klassifizierung als kritische Einrichtung richtet sich gemäß der Neuregelung nach Unternehmensgröße und Umsatz. Erstens müssen Unternehmen zu den achtzehn Sektoren und zweitens mehr als 50 Mitarbeiter oder 10 Millionen Euro Jahresumsatz haben, um als "wichtige Einrichtungen" zu gelten. „Besonders wichtige Einrichtungen – essential entities" gelten Unternehmen mit mehr als 250 Mitarbeitern oder 50 Millionen Euro Jahresumsatz. Die besonders wichtigen Einrichtungen sind zum aktiven Nachweis des Einhaltens der vorgegebenen Regeln verpflichtet. Dies gilt schon bisher für die KRITIS Betreiber.[105] Bisher wurden Unternehmen als kritisch danach eingestuft, ob sie mit dem Ausfall ihrer Leistung 500.000 zu versorgende Personen betreffen.

Die im Folgenden aufgelisteten achtzehn Sektoren zählen zu dem Anwendungsbereich der Richtlinien CER (Critical Entities Resilience Directive) und NIS2 (Network and Information Security), da aus diesen Wirtschaftsbranchen die EU-Bürger mit lebenswichtigen und existentiellen Gütern und Dienstleistungen versorgt werden.[106]

---

[105] Plate, NIS2 – und jetzt? in iX 2024 S. 53.

[106] Anhang I Sektoren mit hoher Kritikalität zur Richtlinie EU 2022/2555 des Europäischen Parlaments und des Rates – Stand: 14.12.2022 S. 123.



27. Die Begründung der neuen Regelungen für kritische Anlagen

In der Begründung des Referentenentwurfs wird die bisherige Rechtslage vor und nach dem Entwurf beschrieben. Grundsätzlich sind in einer Marktwirtschaft die Betreiber kritischer Anlagen aus eigenem Interesse an der Funktionsfähigkeit ihrer Anlagen interessiert. Kommt es allerdings zu Störungen der Versorgung mit Strom, Wasser, Lebensmitteln, kann es zu Kettenreaktionen und Kaskadeneffekte über die gesamte Wertschöpfungskette kommen. Nachteile drohen nicht nur dem einzelnen Versorgungsunternehmen, sondern allen Unternehmen, die von den kritischen Dienstleistungen wie Wasser, Strom, Verkehr, Lebensmitteln abhängig sind, und zwar europaweit.[107] Bisherige Regelungen sind sektorenspezifisch. Sektorenübergreifend und bundeseinheitlich sind dagegen die folgenden neuen Regelungen nach dem KRITIS-DachG zur allgemeinen Verbesserung der Resilienz

- Gleiche Resilienz Maßnahmen,
- Zur Identifizierung kritischen Anlagen,
- Zu gleichen Maßnahmen und Mindeststandards zur Resilienz,
- Zur Aufrechterhaltung des Betriebs kritischer Anlagen,
- Zur zügigen Wiederherstellung gestörter und ausgefallener Anlagen,
- Zu einheitlichen Analyse und Bewertung gleiche Risiken,

[107] Begründung Referentenentwurf, Stand 7.5.2024, S.30.

- Zu einem gleichen Störungsmonitoring,
- Zum fortlaufenden Überblick über gleiche Risiken,
- Zum Austausch von Erfahrungen über gleiche Risiken und gleiche Indizien, die Rückschlüsse auf drohende Risiken zulassen,
- Durch vereinheitlichte Begriffsbestimmungen,
- Durch Mindestvorgaben für Resilienz Maßnahmen,
- Durch die Einführung eines Meldewesens für Sicherheitsvorfälle,
- Durch Berichtspflichten gegenüber der EU Kommission.

Der Anspruch auf die Sicherung störungsfreier Versorgung mit lebenswichtigen Leistungen und der Anspruch auf die Resilienz der Daseinsvorsorge lässt sich aus dem Sozialstaatsprinzip herleiten und umfasst auch die Infrastruktur, auf die jeder angewiesen ist. Das Sozialstaatsprinzip ist als Staatszielbestimmung in Art. 20 I GG und Art. 28 I S.1 GG. begründet. Subjektive Rechte und Ansprüche lassen sich jedoch nicht herleiten.[108]

Die zu beobachtende rechtspolitische Akzeptanz der verpflichtenden Regelungen zur Stärkung der Resilienz der Daseinsvorsorge in Form der Cybersicherheit ergibt sich aus der Bedrohungslage durch die Cyberangriffe und der unternehmensinternen Einsicht, dass dringende Investitionen leichter zu entscheiden und durchzusetzen sind, wenn eine gesetzliche Pflicht dazu besteht. Das Gesetz liefert den IT-Abteilungen die Argumente für das Aufstocken ihrer Budgets und die Delegation von Befugnissen.[109] Hinzu kommt die neu geregelte Geschäftsleiterverantwortung, für die Vorstände und Geschäftsführer persönlich haften, die sie nicht an Angestellte unterhalb der Organebene delegieren und ausdrücklich auch nicht abbedingen können. Beim Genehmigen von finanziellen und personellen Mitteln für die Cybersicherheit im Unternehmen schützen sich in Zukunft die Geschäftsleiter selbst persönlich. Die neue Geschäftsleiterverantwortung für Cybersicherheit begründet damit starke Motive zu erhöhter Aufmerksamkeit und Investitionsbereitschaft.

Die Daseinsvorsorge ist zwar grundsätzlich die Aufgabe der öffentlichen Hand. Nachdem jedoch Krankenhäuser, Wasser-, Energieanbieter und Telekommunikationsnetzbetreiber zunehmend privatisiert wurden, erscheint es als konsequent, auch private Versorgungunternehmen zur Resilienz der von ihnen angebotenen Daseinsvorsorge in Form der Sicherheit vor Cyberangriffen zu verpflichten.

28. Die Ziele und Maßnahmen zur Resilienz nach § 10 KRITIS-DachG und Art.21 NIS-2

Die Anforderungen der NIS2 Richtlinie ist in Art.21 geregelt und enthält zehn Risikomanagementmaßnahmen zur Cybersicherheit. Sie sind abstrakt formuliert und als Grundvoraussetzungen von allen Einrichtungen einzu-

[108] Sachs, Michael, in: Sachs, Grundgesetz Kommentar, 8. Auflage 2018, Art. 20, Rn. 47 ff. Karl-Peter, in: von Mangoldt/Klein/Starck, Kommentar zum Grundgesetz, Band II, 7. Auflage 2018, Art. 20 Rn. 103.

[109] Plate, NIS2 – und jetzt?, in iX 2024 S. 53.

halten. In deutsches Recht übernimmt das KRITIS-Dachgesetz die Vorgaben in § 10. Die Vorschrift nennt in § 10 Abs.1 Nr. 1 bis 6 die Ziele und dazu in Abs.3 Nr.1 bis 6 die Schutzmaßnahmen.

Konkret regelt die Vorschrift in Abs.3

- Nr. 1 das Verhindern der Vorfälle durch Notfallvorsorge
- Nr. 2 den physischen Schutz durch Zäune, Umgebungsüberwachung, Detektionsgeräte,
- Nr. 3 die Reaktion auf Vorfälle, durch Alarmfallpläne, Krisenmanagement,
- Nr. 4 die Wiederherstellung des Betriebs durch Notstromversorgung und Ermittlung alternativer Lieferketten zur Wiederaufnahme des Dienstes,
- Nr. 5 das Personal- und Sicherheitsmanagement,
- Nr.6 das Informieren, Schulen und Üben.

29. Stand des Gesetzgebungsverfahrens zur Umsetzung in deutsches Recht

Die neue **NIS-2-Richtlinie** vom 16.1.2023 EU 2022/2557 ist nunmehr in deutsches Recht umzusetzen, gemäß Art. 26 I **bis zum 17.Oktober 2024**.

Ein offizieller Entwurf mit dem Titel (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz- BSIG) **liegt seit dem 7.5.2024 vor**.[110]

Der zweite Referentenentwurf ist unter den Ressorts schon abgestimmt. Die Länder und Verbände sind angehört. Das KRITIS-Dachgesetz normiert erstmals und einheitlich bundesgesetzliche sektorenübergreifende Mindeststandards. Das KRITIS-Dachgesetz wird neben dem BSIG gelten. Eine größtmögliche Kohärenz wird angestrebt. Ziel und Zweck ist die Stärkung der Resilienz von Betreibern kritischer Anlagen durch physische Maßnahmen.

30. Die Aufrechterhaltung des Betriebs mit Backup Management, Wiederherstellung nach Notfällen und Krisenmanagement nach § 30 Abs.2 Nr. 3 BSIG

30.1 Das Risiko des Datenverlusts durch Datensicherung abwenden

Daten werden immer mehr auf Computern gespeichert. Daten gehen ohne Vorwarnung verloren, wenn der Massenspeicher beschädigt wird, verursacht durch defekte Festplatten, Computerviren, Diebstahl, Brände, versehentliches Löschen, Hardwarefehler aber auch immer vermehrt durch Hackerangriffe. Je mehr Daten verloren gehen können, umso wichtiger wird **die Datensicherung**, Dabei werden die Dateninhalte eines Computers regelmäßig auf ein anderes Medium kopiert, auf eine externe Festplatte oder SSD[111] . Dadurch wird das

[110] Das KRITIS – DachG ist als Art.1 des BSIG geregelt. Art. 2 ist die Änderung, Art. 3 die Regelung zum Inkrafttreten am 18.10.2024.

[111] Der Begriff **SSD** steht für "Solid-State-Drive" oder auch "Halbleiterlaufwerk". Es han-

Risiko des Datenverlusts vermindert. Automatisch werden durch eine **Backup-Software** die zu sichernden Daten auf ein oder sogar mehrere Medien kopiert. Im Schadensfall des Verlusts gleichgültig aus welchen Gründen, existieren **mindestens eine Sicherungskopie**.

30.2 Das Backup-Management als neue gesetzliche Pflicht zur Datensicherung

Das Backup-Management wird nach § 30 Abs. 2 Nr.3 i.V.m.§ 38 BSIG ausdrücklich **zur Pflicht des Geschäftsleiters, der die Letztverantwortung dafür trägt und haftet**. Was Geschäftsleiter deshalb wissen sollten, um diese Backup-Management-Pflicht erfüllen zu können, wird im Folgenden dargestellt.

Das Backup-Management gehört zur Sicherstellung und Aufrechterhaltung des Betriebs, zur Wiederherstellung nach Notfällen und zum Krisenmanagement. Je weiter die Digitalisierung von Unternehmen vorankommt, desto anfälliger werden sie gegen Angriffe auf die IT-Infrastruktur und um so größer werden die Schäden.

Zunächst sind die Störfaktoren wie etwa ein Stromausfall zu identifizieren und zu verhindern.

Ein Backup ist eine Sicherungskopie, mit der Daten oder Systeme wiederhergestellt werden können. Entscheidend ist für ein Backup, wie groß der Zeitraum zwischen der letzten Sicherung und der aktuellen Version der Sicherungskopie sein muss. Oft kann schon das Backup vom Vortag veraltet sein.[112]

Zu unterscheiden ist ein Backup von einem **Archiv**, das die Nachvollziehbarkeit von Datenbeständen sichern soll, auf längere Laufzeiten ausgelegt ist und höhere Speicherkosten verursacht.

30.3 Gegenstand von Backup und Sicherungskopie

Zunächst gilt es ein gesamtes System zu sichern. Die Wiederherstellung des gesamten Systems bringt allerdings Nachteile mit sich. Nach einem IT-Sicherheitsvorfall durch einen Hackerangriff mit Schadsoftware ist nicht auszuschließen, dass die eingeschleuste Schadsoftware im Rahmen der Wiederherstellung mit übernommen wird. Forensiker[113] müssen als Sachverständige dann jedes Bit auf mögliche Infektionen prüfen, um sicher zu sein, dass nicht Teile der Schadsoftware beim Wiederherstellen mitübernommen werden. Dadurch dau-

---

delt sich dabei um ein elektronisches Speichermedium. Für SSD-Speicher werden Flash-basierte Speicherchips und SDRAMs verwendet. Auf Grund der sehr schnellen Zugriffszeiten, ihrem robusten Aufbau und ihrer Geräuschlosigkeit, werden SSD-Festplatten gegenüber herkömmlichen Magnetenspeicher-Laufwerken bevorzugt.

[112] Wienströer, Praxis: Backups aus Sicht der IT-Sicherheit, iX 5/2024 S.129.

[113] **IT-Forensik** wird vom BSI als „die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen, unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung, insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems“ definiert. Forensiker sind die IT-Sachverständigen beim Aufklären von IT-Sicherheitsvorfällen.

ert die Untersuchung von Forensiker lange und blockiert den Geschäftsbetrieb des angegriffenen Unternehmens. Empfohlen wird deshalb, Systeme nach Durchlauf- und Ablagesystem zu trennen und vorrangig Ablagesysteme wie Datenbankserver unbedingt wiederherzustellen, um den Forensiker Aufwand zu reduzieren und den Betrieb schneller wiederaufzunehmen.[114]

30.4 Manipulationssicher Installationssoftware offline aufbewahren

Zur Reduktion des Forensiker Aufwands beim Untersuchen nach Schadsoftware
wird empfohlen, zur Datensicherung vor einem eventuellen IT-Sicherheitsvorfall die Installationssoftware und Installationsroutinen offline[115] zu speichern, um sie vor Manipulationen aus dem Internet zu sichern.[116] Weiter ist zu klären, ob selbstständige Exporte durch das Programm erstellt werden kann. Im Interesse einer schnellen Wiederherstellung des Betriebs wird auch empfohlen, auf einem frischen Server die angegriffene Software zu installieren und zeitliche parallel dazu von Forensikern die Software auf Schadsoftware prüfen zu lassen.

[114] Wienströer, Praxis: Backups aus Sicht der IT-Sicherheit, iX 5/2024 S.130.

[115] **Offline** bedeutet, „kein Zugang zum Internet“, „nicht im Netzwerk“ und bezeichnet in der Informatik einen Zustand, in dem ein Gerät, das über eine Kommunikationsschnittstelle verfügt, nicht bereit ist, Daten über diese Schnittstelle zu empfangen oder zu senden. Das Gegenteil davon ist *online*.

[116] Wienströer, Praxis: Backups aus Sicht der IT-Sicherheit, iX 5/2024 S.130.

30.5 Der Umfang der zu sichernden Daten entweder 3-2-1 oder 3-2-1-1-0

Drei Kopien sind zu sichern, wobei über die produktive Datei hinaus zwei weitere zu kopieren sind. Drei Kopien sind auf zwei unterschiedlichen Medien und eine davon **offsite**, d.h. an einem anderen als dem Ort, an dem das System installiert ist.[117]
Das 3-2-1 Standard Konzept kann erweitert werden um eine weitere Offlinekopie und eine Kopie für das Prüfen auf Fehlerfreiheit der Backups auf das Konzept 3-2-1-1-0.

Die zwei geforderten Backup-Kopien sind von der Backup-Software auf primären und sekundären Speicherorten abzulegen, die sich in getrennten Brandabschnitten befinden.[118]

30.6 Zwei unterschiedliche Medien nutzen

Die zwei Backup-Kopien sollen auf zwei unterschiedlichen Medien liegen, zum Beispiel auf

[117] Ein **Offsite-Backup** ist eine Form der Datenspeicherung, bei der Kopien der Daten an einen sicheren, externen Ort gesendet werden. Dieser entfernte Speicherort ist getrennt vom primären Speichersystem. Im Falle eines Ausfalls oder einer Katastrophe können Sie auf diese Daten zugreifen[1]. Unternehmen nutzen Offsite-Bac, um ihre Daten sicher und zugänglich zu halten, selbst wenn der Hauptstandort ausfällt oder kompromittiert wird. Es ist eine wichtige Maßnahme für **Business Continuity**, um den Geschäftsbetrieb aufrechtzuerhalten.

[118] Wienströer, Praxis: Backups aus Sicht der IT-Sicherheit, iX 5/2024 S.133.

Bändern, Festplatten, Flash[119] oder in der Cloud. Bei der Sicherung auf Bändern müssen diese offline gespeichert sein. Bei dem Cloud-Backup ist zu empfehlen, die Backups mit einem Datum und einem Immutable-Flag[120] zu versehen, und dieses Backup als unveränderlich und nicht verändert zu kennzeichnen.[121]

30.7 Datensicherung in der Cloud

Im IT-Sicherheitsvorfall darf die eigene Hardware on Premises[122] nicht verändert werden, während sie von Versicherungen oder Forensikern untersucht wird. Der Betrieb bleibt solange blockiert. Dagegen lassen sich in der Cloud Systeme wiederherstellen und aktivieren, was als Vorteil gelten kann. Der Betrieb ist schneller wiederherzustellen. Allerdings darf die Notfall-Cloud-Umgebung nicht mit dem Produktionsnetz verbunden sein. Und der Zugriff durch eventuell infizierte Endgeräte muss verhindert sein. Warnend hervorgehoben wird zu Recht, dass ein Backup in der Cloud nur in der Theorie sicher ist. Automatisierte Backups aus der Produktivumgebung lassen sich nicht von der Cloud-Backup trennen und ein Cloud-Backup muss ebenfalls an einem anderen Ort gespeichert werden.[123]

30.8 Datensicherung am andern Ort

Im Konzept 3-2-1 steht die **1 für einen externen anderen Ort** als den Standort des Systems. Vermieden werden sollen die Risiken, die mit dem normalen Standort des Systems verbunden sind, wie zum Beispiel der Gebäudebrand oder der Diebstahl. Der andere Ort kann eine Filiale, ein Bankschließfach oder ein Rechtenzentrum sein.

Die zweite 1 steht für eine Sicherungskopie offline, auf einem Wechseldatenträger z.B. einem Band oder einer USB-Platte, auf jeden Fall nicht über das Netzt erreichbar. Cloud-Speicher wie mit immutable Flag versehen, zählen nicht zu den echten Air Gaps. Eine sicherere Sicherungskopie ist die Firmware WORM[124] auf LTO Bändern. Eine gebrannte

---

[119] **Flash-Speicher** ist eine Technologie, die hohe Performance und geringe Latenzen garantiert und die Leistung mechanischer Festplatten übertrifft.

[120] **Immutable** gleich Unveränderlich bedeutet hier, dass Backup Dateien weder verändert, noch gelöscht werden können. Das ist nur machbar mit Root-Rechten im Linux OS. So kann selbst ein Administrator, am Backup Server, im Repository Dateien weder verändern noch löschen.

[121] Wienströer, Praxis: Backups aus Sicht der IT-Sicherheit, iX 5/2024 S.133.

[122] **On-Premises oder On-Prem** (*in den eigenen Räumlichkeiten*, *vor Ort* oder *lokal*) bezeichnet ein Nutzungs- und Lizenzmodell für Computerprogramme (Software). Bis ca. 2010 war die lokale Nutzung bzw. die Lizenzierung für die lokale Nutzung von Software der Normalfall und hatte daher keine besondere Bezeichnung. Erst seitdem die lokale Nutzung zunehmend von Software as a Service (SaaS) oder Cloud Computing verdrängt wird, ist der Begriff Off-Premises als Antonym entstanden.

[123] Wienströer, Praxis: Backups aus Sicht der IT-Sicherheit, iX 5/2024 S.134.

[124] **WORM** ist ein Akronym für „write once read many“ oder „write once read multiple“ (englisch für „schreibe einmal, lies viel-

CD oder DVD würde ein echtes Hardware-WORM darstellen.[125]

30.9 0 = Null Fehler im Backup

Die 0 im Konzept 3-2-1-1-0 steht für Null Fehler im Backup, weil täglich die Datensicherung kontrolliert wird. Fehlerfreiheit kann nur durch die tägliche Auswertung des Cloud-Speichers und die Prüfung nach Anomalien erreicht werden. Empfohlen wird die Untersuchung der Systeme in vertretbaren Zeiträumen und die regelmäßige Wiederherstellung der Systeme aus den Backup-Daten. Schließlich wird das Training für die routinemäßige Wiederherstellung der Systeme empfohlen, vergleichbar mit Feuerwehrübungen, Notstromtests.

30.10 Die Dauer der Datensicherung und die Empfehlung zur mehrgleisigen Backup Management Datensicherungsstrategie

Als normale Vorhaltezeit gelten drei Monate. Weil sich allerdings Hacker mit ihrer Schadsoftware monatelang unbemerkt im Unternehmensnetz aufhalten können, wird die Sicherheit der Sicherungskopie nicht erhöht. Wichtiger erscheint es, die Sicherungskopie in einer völlig abgetrennten Umgebung als Kopiervorlage aufzubewahren und nicht etwa für die Wiederherstellung wegen versehentlich gelöschten Emails und sonstigen Dateien zu nutzen. Zu Recht wird auf die Praxis der Hacker hingewiesen, unternehmensinterne Anfragen vorzutäuschen um an die Kopien zu kommen. Schließlich wird wegen der verstärkten Hackerangriffe empfohlen, die Datensicherungstechnik, die Speicherorte, häufiger zu wechseln und bei der Datensicherung mehrgleisig und flexibler vorzugehen, um das Ausspähen den Hackern zu erschweren.

31. Die Pflicht zur Zugriffskontrolle nach § 30 Abs.2 Nr. 8 BSIG

Maßnahmen zur Einhaltung der Pflicht nach § 30 Abs. 1 BSIG, um die informationstechnische Sicherheit bei besonders wichtigen und wichtigen Einrichtungen zu gewährleisten, müssen nach § 30 Abs.2 BSIG den Stand der Tech-

---

fach“). Dies bezeichnet Vorkehrungen in der Informationstechnik, die das Löschen, Überschreiben und Ändern von Daten auf einem Speichermedium dauerhaft ausschließen, um vor Datenverlusten durch menschliche Fehler, Programmfehler und Schadsoftware zu schützen. Die dabei eingesetzten Datenspeicher können fortgesetzt bis zu ihrer Kapazitätsgrenze beschrieben und ansonsten nur gelesen werden.

[125] Bei einem **Air Gap** handelt es sich um eine „**physische Netzwerkisolierung**“. Es ist ein Prozess, bei dem Daten durch den Transport eines Speichermediums auf eine externe Festplatte oder ein Magnetband (LTO1-LTO8) aus dem Netzwerk heraus isoliert werden.
Wienströer, Praxis: Backups aus Sicht der IT-Sicherheit, iX 5/2024 S.134.

nik[126] bei den Konzepten für die Zugriffskontrollen einhalten. Aus der Fachliteratur zur Informationstechnik ist deshalb zu ermitteln, welche Risiken bekannt und welche Abwehrtechniken durch Zugriffskontrollen nach dem aktuellen Stand der Technik verfügbar sind.

Das Risiko von Angriffen durch missbrauchten Zugriff ergibt sich aus der aktuellen Statistik des BSI. Bei 20% der Schwachstellen konnten Angreifer Speicher sowie Anwendungsdaten manipulieren, um erbeutete Zugriffsrechte zu erweitern. An dritter Stelle mit 13 % lagen Softwareprodukte ohne funktionierende Zugangskontrollen (Broken Access Control). Sie verletzten das Prinzip der standardmäßigen Verweigerung des Zugangs und erlaubten ohne weitere Zugangskontrolle jeglichem Nutzer den Zugriff, ermöglichten die Umgehung er Zugriffskontrollen oder gewährten authentifizierten Benutzern die Verwendung der Software mit Administratorenrechten.[127]

[126] **Stand der Technik** ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zur Begrenzung des Risikos von Sicherheitsvorfällen durch IT-Ausfällen insgesamt gesichert erscheinen lässt. Bei der Bestimmung des *Standes der Technik* sind insbesondere die in der Anlage [der jeweiligen Rechtsnorm] aufgeführten Kriterien zu berücksichtigen.“ Seit dem Kalkar Beschluss wird der Stand der Technik nach der Dreistufentheorie zwischen den allgemein anerkannten Regeln der Technik und dem Stand von Wissenschaft und Technik eingestuft. BVerfG, 8.8.1978 – 2 BvL 8/77, BVerfGE 49, 89, 143 (Kalkar-Beschluss).

[127] BSI, Die Lage der IT- Sicherheit in Deutschland 2023, S. 34.

Zum Kern eines Sicherheitskonzept gehört die Zugriffskontrolle – das RBAC-Modell (Role-based Access Control). Sie sichert die Verfügbarkeit, die Vertraulichkeit und die Integrität.[128] Unterschieden werden in diesem Konzept Berechtigungen zur Nutzung von Einrichtungen oder zu bestimmten Tätigkeiten, während diese Berechtigung an eine Rolle vergeben werden. In Beziehung zueinander stehen die Berechtigungen, die Rolle, der Berechtigte und die Einrichtung oder Tätigkeit, zu der er berechtigt ist. Der Zugriff ist die Berechtigung, der Zugriffsberechtigte ist die Rolle, und berechtigt wird zur Nutzung einer Software.

31.1 Drei Einschränkungen dienen der IT-Sicherheit

- Nach dem **Least-Privilege-Prinzip** soll jeder Nutzer immer die geringstmögliche Anzahl von Berechtigungen für die berechtigte Nutzung haben. Diese Beschränkung verhindert, dass die Berechtigung missbraucht wird und zum Schaden führt.
- Nach dem Prinzip der **Funktionstrennung** müssen für kritische Benutzungen die Berechtigungen auf mindestens zwei Personen delegiert werden. Damit wird die Wahrscheinlichkeit von Missbrauch der Berechtigungen verringert, weil dann statt nur einer Person zwei kompromittiert oder korrumpiert werden. Diese Einschränkung ist das Zwei-Augen-Prinzip. Getrennt wird im Compliance-System RECHT IM BETRIEB die Stabsfunktion der Beauftragten, die kontrollieren, beraten und

[128] Berberovic, Role Engineering für rollenbasierte Zugriffskontrolle, iX 3/2024 S. 90.

informieren, während die Entscheidungsträger mit Linienfunktion nur entscheiden und ausführen, um Interessenkonflikte zu vermeiden, wenn die Entscheidungsträger sich selbst kontrollieren sollten. Die Berechtigungen beziehen sich im Compliance-System auf das Pflichtenmanagement. Geregelt wird, wer Berechtigungen delegiert, Vorstände und Geschäftsführer in ihrer Funktion als Organe, welche Pflichten beraten, kontrolliert und informiert und erfüllt werden, und nur genau nach Einzelparagraphen bezeichneten Pflichten.

- Nach dem **Prinzip Just-in-time** sollen Berechtigungen zu Aufgaben nur zeitlich begrenzt delegiert werden, um den missbräuchlichen Einsatz von Berechtigungen durch Kompromittierung des Nutzers zu verhindern. Bestimmt wird im Compliance-System auch der Zeitpunkt der Pflichterfüllung je nachdem, ob es Einmal-, Melde-, oder Pflichten sind, um ein bestimmtes Risiko abzuwenden.[129] Der Missbrauch könnte im Löschen, im Manipulieren der Pflichten bestehen, so dass das Unternehmen im Ergebnis rechtswidrig handelt oder Pflichten unterlässt oder rechtswidrig erfüllt, so dass im Ergebnis rechtswidrige unsichere Produkte, z.B. Arzneimittel, Lebensmittel, Autos mit Defekten, oder mit sonstigen Schadensrisiken produziert werden.

Im Ergebnis erweist sich das Rollenkonzept als relational, weil Rollen, die Pflichtenträge, die Pflichten selbst, die Berechtigung zur Organisation der Pflichten, nämlich die Nutzung des Systems zum Ermitteln, Delegieren, Aktualisieren, Erfüllen, Kontrollieren und Dokumentieren, in eine Beziehung durch Verlinkungen gesetzt werden. Die Beziehung durch Verlinken ist dauerhaft, die Rollen, Funktionen oder Aufgaben sind getrennt voneinander. Jeder wird auf seine Aufgabe, seine Pflichten und seine Rechte beschränkt.

32. Die Multi-Faktor-Authentifizierung (MFA) als Geschäftsleiterpflicht nach § 30 Abs.2 Nr.10 BSIG neu

32.1 Das Authentifizierungsverfahren nach Zweck und Nutzen

Die die MFA hat sich als Konzept von Authentifizierungsverfahren etabliert und wird seit Jahren schon im Finanzsektor eingesetzt[130] und entspricht damit dem Stand der Technik, zu dem Geschäftsleiter neuerdings verpflichtet werden.

Die Maßnahmen nach § 30 Abs.1 BSIG neu müssen zumindest nach Abs. 2 Nr.10 umfassen,

- ***Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlicher Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebe-***

[129] Berberovic, Role Engineering für rollenbasierte Zugriffskontrolle, iX 3/2024 S. 93.

[130] Kuppinger, Mehr Sicherheit durch risiko- und kontextbasierte MFA iX 5/2024 S.53.

nenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Mit dem Verfahren der Authentifizierung stellen Unternehmen sicher, dass ausnahmslos berechtigte Personen auf die Unternehmenssoftware zugreifen können. Die Authentifizierung ist für die Cybersicherheit unverzichtbar. Cyberangreifer und Hacker verschaffen sich unbefugten Zugang zu Softwaresystemen, um Benutzernamen und Kennwörter von befugten Personen mit Zugriffsberechtigungen zu erbeuten und damit die kontrollierten Einfallstore zur Unternehmenssoftware zu überwinden.

Das Authentifizierungsverfahren verläuft in drei Etappen.

- Mit dem ersten Schritt der **Identifizierung** definiert der Nutzer seine Identität durch seinen Benutzernamen.
- Beim zweiten Schritt – der **Identifizierung** - bestätigen die Nutzer durch die Eingabe eines Kennworts, das nur sie kennen, dass sie die Person sind, für die sich ausgeben. Um die Sicherheit noch zu verstärken, fordern viele Unternehmen ein drittes Identitätsmerkmal, wie etwa die Telefonnummer, das Geburtsdatum oder den Fingerabdruck.
- Beim dritten Schritt - **der Autorisierung** - wird durch das System geprüft, ob der Nutzer eine Zugriffsberechtigung verfügt.

Das MFA nutzen Unternehmen zum Schutz Ihrer Software Systeme vor Angriffen, zum Schutz der Vertraulichkeit ihrer Kunden, und vor dem Ausspähen von Geschäftsgeheimnissen.

Sind die Zugriffskontrollen unzureichend, können Angreifer Kennwörter erraten oder Anmeldeinformationen missbrauchen.

32.2 Das Risiko des Identitätsdiebstahls durch Phishing-as-a-Service (PhaaS)

Das Risiko besteht darin, dass Schadsoftware installiert wird und Daten missbräuchlich exportiert werden.

Nach der letzten BSI Statistik wurden mit einem Anteil von 6 % Produkte mit Schwachstellen in den Identifikations- und Authentifizierungssystemen noch vergleichsweise selten gemeldet. Dazu zählt das BSI auch die Multifaktor-Authentifizierungen – MFA - . Bekannt sind nach dem BSI inzwischen Schadprogramme, die diese Form der Authentifizierungen umgehen können. Identitätsdiebstahl gilt als kriminelles Geschäftsmodell mit der Abkürzung Phishing-as-a-Service (PhaaS)[131].

Eine Vielzahl von Phaas-Anbietern beliefern Angreifer mit unterschiedlichen Diensten, von der Erstellung, dem Versand von Phishing-E-Mails über die Verwaltung, Weiterleitung bis zu den endgültigen Köderseiten und technischem Support. Fertige Phishing-Seiten werden bekannten Webseiten wie Google, Microsoft, Linkedin, iCloud. Gängig sind Phisching-Proxi-Services, die als Man-in-the-Middle (MITM) zwischen Opfer und der Login-Seite eines Unternehmens tätig sind. In der Regel können sie Zugangsdaten und Cookies stehlen und somit auch Multifaktor-Authentifizierungen umgehen. Bekannt ist Evil-Proxy für seine

[131] BSI, Die Lage der IT- Sicherheit in Deutschland 2023, S. 35, 54.

Phishing-Login-Seiten für Google, Microsoft und für Python Package Index, das offizielle Softwareverzeichnis für die Programmiersprache Python, die von über 11 Millionen Entwicklern weltweit genutzt wird. Eine Kompromittierung dieser Seiten könnte zu Supply-Chain-Angriffen durch bösartige geklonte Code-Repositories führen und im Ergebnis zum Diebstahl von Zugangsdaten führen.
Phishing bleibt ein hohes Cyberrisiko und erfordert entsprechend hohe Anstrengung zur Risikoabwehr. [132]

32.3 Das MFA Verfahren als Nachweis der Identität mit mehreren Komponenten

Ein Passwort allein genügt nicht gegen Hackerangriffe. Die Sicherheit eines Passworts hängt von seiner Komplexität ab, damit es nicht erraten werden kann. Auch noch so komplexe Passwörter schützen nicht vor Phishing Angriffen[133] oder Keyloggern.[134]

Angemessene Sicherheitsmaßnahmen sind nur zu entwickeln, wenn vorher das Risiko ermittelt ist, das abzuwenden und vor dem zu sichern ist. Die Bedrohungslage ist zu analysieren, was als Threat Modeling[135] benannt wird.[136] Über ein zu einfaches Passwort können sich Hacker Zugriff verschaffen und mit dem gleichen Passwort auf verschiedenen Systemen des gleichen Berechtigten verschiedene Konten kompromittieren.
Angefangen hat das MFA Verfahren mit der Zwei-Faktor-Authentifizierung -2FA- durch TANs – Transaktionsnummern – zur Absicherung des Online-Bankings. Zum Passwort mussten sie bei finanziellen Transaktionen zusätzlich eine eindeutige TAN eingeben, die sie einer gedruckten Liste entnahmen. Ohne TAN war keine Geldbewegung zu veranlassen. Die Weiterentwicklung bestand darin, dass weitere Komponenten angegeben werden mussten, um die Sicherheit zu erhöhen nämlich

- Ein Geheimnis, das nur der Benutzer kennen sollte, wie ein Passwort, ein PIN oder die Antwort auf Sicherheitsfragen;

---

[132] BSI, Die Lage der IT- Sicherheit in Deutschland 2023, S. 54.

[133] **Phishing** gilt als Diebstahl von persönlichen Daten, Anmeldinformationen und Passwörtern mit Hilfe von gefälschten E-Mails oder Websites.

[134] **Keylogger** sind Programme oder Geräte, die Tastatureingaben mitprotokollieren. Gefahr geht von solchen Keyloggern aus, die speziell Anmeldedaten wie Namen und Passwörter auslesen und unbefugt an Dritte übermitteln. Das ist eine Bedrohung der Datensicherheit Ihrer E-Mail-Passwörter, Social-Media-Konten oder Onlinebanking-Daten. Solche Keylogger werden nicht nur von einzelnen Hackern, sondern ebenso auch von Ermittlungsbehörden und Nachrichtendiensten genutzt, um vertrauliche Daten auszuspionieren. Der Begriff Keylogger wird häufig synonym mit Spyware verwendet. Spyware ist aber der übergeordnete Begriff für Schad-Software, die gezielt Informationen des Nutzers ausschnüffelt. Der Begriff „Keylogger“ ist enger gefasst, da diese lediglich die Tastatureingaben ermitteln.

[135] **Thread Modeling** ist die Bedrohungsanalyse gegen IT-System, um Cyberrisiken zu verringern.

[136] Rodewig, MFA für Unternehmensanwendungen, iX 5/2024 S. 48.

- Einen physischen Gegenstand, den der Benutzer bei sich trägt, wie ein Mobiltelefon, oder eine Smartcard;
- Ein biometrisches Merkmal wie einen Fingerabdruck oder ein Irisscan oder die Gesichtserkennung.

Nur mehrere Faktoren zu Authentifizierung schützen den Benutzer vor unberechtigten Zugriffen.

Unberechtigte Zugriffe können in verschiedenen Varianten drohen.

- **Passwortdiebstahl** ist das häufigste Angriffsverfahren durch Ausspähen oder Erraten von zu einfachen Passwörtern.
- **Phishingangriffe** ***v***ersuchen, Benutzer zur Preisgabe ihrer Anmeldeinformationen auf gefälschten Websites zu bewegen.
- **Social Engineering** ist die Methode, Zugang zu Konten zu erlangen, indem sich Angreifer als legitime Benutzer ausgeben, um den Kundensupport zu überlisten.
- Mit **Brute-Force-Angriffen** versuchen Angreifer durch verschiedene Kombinationen Passwörter zu erraten.
- Mit **Man-in-the-Middle-Angriffe** versuchen Angreifer die Kommunikation zwischen Benutzer und Server abzufangen und zu manipulieren.
- Mit dem **Kontodiebstahl** versuchen Angreifer physischen Zugriff auf Geräte zu erlangen, um Anmeldeinformationen zu erlangen.

Zum Stand der Technik gehören neben den TAN Listen weitere Methoden, auf die Geschäftsleiter zur Erfüllung ihrer Pflichten zur Cybersicherheit zurückgreifen können, um Cybersicherheit für ihre Unternehmenssoftware zu gewährleisten.

- Mit der **SMS-basierten 2FA** Methode wird den Nutzern ein einmaliger Code per SMS mitgeteilt, den sie mit dem Passwort eingeben müssen.
- Mit der **Authentifizierungs-App** wie z.B. Google Authenticator oder Microsoft Authenticator werden regelmäßig neue Codes erstellt, die als zweiter Faktor eingegeben werden können. Ihr Vorteil ist die Unabhängigkeit von Telefonnetzwerksicherheitslücken.
- Mit **Hardwaretoken** können Unternehmen physiche Token an Kunden ausgeben, die einen Code erstellen, der als zweiter Faktor genutzt werden kann.
- Mit **Pushbenachrichtigungen** kann ein Service wie Cisco Duo Pushnachrichten auf Smartphones senden, die Nutzer akzeptieren können und um sich damit zu authentifizieren.
- Biometrische 2FA Methoden verwenden biometrische Daten wie Fingerabdrücke oder Gesichtserkennung als zweiten Authentifizierungsfaktor. Sensoren machen dieses Verfahren möglich.
- Mit der E-Mail-basierten 2FA Methode werden einmalige Codes oder Links an die E-Mail-Adresse des Nutzers gesendet, wobei die Sicherheitslücke in einem kompromittierten E-Mail-Konto bestehen kann.
- Mit der Voice-basierten 2FA Methode erhalten Nutzer einen Anruf und müssen einen Code eingeben oder den Anruf bestätigen. Schlechte Internetverbindungen schränken den Nutzen ein.

Die Wahl einer Methode hängt von dem Sicherheitsniveau, den Kosten oder der

Zielgruppe ab. Empfohlen wird die Aufklärung über die Sicherungsfunktion. Softwaretoken, Pushnachrichten, E-Mail-Codes gelten als komfortable 2FA Codes. Bei Pushnachrichten muss eine App auf dem Smartphone installiert sein. Hardwaretoken müssen immer griffbereit sein und es gibt kein Backup. Im App-Bereich gelten Pushnachrichten als aktueller Stand der Technik.[137]

Für die technische Umsetzung wird die Einschaltung spezialisierter Dienste empfohlen, wie zum Beispiel Amazon Web Services (AWS), mit dem eine Vielzahl von Funktionen möglich sind, wie z.B. Benutzer- und Authentifizierungsmerkmale hinzufügen, das Speichern und Synchronisieren von Benutzerdaten über Geräte hinweg, Offlinezugriffe, das Speichern verschlüsselter Informationen, das Einsetzen verschiedener Authentifizierungsmethoden, MFA ist eine einfache Konfigurationsoption für einen Benutzerpool und kann als für alle Poolnutzer für erforderlich oder optional gewählt werden. Multi-Faktor-Authentifizierung gilt als uneingeschränkt zeitgemäß.[138]

32.4 Die „kontinuierliche“ risikoangepasste Authentifizierung

In § 30 Abs. 2 Nr. 10 BSIG werden Geschäftsleiter zur kontinuierlichen Authentifizierung verpflichtet. Kontinuierliche Authentifizierung erfordert die laufenden und möglicherweise sich verändernde Risiko- und Bedrohungslage. Deshalb wird als erforderlich verlangt, Kontexte und laufend aufgenommene Signale als Multi-Faktoren zu berücksichtigen. Im Finanzsektor wird zum Schutz von Transaktionen diese Risikoanalyse praktiziert. Dabei sind statische Authentifizierungsverfahren unter Verwendung von Benutzernamen und Kennwort auch variirende Faktoren zu berücksichtigen, so zum Beispiel wenn das Signal eingeht, dass der Nutzer den üblichen Standort oder auffällig die üblichen Zugriffszeiten gewechselt hat.

Unter der adaptiven Authentifizierung wird das Erkennen und Bewerten von Risiken für dem jeweiligen Zugriff verstanden. Diese Risikoanalyse hat sich bei Banken durchgesetzt, weil man so Betrug bei jeder individuellen Transaktion zu vermeiden bestrebt war. Auf unterschiedliche Risiken war auch mit unterschiedlichen Abwendungsmaßnahmen zu reagieren. Benannt werden unterschiedliche Standards, NiST SP 800-63-3, IAL (Identity Assurance Level), AAL (Authenticator Assurance Level), FAL (Federation Assurance Level). Die adaptive Authentifizierung verursacht mehr

[137] Rodewig, MFA für Unternehmensanwendungen, iX 5/2024 S. 52.

[138] Rodewig, MFA für Unternehmensanwendungen, iX 5/2024 S. 54 und 59.; Kuppinger, Mehr Sicherheit durch risiko- und kontextbasierte MFA iX 5/2024 S.54.

Kosten und Aufwand, weshalb sie nicht flächendeckend eingesetzt werden. [139]
Je höher Anspruch nach Sicherheit umso höher steigen die Kosten. Der Grenzwert der Kosten für IT-Sicherheit steigt gegen unendlich, wenn 100 Prozent angestrebt werden, was unmöglich erscheint. Mit technischen Maßnahmen lassen sich kriminelle Verhaltensweisen wie Betrug oder Bestechung nicht erfassen.[140]
Die risikobasierte adaptive MFA wird zum Standard. Die DIN ISO 27001:2022 definiert in A.8.16 unter Monitoring Activities, mit denen anomales Verhalten erkannt werden soll, das individuell zu bewerten ist. Auch die gesetzliche Regelung in § 30 Abs.2 Nr.10 BSIG neu verpflichtet zu kontinuierlichem Authentifizieren, was bedeutet, dass wechselnde Risiken angepasst zu bewerten und zu analysieren sind. Cyberangriffe werden nicht standardisiert ausgeführt, sondern wechseln je nach Schwachstellen und deren Ausnutzbarkeit. Authentifizierungsverfahren sind auf das Erkennen anomaler Signale eingestellt. Analysiert werden können das individuelle Verhalten potentieller Angreifer, die von befugten Nutzern durch sich unterscheiden lassen und durch sogar das Wisch- und Tippverhalten auf dem benutzten Gerät.[141]
Softwareprodukte wie XDR erkennen Sicherheitsrisiken und können sogar darauf reagieren. Je nach Kontext und Risiko können Authentifizierungsmechanismen variieren.[142]

32.5 Die Nutzung von Passkeys

Passkeys sind eine Fortentwicklung und sicherere und benutzerfreundlichere Alternative zu herkömmlichen Passwörtern. Passkeys sollen nicht nur die Sicherheit eines Anmeldvorgangs steigern, sondern das Eingeben eines Passwortes überflüssig machen. Die Verwendung von **Kryptographie** macht dies möglich. **Kryptographie** ist ursprünglich die Wissenschaft der Verschlüsselung von Informationen. Heute befasst sie sich auch allgemein mit dem Thema Informationssicherheit, also der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind.
Mit einem Kryptosystem werden Daten und Texte gegenüber Dritten geheimgehalten.
Vier Ziele lassen sich mit Kryptographie zum Schutz von Daten, Nachrichten verfolgen.

- Erstens dient Kryptographie der Vertraulichkeit und dem Zugriffsschutz, damit nur befugte Personen Daten und Nachrichten lesen und informiert werden können.
- Zweitens dient Kryptographie der Integrität und dem Änderungsschutz, damit Daten unverändert und nachweisbar vollständig bleiben.
- Drittens wird Authentizität und Fälschungschutz gesichert, damit die Urheber der Daten oder ein Absender einer Nachricht unzweifelhaft identifi-

[139] Kuppinger, Mehr Sicherheit durch risiko- und kontextbasierte MFA iX 5/2024 S.55.

[140] Kuppinger, Mehr Sicherheit durch risiko- und kontextbasierte MFA iX 5/2024 S.56 mit anschaulicher Graphik.

[141] Kuppinger, Mehr Sicherheit durch risiko- und kontextbasierte MFA iX 5/2024 S.59.

[142] Kuppinger, Mehr Sicherheit durch risiko- und kontextbasierte MFA iX 5/2024 S.60.

zierbar bleibt und seine Urheberschaft nachprüfbar ist.

- Viertens sichert Kryptographie die Verbindlichkeit von Daten und Nachrichten, die der Urheber nicht mehr bestreiben kann und gegenüber Dritten nachgewiesen werden kann. [143]

Zwei Kryptoverfahren lassen sich unterscheiden,

Symmetrische Verfahren verwenden einen Schlüssel für eine Kommunikationsbeziehung für alle Verfahren, und zwar für das Verschlüsseln und das Entschlüsseln. Der Schlüsseltausch war das Problem. Über einen sicheren Weg mussten die Kommunikationspartner den gemeinsamen Schlüssel tauschen, was unüberschaubar werden konnte, wenn eine Vielzahl von Personen beteiligt waren. Diese Verfahren wird auch als Geheimschlüssel-Verfahren oder Geteiltschlüssel-Verfahren benannt.

Asymmetrisch Kryptoverfahren verwenden für jeden Teilnehmer ein Schlüsselpaar, den öffentlichen Schlüssel zum Verschlüsseln von Daten und den anderen privaten Schlüssel zur Entschlüsselung der geheimen Daten, der vom Schlüsselinhaber geheimgehalten werden muss. Der Besitz des öffentlichen Schlüssels berührt die Sicherheit des privaten nicht. Das Public-Key-Verfahren wird auch zur Authentifizierung genutzt. Mit dem privaten Schlüssel kann sein Besitzer Daten entschlüsseln, die mit dem öffentlichen verschlüsselt wurden und er kann sich vor allem sich authentifizieren.[144]

FAZIT

Besonders Geschäftsleitern und ganz speziell den Geschäftsleitern kritischer Anlagen, wie allen Versorgern von Energie, Wasser und sonstigen Leistungen der Daseinsvorsorge, ist zu empfehlen, sich mit der neuen Rechtslage zur Abwendung von Cyber- und IT-Risiken durch die hochaktuellen Referentenentwürfe zum BSIG mit dem neuen BSI-Gesetz- sowie dem KRITIS-DachG vertraut zu machen. Der Anwendungsbereich der kritischen Infrastruktur ist auf etwa 30 000 Unternehmen ausgeweitet. Den Geschäftsleitern ist die Verantwortung und die persönliche Haftung erstmalig und neu gesetzlich ausdrücklich übertragen worden, die sie nicht delegieren oder abbedingen können. Die fehlende IT-Kompetenz müssen sie sich durch Schulungen aneignen und nachweisen. Geschäftsleiter müssen sich in die Lage versetzen, zur Vermeidung von Cyberattacken zumindest die richtigen Fragen an ihre IT-Berater zu stellen, um Schwachstellen an der im Unternehmen eingesetzten Software prüfen zu können.

Dazu gehört es, SBOMs mit Benennung der Einzelkomponenten abzufragen.

Das Schwachstellen Management ist wegen einer täglich neuen Risikolage eine erhebliche Herausforderung für die Organisation eines Unternehmens kritischer Infrastruktur. Monatlich werden aktuell 2.500 neue Schwachstellen

[143] Ertel, Wolfgang, Angewandte Kryptographie, 2.Aufl. S……

[144] Pohlmann, Norbert, Cybersicherheit, Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cybersicherheitssystemen in der Digitalisierung, S…….

erfasst. Schließlich drohen existentielle Schäden durch die unberechenbaren Angriffe mit Vorfällen und nicht kalkulierbaren Schadensfolgen. Das Compliance-Management-System RECHT IM BETRIEB bietet die Einhaltung aller sechs Organisationspflichten und vor allem die Nachweismöglichkeiten. Geschäftsleiter vermeiden damit präventiv den eventuellen Vorwurf des Verschuldens bei der Organisation der Rechtspflichten zum Schutz vor IT- und Cyberrisiken, sollte es nämlich trotz aller Compliance Bemühungen zu einem Rechtsverstoß kommen.

Literaturverzeichnis

Allianz Risk Barometer 2023;

Anhang I Sektoren mit hoher Kritikalität zur Richtlinie EU 2022/2555 des Europäischen Parlaments und des Rates – Stand: 14.12.2022

Begründung Referentenentwurf des Bundesministeriums des Innern und für Heimat, Stand 7.5.2024, Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

BGH vom 17.10.1967, NJW 1968,247 – Schubstreben Urteil.

BGH, 26.11.1989 – VI ZR 212/66; BGHZ 51, 91 – Hühnerpestentscheidung.

BGH, 2.2.1996 – V ZR 239/94, BGHZ 132,30, BB 1996, 924, IKB Urteil.

BGHZ 92, 143 vom 18.9.1984 Kupolofen Urteil

BGHZ 132,30,36, BB 1996, 924 Wissensaufspaltungs-Urteil;

BGH, 20.9.2011 – II ZR 234/09 (OLG Hamburg), NJW – RR 2011, 1670 (ISION Urteil)

Biermann, Kai, Bug Bounty, Kopfgeldjagd im Internet, in Zeit online, 3.Sept.2013.

Braun Gunnar, Wie viel Standard steckt in SBOMs, in iX 9/2023

Deutscher Anwaltsspiegel, CyberSecurity ist C-Level Aufgabe, Verschärfte Haftung für Leitungsorgane in Unternehmen: Kommt der Cybervorstand, 24. Mai 2023, von Dr. Kristina Schreiber und Dr. Eren Basar.

FAZ vom 11.05.2024, Im digitalen Dauerfeuer

FAZ vom 14.05.2024, Die Bedrohung durch Cyberangriffe wächst.

FAZ vom 31.05.2024, Kriminellen die Grundlage entziehen im Lokalteil S.1.

FAZ vom 28.Mai,2024, Cyberangriffe nehmen zu.

Frank und Casper, iX 12/2023, Schwachstellenmanagement: mehr als Scannen und Finden, mit aufschlussreicher Abbildung 2 zum Stand von 19.10.2023.

KPMG Lünendonk-Studie 2023, Von Cyber Security zu Cyber Resilience, Wie Unternehmen auf die steigende Bedrohungslage realgieren;

Haar, Tobias, iX 2/2022 Neues Vertragsrecht zu digitalen Produkten, Zum Schutze der Kunden, Seite 99

Heise Security, „Deutlicher Anstieg der SQL-Injection-Angriffe, und Giftspritze“ aus

Jonas/Stroebe/Hewstone, Sozialpsychologie, 5.Aufl., S. 302

Miller, Charles, The Legitimate Vulnerability Market: The Secret World of 0-day Exploit Sales; Patrick Beuth, Der perfekte iPhone-Hack kostet zwei Millionen Dollar.

Offenlegung oder Enthüllung

Plate, NIS2 – und jetzt?, in iX 2024

Plogsties, iX 3/2024, Was die SBOM für die Cloud bedeutet

Pressemitteilung Bitkom, Wirtschaftsschutz 2023, vom 1.9.2023

Rack, Compliance Berater, 5/2013, Die Organisationspflicht nach der höchstrichterlichen Rechtsprechung mit Einzelnachweisen zur Risikoanalyse;

Rack, Compliance Berater, 6/2013, Die Organisationspflicht zur Delegation;

Rack, Compliance Berater 7/2013, Die Aktualisierung von Unternehmenspflichten

Rack, Compliance Berater 8/2014, Die rechtlichen Voraussetzungen eines Compliance-Management-Systems, mit Einzelnachweisen aus Urteilen zu jeder Organisationspflicht.

Rack, Compliance Berater 6/2017 S. 206 Das Rechtsrisiko des Dunning-Kruger-Effekts - eine psychologische Erklärung für Rechtsverstöße wegen unterlassener präventiver Rechtsprüfung.

Rack, Compliance Berater, 2/2013, Informationsmanagement als Organisationspflicht, mit weiteren Nachweisen aus der BGH-Rspr.

Redeker, IT-Recht, Rn.343; Schimmer DuD 2006,616; Paulus/Tegge DuD 2006,623; Klett/Gehrmann, MMR 2022,435 auch unter Berücksichtigung des Mängelbegriffs

Referentenentwurf zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, Stand 7.5.2024, Seite 155 zu § 38 Abs.1 BSIG.

Referentenentwurf zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, Stand 7.5.2024, Seite 147 zu § 30 Abs.1 BSIG

Referentenentwurf zur Umsetzung der NIS-2-Richtlinie zu § 30 Abs.2 BSIG, Seite 148 Bearbeitungsstand 7.5.2024.

Referentenentwurf vom 21.12.2023

Referentenentwurf vom 21.12.2023, S. 1 und 2 unter Problem und Ziel

RG, 14.12.1911 – VI 75/11, RGZ 78, 107 (Kutscher-Urteil);

RG, 12.1.1938 – VI172/37, RGJW 1938, 1651 (Kleinbahn-Urteil);

RG, 25.2.1915 – VI 526/14,

RGZ 87 (1916), 1 (Heilsalz-Urteil);

BGH, 25.10.1951 – III ZR 95/50, BGHZ 4,1 (Benzinfahrt-Urteil);

BGH, 9.2.1960 – VIII ZR 51/59, BGHZ 32 (1960), 53(Besitzdiener-Urteil).

Sachs, Michael, in: Sachs, Grundgesetz Kommentar, 8. Auflage 2018, Art. 20, Rn. 47 ff. Karl-Peter, in: von Mangoldt/Klein/Starck, Kommentar zum Grundgesetz, Band II, 7. Auflage 2018, Art. 20 Rn. 103

Schneider, Udo, iX10/2022. SOFTWARE BILLS OF MATERIALS, SBOMs – Stücklisten für Software

Standard 200-2 zur IT Grundschutz-Methodik

Tagesschau vom 8.9.2023

VMWARE White Paper: DIE WICHTIGSTEN GRUNDSÄTZE DER CYBER-HYGIENE RUND UM CLOUD UND MOBILITÄT,

Weidenhammer, in: All About Security, Angriff auf die Supply Chain-Solarwinds

Wikipedia zu Bug-Bounty-Programmen, mit weiteren Nachweisen zu unterschiedlichen Programmen, u.a. Microsoft, Online Services Bug Bounty Terms.

Wintergerst, Bitkom-Präsident, Wirtschaftsschutz 2023, mit detaillierter Darstellung der Risikolage

Pflichtenprofil

Gesetz über das Bundesamt für Sicherheit in der Informations-technik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)

§ 7 Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte

Dem Bundesamt ist in den Zeiten, zu denen die Räume normalerweise für die jeweilige geschäftliche oder betriebliche Nutzung zur Verfügung stehen, zu den Grundstücken und Betriebsräumen, einschließlich Datenverarbeitungsanlagen und -geräten, die für die Kommunikationstechnik des Bundes verwendet werden, Zugang zu gewähren.

§ 12 Bestandsdatenauskunft

Der auf Grund eines Auskunftsverlangens Verpflichtete hat die zur Auskunftserteilung erforderlichen Daten unverzüglich und vollständig zu übermitteln.

§ 14 Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen

Die Hersteller haben eine Auskunftspflicht betreffend auf dem Markt bereitgestellter oder zur Bereitstellung auf dem Markt vorgesehener informationstechnischer Produkte und Systeme zur Erfüllung der Aufgaben des Bundesamts.

§ 18 Anordnungen von Maßnahmen des Bundesamtes gegenüber Herstellern von IKT-Produkten

Soweit erforderlich, kann das Bundesamt von einem Hersteller betroffener IKT-Produkte die Mitwirkung an der Beseitigung oder Vermeidung erheblicher Sicherheitsvorfälle bei besonders wichtigen Einrichtungen und wichtigen Einrichtungen verlangen.

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten.

§ 31 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

Betreiber kritischer Anlagen sind verpflichtet, Systeme zur Angriffserkennung einzusetzen.

§ 32 Meldepflichten

Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet,

die aufgezählten Informationen an eine vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete gemeinsame Meldestelle zu melden.

§ 33 Registrierungspflicht

Besonders wichtige Einrichtungen und wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter sind verpflichtet, spätestens drei Monate, nachdem sie erstmals oder erneut als eine der vorgenannten Einrichtungen gelten oder Domain-Name- Registry-Dienste anbieten, dem Bundesamt über eine gemeinsam vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit bestimmte Angaben zu übermitteln.

§ 34 Besondere Registrierungspflicht für bestimmte Einrichtungsarten

Eine Einrichtung der in § 64 Absatz 1 Satz 1 genannten Einrichtungsart ist verpflichtet, bis zum 17. Januar 2025 dem Bundesamt die in § 34 Absatz 1 genannten Angaben zu übermitteln.

§ 35 Unterrichtungspflichten

Im Fall eines erheblichen Sicherheitsvorfalls kann das Bundesamt besonders wichtige Einrichtungen und wichtige Einrichtungen anweisen, die Empfänger ihrer Dienste unverzüglich über diesen erheblichen Sicherheitsvorfall zu unterrichten, der die Erbringung des jeweiligen Dienstes beeinträchtigen könnten.

§ 38 Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen.

§ 39 Nachweispflichten für Betreiber kritischer Anlagen

Betreiber kritischer Anlagen haben die Erfüllung der Anforderungen nach § 30 Absatz 1 und § 31 zu einem vom Bundesamt im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe festgelegten Zeitpunkt frühestens drei Jahre nachdem sie erstmals oder erneut als ein Betreiber einer kritischen Anlage gelten und anschließend alle drei Jahre dem Bundesamt auf geeignete Weise nachzuweisen.

§ 41 Untersagung des Einsatzes kritischer Komponenten

Ein Betreiber kritischer Anlagen hat den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Absatz 1 Nummer 22 dem Bundesministerium des Innern und für Heimat vor ihrem Einsatz anzuzeigen.

§ 43 Informations-sicherheitsmanagement

Die Einrichtungsleitung ist dafür verantwortlich, unter Berücksichtigung der Belange des IT-Betriebs die Voraussetzungen zur Gewährleistung der Informationssicherheit zu schaffen.

§ 51 Pflicht zum Führen einer Datenbank

Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domain Name Systems zu leisten, sind Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister verpflichtet, genaue und vollständige Domain-Namen-Registrierungsdaten in einer eigenen Datenbank im Einklang mit dem Datenschutzrecht in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt zu sammeln und zu pflegen.

§ 52 Verpflichtung zur Zugangsgewährung

Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister sind verpflichtet, einem berechtigten Zugangsnachfrager auf rechtmäßigen und hinreichend begründeten Antrag im Einklang mit dem Datenschutzrecht Zugang zu bestimmten Domain-Namen-Registrierungsdaten zu gewähren.

§ 53 Kooperationspflicht

Zur Vermeidung der doppelten Erhebung von Domain-Namen-Registrierungsdaten sind Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister insoweit zur Kooperation verpflichtet.

§ 55 Konformitätsbewertung und Konformitätserklärung

Der Aussteller hält die Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte, - Dienste, der Person oder der IT-Sicherheitsdienstleistung mit den festgelegten Kriterien während eines Zeitraums, der vom Bundesamt in der Technischen Richtlinie nach Absatz 1 festgelegt wurde, für das Bundesamt bereit.

§ 56 Nationale Behörde für die Cybersicherheitszertifizierung

Das IT-Sicherheitskennzeichen darf nur dann für ein Produkt verwendet werden, wenn das Bundesamt das IT-Sicherheitskennzeichen für dieses Produkt freigegeben hat. Hat das Bundesamt die Freigabe erteilt, ist das Etikett des IT-Sicherheitskennzeichens auf dem jeweiligen Produkt oder auf dessen Umverpackung anzubringen, sofern dies nach der Beschaffenheit des Produktes möglich ist.

Glossar

Air Gap

Bei einem **Air Gap** handelt es sich um eine „**physische Netzwerkisolierung**“. Es ist ein Prozess, bei dem Daten durch den Transport eines Speichermediums auf eine externe Festplatte oder ein Magnetband (LTO1-LTO8) aus dem Netzwerk heraus isoliert werden.

Authentifizierte Scans

Bei **authentifizierten Scans** bei denen authentifizierte Benutzer mit legitimen Anmeldedaten nach Schwachstellen suchen und eine Innensicht des Systems nutzen, werden mehr Schwachstellen erkannt und sich ein vollständiger Eindruck verschafft.

Container Image

Ein **Container Image** ist ein relativ isoliertes und unveränderliches Paket aus einer Software und den zur Laufzeit benötigten Werkzeugen und Dateien. Ein Image ist folglich für sich genommen lauffähig und äußerst robust

CVSS

CVSS (Common Vulnerability Scoring System): Dieses System bewertet Schwachstellen auf einer Skala von 0 bis 10. Ein höherer CVSS-Score bedeutet eine größere Bedrohung. Die Bewertung basiert auf Faktoren wie Ausnutzbarkeit, Auswirkungen und Komplexität.

Dependency Track

Ein **Dependency Track** ist ein Instrument, um Risiken in Softwarelieferketten zu identifizieren und zu reduzieren.

Dropper/ Viren-Dropper

Ein **Dropper** oder **Viren-Dropper** ist ein eigenständig ausführbares Computerprogramm, das zur Freisetzung eines Computervirus dient. Dropper werden meist für eine Erstinfektion von Cyberkriminellen verwendet.

Environmental Score

Der **Environmental Score** berücksichtigt den jeweiligen Schutzbedarf der betroffenen Systeme.

Flash- Speicher

Flash-Speicher ist eine Technologie, die hohe Performance und geringe Latenzen garantiert und die Leistung mechanischer Festplatten übertrifft.

Github

Github ist ein Onlinedienst zur Softwareentwicklung und Versionsverwaltung für Softwareprojekte auf Git-Basis. Das Unternehmen GitHub, Inc. hat seinen Sitz in San Fancisco und gehört zu Microsoft.

Immutable

Immutable gleich Unveränderlich bedeutet hier, dass Backup Dateien weder

verändert, noch gelöscht werden können. Das ist nur machbar mit Root-Rechten im Linux OS. So kann selbst ein Administrator, am Backup Server, im Repository Dateien weder verändern noch löschen.

Keylogger — **Keylogger** sind Programme oder Geräte, die Tastatureingaben mitprotokollieren. Gefahr geht von solchen Keyloggern aus, die speziell Anmeldedaten wie Namen und Passwörter auslesen und unbefugt an Dritte übermitteln. Das ist eine Bedrohung der Datensicherheit Ihrer E-Mail-Passwörter, Social-Media-Konten oder Onlinebanking-Daten. Solche Keylogger werden nicht nur von einzelnen Hackern, sondern ebenso auch von Ermittlungsbehörden und Nachrichtendiensten genutzt, um vertrauliche Daten auszuspionieren. Der Begriff Keylogger wird häufig synonym mit Spyware verwendet. Spyware ist aber der übergeordnete Begriff für Schad-Software, die gezielt Informationen des Nutzers ausschnüffelt. Der Begriff „Keylogger“ ist enger gefasst, da diese lediglich die Tastatureingaben ermitteln.

Kryptographie — **Kryptographie** bzw. Kryptografie, deutsch ‚verborgen‘, ‚geheim‘, ist ursprünglich die Wissenschaft der Verschlüsselung von Informationen. Heute befasst sie sich auch allgemein mit dem Thema Informationssicherheit, also der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen Manipulation und unbefugtes Lesen sind.

Logdatei — Eine **Logdatei** enthält das automatisch geführte Protokoll aller Aktionen von Prozessen auf einem Computersystem.

Lokale Exploits — Bei **Lokalen Exploits** werden Sicherheitslücken in den Programmen ausgenutzt, mit denen die Datei eingelesen wird.

Metrik (Softwaremetrik) — Eine **Softwaremetrik**, oder kurz **Metrik**, ist eine (meist mathematische) Funktion, die eine Eigenschaft von Software in einen Zahlenwert, auch **Maßzahl** genannt, abbildet. Hierdurch werden formale Vergleichs- und Bewertungsmöglichkeiten geschaffen.

Nicht authentifizierte Scans — Bei **nicht authentifizierten Scans** handelt es sich um Oberflächen-Scans, mit denen Hintertüren, nicht gepatchte Software und sonstige Sicherheitslücken gesucht werden können.

NIST — **NIST** ist das National Institute of Standards and Technology, eine nichtregulatorische Behörde, die Innovationen durch Förderung der Wissenschaft von Standards und Technologie fördert.

On-Premises	**On-Premises oder On-Prem** (*in den eigenen Räumlichkeiten*, *vor Ort* oder *lokal*) bezeichnet ein Nutzungs- und Lizenzmodell für Computerprogramme (Software). Bis ca. 2010 war die lokale Nutzung bzw. die Lizenzierung für die lokale Nutzung von Software der Normalfall und hatte daher keine besondere Bezeichnung. Erst seitdem die lokale Nutzung zunehmend von Software as a Service (SaaS) oder Cloud Computing verdrängt wird, ist der Begriff Off-Premises als Antonym entstanden.
OWASP	Die Open Web Application Security Project -**OWASP**- ist eine Non-Profit-Organisation mit dem Ziel, die Sicherheit von Anwendungen, Diensten und Software im Allgemeinen zu verbessern. Durch Schaffung von Transparenz sollen Endanwender und Organisationen fundierte Entscheidungen über wirkliche Sicherheitsrisiken in Software treffen können. Innerhalb dieser Gemeinschaft aus Firmen und sonstigen Einrichtungen aus aller Welt werden frei verfügbare Informationsmaterialien, Methoden, Werkzeuge und Technologien erarbeitet.
Passkeys	**Passkeys** sind eine Fortentwicklung und sicherere und benutzerfreundlichere Alternative zu herkömmlichen Passwörtern.
Patch	Ein **Patch** ist eine Nachbesserung oder Korrekturauslieferung für Software oder Daten aus Endanwendersicht, um Fehler zu beheben, bekannt gewordene Sicherheitslücken zu schließen sowie bislang nicht vorhandene Funktionen nachzurüsten.
Phishing	**Phishing** gilt als Diebstahl von persönlichen Daten, Anmeldinformationen und Passwörtern mit Hilfe von gefälschten E-Mails oder Websites.
Programmcode	Als **Programmcode** werden die Anweisungen bezeichnet, die im Rahmen der Softwareentwicklung für ein bestimmtes Computerprogramm oder einen Teil davon entstehen und die dessen Funktionalität in einer bestimmten Programmiersprache beschreiben bzw. repräsentieren.
Ransomware-Angriffe	Bei **Ransomware-Angriffen** werden Computer und andere Systeme blockiert und die Betreiber werden anschließend erpresst.
Remote Exploits	Bei **Remote Exploits** werden über Angriffe aus dem Internet mit Hilfe manipulierter Datenpaketen auf Schwachstellen in der Netzwerksoftware Sicherheitslücken ausgespäht.
Repository	Ein **Repository** ist ein verwaltetes Verzeichnis zur Speicherung und Beschreibung digitaler Objekte für ein digitales Archiv.

Responsible Disclosure	Bei einer **Responsible Disclosure** werden die betroffenen Unternehmen zuerst informiert und es wird ein Zeitfenster von üblicherweise 60 Tagen eingeräumt, um die Schwachstelle zu beheben.
Score	**Score** in Bezug auf Schwachstellen ist eine Bewertung oder ein Punktwert, der die Schwere oder das Risiko einer Sicherheitslücke quantifiziert. Es gibt verschiedene Score-Systeme, die von Sicherheitsexperten verwendet werden, um die Bedrohlichkeit von Schwachstellen zu bewerten.
SSD	Der Begriff **SSD** steht für "Solid-State-Drive" oder auch "Halbleiterlaufwerk". Es handelt sich dabei um ein elektronisches Speichermedium. Für SSD-Speicher werden Flash-basierte Speicherchips und SDRAMs verwendet. Aufgrund der sehr schnellen Zugriffszeiten, ihrem robusten Aufbau und ihrer Geräuschlosigkeit werden SSD-Festplatten gegenüber herkömmlichen Magnetenspeicher-Laufwerken bevorzugt.
SQL-Injection-Exploits	**SQL-Injection-Exploits** stellen eine Gefahr dar, weil sie bei Webanwendungen eingesetzt werden, die eine SQL-Datenbank nutzen, und über das Internet sehr leicht zugänglich sind oder auch grundsätzlich für jede Anwendung gefährlich sind, die auf eine SQL-Datenbank zugreifen.
Tag	**Tag** (Etikett, Mal, [Ab-]Zeichen, Auszeichner, Anhänger oder Schildchen) ist eine Auszeichnung eines Datenbestandes mit zusätzlichen Informationen.
Temporal Score	Der **Temporal Score** bezieht eine aktuelle Momentaufnahme der verfügbaren Exploits und der Schutzmaßnahmen, der Patchs sowie der Zuverlässigkeit der Berichte zu der Schwachstelle mit ein.
Thread Modeling	**Thread Modeling** ist die Bedrohungsanalyse gegen IT-System, um Cyberrisiken zu verringern.
WORM	**WORM** ist ein Akronym für „write once read many“ oder „write once read multiple“ (englisch für „schreibe einmal, lies vielfach“). Dies bezeichnet Vorkehrungen in der Informationstechnik, die das Löschen, Überschreiben und Ändern von Daten auf einem Speichermedium dauerhaft ausschließen, um vor Datenverlusten durch menschliche Fehler, Programmfehler und Schadsoftware zu schützen. Die dabei eingesetzten Datenspeicher können fortgesetzt bis zu ihrer Kapazitätsgrenze beschrieben und ansonsten nur gelesen werden.

Zero-Day-Exploits **Zero-Day-Exploits** werden eingesetzt, bevor es einen Patch, eine Lösung zur Schwachstelle, gibt und dadurch Entwickler keine Zeit zur Nachbesserung haben, der Hacker sie nicht dem Entwickler meldet, sie geheim hält und als offene Schwachstelle für längere Zeit ausnutzt.