WHITEPAPER

IT-Security auf dem **Stand der Technik** 2. Auflage

Wie sind Unternehmen, CISOs, Vorstände und Geschäftsführer in Zukunft sicher aufgestellt?

ESET 100% Made in EU IT-Security

ESET Digital Security
Progress. Protected.

↗ ESET.DE/STAND-DER-TECHNIK

Wenn Mark Twain in seinen Studien die deutsche Sprache als „verzwickt“ und „verwirrend“ beschreibt, hat er mit Sicherheit nicht mal einen einzigen juristischen Text gelesen. In diesem Fall wäre das Urteil womöglich noch verheerender ausgefallen.

Wir wissen, dass das sogenannte Juristenlatein oftmals schwere Kost ist, selbst häppchenweise serviert. Ausgerechnet bei diesem Thema führt allerdings kein Weg an Recht und Gesetz vorbei. Doch seien Sie unbesorgt, wir haben noch ein paar Kapitel im Ärmel, die keine Raketenwissenschaft sind. Bleiben Sie also am Ball – wie auch bei IT-Sicherheit selbst.

Wir wünschen viel Freude beim Stöbern.

Autor:
Michael Schröder / ESET Deutschland GmbH
Security-Awareness-Koordinator (TÜV) – Datenschutzbeauftragter (DSC)

Co-Autor:
Stefan Sander / SDS Rechtsanwälte Sander Schöning PartG mbB
Rechtsanwalt - Fachanwalt für IT-Recht - Software-Systemingenieur

März 2024, 2. Auflage

↗ ESET.DE/STAND-DER-TECHNIK

Einleitung

In der heutigen digitalen Welt ist IT-Sicherheit ein wichtiger Faktor für Organisationen jeder Größe und Branche. Besonders im Bereich der Kritischen Infrastruktur gibt es mittlerweile hohe Anforderungen an die Cybersicherheit, um einen störungsfreien Ablauf gewährleisten zu können. Die IT-Sicherheit als ausdrückliche gesetzliche Anforderung an Organisationen wurde insbesondere durch die **Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union** vom 14.12.2022 („NIS-2-Richtlinie“) auf europäischer Ebene erneut ausgeweitet. Die nationalen Rechtsvorschriften zur Umsetzung dieser Richtlinie müssen in allen Mitgliedstaaten der EU ab dem 18.10.2024 angewendet werden.

Neben den gesetzlichen Anforderungen gelangt zunehmend das Eigeninteresse aller Organisationen, nicht zum hilflosen Opfer von Cyberkriminellen zu werden, in den Fokus der öffentlichen Wahrnehmung und Berichterstattung von Massenmedien. Risikominimierung ist für alle Organisationen, unabhängig von deren Größe und etwaiger Einstufung als „kritisch“ für die Gesellschaft, das Gebot der Stunde. Zu oft wurden in letzter Zeit die Versäumnisse in der IT-Sicherheit sichtbar und zahlreiche Organisationen gerieten nach einem Cyberangriff in eine finanziell oder sogar existenziell bedrohliche Schieflage.

Die vielerorts vorhandenen Defizite in der IT-Sicherheit wiegen umso schwerer, als dass schon seit langer Zeit Organisationen ohne dahinterstehende, unbegrenzt haftende Gesellschafter (d.h. insbesondere Aktiengesellschaften und Gesellschaften mit beschränkter Haftung) eine Risikofrüherkennung und ein effektives Risikomanagement betreiben müssen. Dabei sind **angemessene Maßnahmen** zu treffen, um sich vor Cyberangriffen zu schützen. Der hierbei vielfach relevante **Stand der Technik** wird jedoch oft nur unzureichend beschrieben und erläutert. Dieses Whitepaper soll dazu beitragen, diese Lücke zu schließen.

Ungeachtet des Inhalts rechtlicher Pflichten sowie des Eigeninteresses an der Vermeidung und Verminderung von Risiken kommt es zunehmend in Mode, die danach verbleibenden Risiken aus dem Bereich der Informationssicherheit nicht länger selbst zu tragen, sondern sie zu übertragen. Somit ergeben sich automatisch Herausforderungen für Cyberversicherungen. Wie in allen Versicherungszweigen üblich, arbeiten auch solche Policen mit Obliegenheiten des Versicherungsnehmers. Und so kann es dann im Schadensfall vorkommen, dass der Versicherer feststellt, der geschädigte Versicherungsnehmer habe nur unzureichende Vorkehrungen und Maßnahmen getroffen und dass somit ein Teil oder der gesamte Schaden nicht vom Versicherer zu ersetzen ist.

Eine mögliche Lösung zur effektiven Risikominimierung sind **Zero Trust Security-Ansätze**, die auf einem mehrschichtigen, aufeinander aufbauenden Reifegradmodell basieren. Sie bringen die Bedürfnisse einer Vielzahl von Organisationen in eine klare Reihenfolge. Eine umfassende Sicherheitsstrategie beinhaltet in jedem Fall eine zusätzliche individuelle Bewertung sowie Absicherung möglicher Angriffsvektoren.

Um den heutigen Anforderungen an IT-Sicherheit gerecht zu werden, gibt es eine Vielzahl dedizierter technologischer Lösungen und Services, die von Experten bereitgestellt werden. Diese können Organisationen bei der Einhaltung des Stands der Technik maßgeblich unterstützen. Hier kann das Motto „Risikominimierung vs. Raketenwissenschaft“ durchaus auch in Anbetracht der wirtschaftlichen Aspekte zielführender sein als langfristige oder aufgeschobene Projekte.

Insgesamt ist es wichtig, dass Organisationen nicht nur die immense gesellschaftliche bzw. geopolitische Bedeutung und den Stellenwert von IT-Sicherheit im genannten Geltungsbereich, sondern ganz konkret den Mehrwert für sich selbst verstehen. Durch angemessene Maßnahmen und die Wahl einer passenden Strategie kann eine erfolgreiche Risikominimierung auch zeitnah erreicht werden.

Die Aufwendungen und Ressourcen hierfür werden von Verantwortlichen oftmals viel zu hoch eingeschätzt, hier soll unser Whitepaper für mehr Realismus sorgen.

Wir hoffen Sie erhalten beim Lesen einen informativen Einblick in das Thema.

Stefan Sander
Fachanwalt für IT-Recht und Software-Systemingenieur
SDS Rechtsanwälte Sander Schöning PartG mbB

Michael Schröder
Security-Awareness-Koordinator (TÜV)
Datenschutzbeauftragter (DSC)
ESET Deutschland GmbH

Inhaltsverzeichnis

1. "Stand der Technik"
Herkunft & Definition

Woher stammt diese Formulierung?

Ob auf europäischer Ebene oder im deutschsprachigen Raum – ein Großteil der relevanten Gesetze zur Informationssicherheit beinhalten die Formulierung „Stand der Technik". Doch was steckt konkret hinter diesem Begriff?

Verwendet der Gesetzgeber die Formulierung „Stand der Technik", so handelt es sich um einen sogenannten **unbestimmten Rechtsbegriff**. Die Verwendung von unbestimmten Rechtsbegriffen ist üblich und sinnvoll, weil sich damit das Gesetz auf eine abstrakte Regelung beschränkt, die für eine Vielzahl von Fällen Geltung beanspruchen kann. Insbesondere im Technikrecht ist dieser Vorteil von noch größerer Bedeutung, da das Gesetz nicht ständig überarbeitet und wieder ins Gesetzgebungsverfahren eingebracht werden muss, nur weil sich der Sachverhalt bzw. die Technik weiterentwickelt hat. Die abstrakte Regelung bleibt meist von der Veränderung der Lebenswirklichkeit unberührt und kann auch auf die neue Situation angewendet werden. Daraus ergibt sich die zwingende Schlussfolgerung, dass der konkrete Inhalt der Formulierung **Stand der Technik** veränderlich ist.

Abb. 1: Drei-Stufen-Theorie

Damit präzisiert sich die Frage dahingehend, wie der Stand der Technik im Einzelfall zu bestimmen ist. Dazu ist zunächst in den Blick zu nehmen, dass der Gesetzgeber daneben regelmäßig auch noch zwei andere unbestimmte Rechtsbegriffe verwendet (siehe Abbildung 1), nämlich die „allgemein anerkannten Regeln der Technik" (die geringere Anforderungen stellen) sowie den „Stand der Wissenschaft und Forschung" (der noch höhere Anforderungen stellt). Hieraus lässt sich Folgendes ableiten: Wenn das Gesetz (nur) auf die allgemein anerkannten Regeln der Technik verweist, dann können die Behörden und Gerichte sich darauf beschränken, die herrschende Auffassung unter den **technischen Praktikern** zu ermitteln, um festzustellen, ob die jeweilige Maßnahme den gesetzlichen Anforderungen genügt. Der Nachteil besteht darin, dass die Rechtsordnung mit diesem (Qualitäts-) Maßstab stets einer weiterstrebenden technischen Entwicklung hinterherhinkt. Dies wird vermieden, wenn das Gesetz auf den „Stand der Technik" abhebt.

Bezogen auf einen konkreten Einzelfall gestaltet sich hinsichtlich der Formel vom „Stand der Technik" die Feststellung und Beurteilung der maßgeblichen Tatsachen für Behörden und Gerichte schwieriger als beim Maßstab der allgemein anerkannten Regeln der Technik. Sie müssen zur Ermittlung des Standes der Technik in die Meinungsstreitigkeiten der Techniker eintreten, um zu ermitteln, was technisch notwendig, geeignet, angemessen und vermeidbar ist. Dabei können sie sich jedoch auf die herrschende Auffassung unter den **technischen Wissenschaftlern** stützen, ohne zwingend zu wissenschaftlichen Streitfragen Stellung nehmen zu müssen. Nicht erforderlich ist demgegenüber, dass sich die in Rede stehende Technik oder Maßnahme bereits über lange Zeit am Markt bzw. in der Praxis bewährt haben müsste.

Auf den Arbeitsalltag gemünzt bedeutet dies, dass zu einem unbestimmten Zeitraum konkrete notwendige technische Anforderungen in einer Organisation erfüllt sein müssen, ohne dass jedoch explizite Maßnahmen festgelegt wurden. Festgelegt ist hingegen das angestrebte Qualitätsniveau, welches sich bezogen auf eine konkrete technische Einrichtung typischerweise mit Zeitablauf verschlechtert, weil neuere (und bessere) Techniken auf den Markt treten.

Um die aufkommende Präsenz dieser Thematik zu verstehen, muss man zunächst die aktuell relevanten Gesetze betrachten, an die Organisationen und Unternehmen hinsichtlich IT-Security-Standards gebunden sind. Die hier aufgeführten Gesetze sind in diesem Kontext besonders relevant und daher ohne Anspruch auf Vollständigkeit, schon allein um den Umfang im Rahmen zu halten.

Was ist der „Stand der Technik"?

Die gesetzliche Anforderung „Stand der Technik" ist eine qualitative Anforderung und verschiebt den Maßstab des Gebotenen an die Front der technischen Entwicklung. Fordert das Gesetz die Einhaltung des Standes der Technik, muss fortlaufend neu investiert werden und jeweils die am Markt verfügbare IT-Sicherheitsmaßnahme beschafft und eingesetzt werden, die die Erreichung eines hohen Schutzniveaus für die IT-Sicherheit voraussichtlich als gesichert erscheinen lässt. [grundlegend dazu schon Bundesverfassungsgericht, Beschl. v. 8.8.1978 – 2 BvL 8/77]

1.1. Gesetzliche Rahmenbedingungen (EU / Deutschsprachiger Raum)

Woran muss ich mich halten?

Der zuletzt noch wichtigste Baustein war die europäische **Richtlinie (EU) 2016/1148 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union** („NIS-Richtlinie") vom 6.7.2016 – deren Aufhebung bereits beschlossen wurde (die Wirkung wird zeitgleich zum Inkrafttreten der neuen Regeln eintreten, Stichtag: 18.10.2024). Diese Richtlinie bzw. die Umsetzung in nationales Recht nahm hauptsächlich den Schutz Kritischer Infrastrukturen in den Blick. In Deutschland wurden dementsprechende Vorgaben in das Gesetz über das ↗ Bundesamt für Sicherheit in der Informationstechnik (kurz: BSI-Gesetz)[1] aufgenommen. In Österreich wurde 2018 zur Umsetzung der EU-Vorgaben das ↗ Netz- und Informationssystemsicherheitsgesetz (NISG)[2] geschaffen. Im Gegensatz dazu hatte die Schweiz keine Verpflichtung, das Schweizer Recht an die NIS-Richtlinie der Europäischen Union anzupassen. Das Thema als solches war jedoch auch dort schon zuvor bekannt: Die Schweiz hatte eine ↗ nationale Strategie zum Schutz vor Cyberrisiken (NCS)[3], welche in Folge der Gedanken, Beweggründe und Wertungen in der NIS-Richtlinie überarbeitet wurde.

Der deutsche Gesetzgeber hatte noch vor Verabschiedung der NIS-Richtlinie bereits mit dem sogenannten „IT-Sicherheitsgesetz" (2015), welches kein eigenes Stammgesetz wie z.B. das BGB, sondern nur ein Änderungsgesetz war, zahlreiche deutsche Gesetze im Hinblick auf das Thema verschärft – so auch das BSI-Gesetz. Zur Umsetzung der NIS-Richtlinie bedurfte es dann kaum noch weiterer Anpassungen. Eine weitere Verschärfung der Gesetzeslage brachte das auf den Namen ↗ „IT-Sicherheitsgesetz 2.0" getaufte Änderungsgesetz (2021)[4].

Mit Blick auf die Zukunft ist anzumerken, dass durch die ↗ NIS-2-Richtlinie[5] über die bislang regulierten **besonders wichtigen** Organisationen hinaus demnächst auch die **wichtigen** Organisationen (ab einer Größe von 50 Mitarbeitern) als Adressaten des Gesetzes in den Fokus geraten. Der Anwendungsbereich der gesetzlichen Pflichten steigert sich damit um eine enorme Anzahl von Organisationen.

Exkurs: DSGVO

Die Datenschutz-Grundverordnung (DSGVO) sorgte mit Inkrafttreten im Jahr 2018 wirtschaftlich und gesellschaftlich für große Aufregung, wenngleich sie viele Textpassagen der Datenschutz-Richtlinie aus dem Jahr 1995 übernahm bzw. fortführte. Die Verordnung ist jedoch – im Unterschied zur Richtlinie – in allen Mitgliedsstaaten der EU unmittelbar anwendbar und gibt vor, wie die personenbezogenen Daten durch private und öffentliche Verantwortliche verarbeitet werden dürfen bzw. was sie abseits dieser Frage sonst noch zu beachten haben. Der Wechsel von Richtlinie zu Verordnung brachte eine noch weitergehende Vereinheitlichung des Datenschutzes in der EU. Durch die in der DSGVO enthaltenen Bußgelddrohungen erlangte die Tatsache erstmals auch mediale Aufmerksamkeit, dass das Datenschutzrecht schon seit jeher sehr deutliche Forderungen an die Sicherheit der Verarbeitung von Daten stellt – und dies unabhängig von der Größe der Organisation, sodass auch alle KMU davon betroffen sind. Ein Beispiel für eine der Anforderungen:

Unter Berücksichtigung des Stands der Technik […] treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten […]

Quelle: ↗ Abschnitt 2, Artikel 32 EU-DSGVO: Sicherheit der Verarbeitung[6]

Wissen auffrischen? **Besuchen Sie unser Media Center auf eset.de/stand-der-technik**

Gesetzlicher Rahmen in Deutschland

Das BSI-Gesetz regelt – aktuell noch in Umsetzung der NIS-Richtlinie – Pflichten u.a. für die Betreiber von sogenannten Kritischen Infrastrukturen (KRITIS). Es definiert dabei diese als Einrichtungen, Anlagen oder Teile davon, die einerseits einem bestimmten Sektor* angehören und andererseits von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Dieses zweite Kriterium, die hohe Bedeutung einer Anlage, wird aktuell durch Schwellenwerte bzw. deren Übersteigen festgelegt, die in einer auf das BSI-Gesetz gestützten ↗ Rechtsverordnung des Bundesinnenministeriums (BMI) namens BSI-KritisV[7] enthalten sind. Weitere Adressaten des BSI-Gesetzes sind Anbieter bestimmter digitaler Dienste.

Zentraler Inhalt ist die Aufforderung, die Resilienz der Systeme im Hinblick auf die Cybersicherheit zu stärken. Konkret müssen die KRITIS-Betreiber die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse sicherstellen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. In diesem

* Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung

Zusammenhang entschied der Gesetzgeber, dass der Stand der Technik einzuhalten ist – und dies nicht nur bezogen auf einen bestimmten Zeitpunkt, etwa die Genehmigung oder die Inbetriebnahme einer solchen Anlage, sondern ohne weitere Angaben – mithin fortlaufend beim Betrieb der Anlage.

Schon mit der ersten Version des IT-Sicherheitsgesetzes (2015) stand allerdings fest, dass dieses auch **allgemein zur Verbesserung der IT-Sicherheit in Unternehmen und der Verwaltung herangezogen werden soll.** Erst Anfang 2021 reformierte der Gesetzgeber diese Grundlage zum IT-Sicherheitsgesetz 2.0 und stärkte damit auch die Rolle und Verantwortung des Bundesamts für Sicherheit in der Informationstechnik (BSI) merklich. Eine Ausweitung des Adressatenkreises erfolgte dabei jedoch nur in homöopathischer Dosierung, durch Hinzunahme des Begriffs der Unternehmen im besonderen öffentlichen Interesse.

Da sich die nationale Gesetzgebung im europäischen Wirtschaftsraum mittlerweile oft von den europäischen Anforderungen (d.h. Richtlinien der EU) ableitet, ist es eine Gewissheit, dass umfangreiche Änderungen an den aktuellen Regelungen des BSI-Gesetzes erfolgen werden. Ob das Änderungsgesetz zur Umsetzung der Vorgaben der NIS-2-Richtlinie in nationales Recht als „IT-Sicherheitsgesetz 3.0" übergehen wird, ist offen. Fest steht bereits, dass sich schon allein der Geltungsbereich der Vorgaben für KRITIS-Betreiber von derzeit acht auf dann 18 Sektoren ausweiten wird und – insoweit ändert sich die Rechtslage massiv – zukünftig nicht mehr erforderlich ist, dass eine Anlage aufgrund empirischer Erhebungen faktisch für die Versorgungssicherheit der Bevölkerung kritisch ist. Vielmehr wird zukünftig die Kritikalität allein daraus abgeleitet, dass ein Unternehmen in einem der genannten Sektoren tätig ist (und mindestens 50 Mitarbeiter beschäftigt).

Zu den heute bereits im BSI-Gesetz angelegten Pflichten gehören unter anderem die Überwachung aber auch die Meldung von Informationssicherheitsvorfällen sowie die Umsetzung von Maßnahmen zur Informationssicherheit, die dem Stand der Technik entsprechen. Der Nachweis über die Einhaltung der Sicherheitsanforderungen kann dabei vom Betreiber durch national oder international anerkannte Standards wie z.B. ISO 27001, den BSI-Grundschutz oder weitere in der Praxis erprobte Vorbilder erfolgen.

Exkurs: Die Rolle des BSI

Das BSI ist als zentrale Cybersicherheitsbehörde in Deutschland zuständig für die Durchsetzung und Überwachung der auf die IT-Sicherheit bezogenen Pflichten aus dem BSI-Gesetz sowie anderen Gesetzen, Verordnungen und Richtlinien. Es arbeitet eng mit den Betreibern Kritischer Infrastrukturen zusammen und dient sowohl als Kompetenzzentrum, Beratungsstelle aber auch als nationale Behörde für Cybersicherheitszertifizierungen (National Cybersecurity Certification Authority – kurz: NCCA) im Sinne der Verordnung (EU) 2019/881 (auch bekannt als „EU Cybersecurity Act").

Die Gesetzeslage in Österreich und der Schweiz

Die Pendants zum deutschen BSI-Gesetz sind das ↗ NISG (Netz- und Informationssystemsicherheitsgesetz, ausführlich dazu der Bericht des Rechnungshofes: Koordination der Cyber-Sicherheit)[8] aus Österreich sowie das ↗ ISG (Informationssicherheitsgesetz)[9] in der Schweiz, die ebenso die NIS-Richtlinie in nationales Recht umsetzen. Im Vergleich zum BSI-Gesetz unterscheidet sich der rechtliche Rahmen nur in Nuancen und wird daher im weiteren Verlauf dieses Whitepapers nicht differenziert betrachtet.

1.2. **Mindestniveau** für Stand der Technik

Woran orientiere ich mich?

Lautet eine gesetzliche Anforderung „nur", dass der Stand der Technik (neben anderen Kriterien) zu **beachten** ist, wird dies vom Gesetzgeber regelmäßig mit einem Ziel verknüpft (z.B. „um dem Risiko angemessene Maßnahmen entgegenzusetzen"). Hier beschreibt der Stand der Technik die qualitative Anforderung an die zu treffenden Maßnahmen.

Anders ist die Pflichtenlage, wenn der Gesetzgeber verlangt, dass der Stand der Technik beim Betrieb einer Anlage oder generell einer Organisation **eingehalten** wird. Dann beschreibt das qualitative Kriterium „Stand der Technik" das Mindestniveau für IT-Sicherheit. Wie sich schon aus der Definition des Begriffs ergibt, ist der jeweils aktuelle Stand der Technik gemeint, d.h. für die Organisation gilt es, ein sich bewegendes Ziel zu erreichen. Denn die Anforderung ist vom Gesetzgeber ja nicht auf einen bestimmten Zeitpunkt bezogen, etwa die Beantragung der Genehmigung für eine Anlage. Daraus folgt, dass allein durch Zeitablauf bzw. die unaufhaltsame, weiterstrebende **technische Entwicklung** im Prinzip alle einzelnen, konkreten Maßnahmen veralten. Sie fallen unter gegebenen Umständen aus der Zielvorgabe heraus, eben dann, wenn neue Maßnahmen bzw. Produkte auf dem Markt verfügbar werden, die ein (noch) höheres Maß an Qualität bzw. IT-Sicherheit versprechen. In diversen Fachartikeln und Publikationen wird die Phrase vom Stand der Technik beschrieben mit dem **aktuellen technischen und gegebenenfalls organisatorischen Standard für die Informationssicherheit**, den nicht nur Betreiber Kritischer Infrastrukturen erreichen und aufrechterhalten müssen, sondern auch angrenzende Dienstleister und Zulieferer (siehe „1.3. Erweiterung des Geltungsbereichs: Besonders wichtige und wichtige Einrichtungen" auf Seite 13) sicherzustellen haben. Die Einhaltung ist ebenfalls elementar für den Abschluss einer Cyberversicherung, hier meistens in Bezug auf die Obliegenheiten des Versicherungsnehmers.

Elementar für diese Betrachtung ist also, dass **Stand der Technik ein dynamischer Begriff** ist. Das heißt, der unter die Definition fallende Inhalt ändert sich im Laufe der Zeit, je nach den aktuellen Entwicklungen in der Informationssicherheit. Alle Verantwortlichen müssen daher regelmäßig ihre eingesetzten Methodiken und Technologien überprüfen und aktualisieren, um das Mindestniveau Stand der Technik aufrechtzuerhalten. Das genannte Mindestniveau dient als Basis für die Umsetzung der Anforderungen und soll per se die **Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit** von Informations- und Kommunikationssystemen gewährleisten.

Auch dann, wenn Verantwortliche nur **angemessene Maßnahmen** zur Informationssicherheit umsetzen müssen, läuft dies im Ergebnis häufig darauf hinaus, dass solche Maßnahmen ausgewählt werden, die dem Stand der Technik entsprechen. Denn die Beurteilung der Angemessenheit nimmt regelmäßig Bezug auf die aktuelle Bedrohungslage und Risiken, sodass die Maßnahmen allen jeweils aktuell gebräuchlichen Angriffsvektoren begegnen müssen. Veraltete Maßnahmen, die nur noch den allgemein anerkannten Regeln der Technik entsprechen, schaffen es meistens nicht, das von der Angemessenheit geforderte Niveau zu erreichen.

Letztlich lässt sich jedoch kaum ein gemeingültiges Bild oder eine pauschale Beschreibung aus den zur Verfügung stehenden gesetzlichen Rahmenbedingungen formulieren. Es ergibt daher durchaus mehr Sinn, sich an Modellen zu orientieren, die aus Expertensicht als anerkannt und praxisorientiert bezeichnet werden können.

Ein lobenswertes Beispiel findet sich in der ↗ Handreichung zum „Stand der Technik“[10] des Bundesverbands IT-Sicherheit e.V. (TeleTrusT). Es liegt in der Natur der Dinge, dass diese Handreichung ebenso fortlaufend aktualisiert werden muss, um der eigenen Überschrift gerecht werden zu können; eine Aufgabe, der sich der TeleTrusT-Verband fortlaufend verschrieben hat. Diese Handreichung listet neben organisatorischen Maßnahmen eine Vielzahl technologischer Ansätze und Lösungen auf, deren Wirkung und Nutzen detailliert beschrieben werden. Hinzu kommt, dass neben den üblichen Features anhand eines Graphen ebenfalls eine Einstufung bezüglich der Anerkennung und dessen Praxiserprobung mit Hinblick auf den Stand der Technik erfolgt (siehe Abbildung 2).

Welche Schutzziele werden durch die Maßnahmen abgedeckt?

- ☐ Verfügbarkeit
- ☑ Integrität
- ☑ Vertraulichkeit
- ☑ Authentizität

SdWF - Stand der Wissenschaft und Forschung
SdT - Stand der Technik
aaRT - allgemein anerkannten Regeln der Technik

Einordung der Maßnahmen

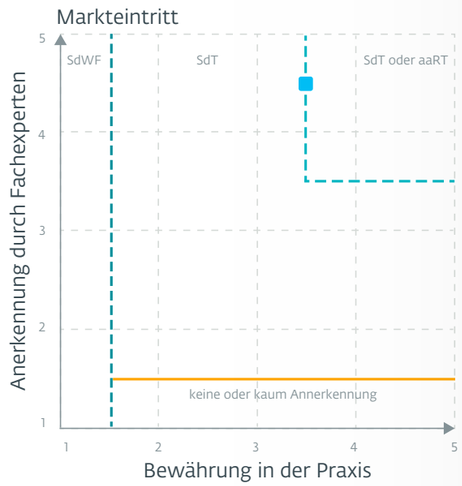

Abb. 2: Beispiel: Einordnung der Maßnahme Multi-Faktor-Authentifizierung

1.3. Erweiterung des Geltungsbereichs: Besonders wichtige und wichtige Einrichtungen

Wer ist direkt betroffen?

Nicht alle vom TeleTrusT-Verband beschriebenen Lösungen und Maßnahmen können bzw. müssen pauschal in allen Bereichen genutzt werden. Aktuell ist eine Betrachtung insbesondere relevant für Organisationen und Unternehmen, die unter die nationalen Regelungen zur Umsetzung der NIS-Richtlinie fallen, mithin Anbieter von Online-Diensten und Betreiber Kritischer Infrastrukturen in der gesamten EU, die für den unterbrechungsfreien Fortbestand der (Wirtschafts-)Systeme und damit auch der öffentlichen Ordnung von hoher Bedeutung sind.

Diese begrenzte Bedeutung wird sich mit Inkrafttreten der nationalen Regelungen zur Umsetzung der NIS-2-Richtlinie (bis spätestens Oktober 2024) massiv verändern und auf 18 Sektoren aus zwei verschiedenen Einstufungen ausweiten. Hierdurch werden auch die bisher stark fragmentierten Schwellenwert-Tabellen durch einheitliche Regeln abgelöst, weil es nicht mehr darauf ankommen wird, dass eine Anlage faktisch (d.h. bei Überschreitung der Schwellenwerte) für die Versorgungssicherheit der Bevölkerung kritisch ist. Vielmehr wird zukünftig die Kritikalität allein daraus abgeleitet, dass ein Unternehmen in einem der genannten Sektoren tätig ist und mindestens 50 Mitarbeiter beschäftigt. Die Aufteilung auf **besonders wichtige und wichtige Einrichtungen** erlaubt dabei nicht nur die exakte Bestimmung der Regulierung ab einer gewissen Organisationsgröße. Es werden auch gleichzeitig die Rahmen für Sanktionen (in Form von Geldstrafen) bei Verstößen festgesetzt. Die Richtlinie fordert von den Mitgliedsstaaten, in ihren Gesetzen Höchststrafen von mindestens 7 Millionen EUR (oder sogar 1,4 % des weltweiten Umsatzes) für **wichtige Einrichtungen** und mindestens 10 Millionen EUR (oder 2 % des weltweiten Umsatzes) für **besonders wichtige Einrichtungen** festzulegen.

Vor allem der **Schwellenwert von 50 Mitarbeitern** für die Betriebsgröße von **mittleren Unternehmen**, die in den Anwendungsbereich der NIS-2-Richtlinie und damit zukünftig der entsprechenden Umsetzungsgesetze der Mitgliedsstaaten der EU fallen, dürfte nicht nur hierzulande im Mittelstand viele überraschen. Entscheidend ist der im Laufe der Jahre immer wieder überarbeitete ↗ Benutzerleitfaden zur Definition von KMU der Europäischen Kommission, Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU[11].

Danach zählen derzeit Organisationen mit mindestens 50 Beschäftigten und einem Jahresumsatz von über 10 Mio. EUR oder einer Bilanzsumme von über 10 Mio. EUR zur Kategorie der mittleren Unternehmen. Ab 250 Beschäftigten und einem Umsatz über 50 Mio. EUR oder einer Bilanzsumme von über 43 Mio. EUR qualifiziert man sich als großes Unternehmen und verlässt damit den Bereich der KMU (siehe Abbildung 3).

A Besonders wichtige Einrichtungen

Große Betreiber aus 11 Sektoren (Anhang I) und Sonderfälle

B Wichtige Einrichtungen

Große/Mittlere Betreiber aus allen 18 Sektoren und Sonderfälle, soweit nicht von besonders wichtigen Einrichtungen erfasst

Mittlere Unternehmen

- Mindestens 50 Beschäftigte
- Jahresumsatz/Jahresbilanz > 10 Mio. EUR

Große Unternehmen

- Mindestens 250 Beschäftigte
- Umsatz > 50 Mio. EUR
- Bilanz > 43 Mio. EUR

Unabhängig von Unternehmensgröße

Qualifizierende Faktoren, z.B.:

- Kritische Tätigkeit
- Auswirkung auf öffentliche Ordnung
- Systemrisiken
- Grenzüberschreitende Auswirkungen

Abb. 3: Schwellenwerte und Definitionen nach NIS-2-Richtlinie

Hinweis für Unternehmen unterhalb der Schwellenwerte

Neben den beschriebenen Kriterien ist die Tatsache wichtig, dass auch kleinere Organisationen, die unterhalb des Schwellenwertes von 50 Mitarbeitern bleiben, trotzdem betroffen sein können und reguliert werden. Qualifizierende Faktoren sind neben der Einstufung als kritische Tätigkeit die Auswirkungen auf die öffentliche Ordnung, Systemrisiken oder gar sogenannte grenzüberschreitende Auswirkungen (siehe Abbildung 4). So wäre es beispielsweise denkbar, dass auch ein kleiner Abwasserbetrieb mit lediglich zehn Beschäftigten und geringem Umsatz in den Kreis der regulierten Unternehmen fällt. Es bleibt abzuwarten, wie die jeweiligen Mitgliedsstaaten der EU die NIS-2-Richtlinie umsetzen werden, weil diesbezüglich durchaus Spielräume bestehen.

Sektoren nach Anhang I	Sektoren nach Anhang II
Energie	Post- und Kurierdienste
Verkehr und Transport	Abfallwirtschaft
Bankwesen	Produktion, Herstellung und Handel mit chemischen Stoffen
Finanzmärkte	Produktion, Verarbeitung und Handel von Lebensmitteln
Gesundheitswesen	Verarbeitendes Gewerbe/Herstellung von Waren
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschungseinrichtungen
Digitale Infrastruktur	
ICT* Service Management (Managed Service Provider - MSP)	
Öffentliche Verwaltung	
Weltraum	

Abb. 4: Sektorenübersicht nach NIS-2-Richtlinie

* Information and Communication Technology

Sektorenzugehörigkeit für Dienstleister und Zulieferer

Bereits nach aktueller Rechtslage unter dem BSI-Gesetz können Unternehmen, die Dienstleistungen oder Produkte an KRITIS-Betreiber oder Unternehmen von besonderem öffentlichen Interesse liefern, auch unmittelbar in den Geltungsbereich der Regulierungen fallen. Eine Vielzahl von Produkten und Services können dabei eine wichtige Rolle bei der Aufrechterhaltung und Integrität Kritischer Infrastrukturen spielen, insbesondere wenn ein Zulieferer wegen seiner Alleinstellungsmerkmale von wesentlicher Bedeutung für das Unternehmen in besonderem öffentlichen Interesse angesehen wird. Aktuelle Sicherheitsvorfälle aus der Kategorie **Supply Chain-Angriffe** (siehe Exkurs) bekräftigen diese Einschätzung mehr als deutlich.

In einigen Fällen kann die Regulierung erfordern, dass Dienstleister und Zulieferer die gleichen Mindeststandards für IT-Sicherheit einhalten müssen wie die Betreiber Kritischer Infrastrukturen selbst. Dabei zu berücksichtigt ist, dass die Anforderungen für Dienstleister und Zulieferer je nach Regulierung und Land variieren können. Es wird daher empfohlen, sich an die zuständigen Stellen zu wenden, um die genauen Anforderungen zu erfahren.

Exkurs: Was ist ein Supply Chain-Angriff?

Hierbei nutzen Kriminelle einen oder mehrere Zulieferer des eigentlich anvisierten Unternehmens als Einfallstor für den Cyberangriff. Daher wird auch häufig von einem Drittanbieterangriff gesprochen. Denn gemeint ist üblicherweise einer der vielen angebundenen Lieferanten aus dem eigenen Portfolio. Dabei ist es eher unerheblich, ob dieser Zulieferer wichtige Produktionsmaterialien, Services oder ganze Outsourcing-Strukturen liefert – er ist lediglich Mittel zum Zweck, um ins Netzwerk des Opfers zu gelangen.

Es ist allerdings äußerst schwierig vorherzusagen, welche konkreten Angriffsvektoren Kriminelle als Einfallstor nutzen. Ob Schwachstellen in der Software, Social Engineering bei Mitarbeitern oder die mögliche Übernahme ganzer vernetzter Systeme, die Bandbreite ist mittlerweile sehr groß. Leider finden sich in der Realität fast täglich bedeutende Cybersicherheitsvorfälle in der Presse wieder.

2. Im Blickpunkt: Cyberversicherung als Herausforderung für Unternehmen

Bin ich versicherbar?

Das Thema **Cyberversicherung** hat sich in den letzten Jahren insbesondere für Versicherungsnehmer drastisch verändert. Diese Versicherungsart entwickelte sich zum wachstumsstärksten Markt der gesamten Branche. Trotz steigender Nachfrage ist es für Organisationen heute deutlich schwieriger, eine Versicherung gegen das Risiko von Cyberangriffen abzuschließen, als dies beispielsweise vor 2018 der Fall war. Das liegt vor allem daran, dass inzwischen andere Maßstäbe bei der Einschätzung des Sicherheitsniveaus einer Organisation herangezogen werden. Die **NotPetya-Angriffe** (eine Gruppe von Erpressungstrojanern) im Jahr 2017 und die damit verbundenen Kosten in Milliardenhöhe haben viele Versicherer sensibilisiert, ihre Risikobewertungen zu überdenken und neu zu strukturieren. Aufgrund der stetig steigenden Schadensfälle durch erfolgreiche Cyberangriffe stehen auch bestehende Verträge auf dem Prüfstand und werden teilweise gekündigt.

Betreuung von Endkunden durch einen externen IT-Dienstleister

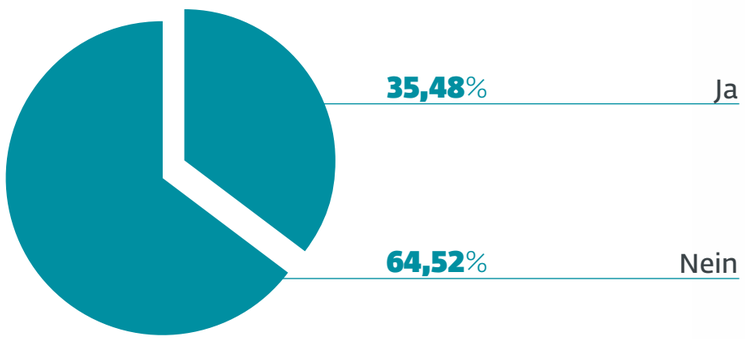

Abb. 5: Betreuung von Endkunden durch einen externen Dienstleister, ESET Umfrage zum Stand der IT-Sicherheit 2023

Eine Cyberversicherung sollte bei den meisten Organisationen ein fester Bestandteil der ganzheitlichen Risikomanagementstrategie sein. Damit möchten sich die Versicherten beispielsweise vor Störungen im Alltag, Datenverschlüsselungen durch Ransomware-Angriffe oder Haftpflichtschäden bei Datenschutzvorfällen absichern. Zudem soll das Risiko der damit verbundenen Kosten für die Wiederherstellung des (Geschäfts-)Betriebs, die Lohnfortzahlung oder den Gewinnausfall minimiert werden. Umso wichtiger ist es zu verstehen, wo die Probleme liegen und was die Gründe dafür sind, dass Organisationen unter bestimmten Umständen keine Versicherungspolice erhalten. Darüber hinaus sollte Verantwortlichen klar sein, dass mit Cyberversicherungspolicen nur ein Teil der Risiken abgedeckt werden kann. Ein (betreuter) Aufbau eigener Schutzmaßnahmen und (regelmäßiger) Investments in die Infrastruktur sind deshalb auch unabhängig von den Anforderungen der Versicherer unerlässlich.

Aus dem Spannungsfeld zwischen Cyberversicherungen und den Anforderungen an die Einhaltung des Standes der Technik ergibt sich die Frage, inwieweit ein Versicherungsnehmer seiner Verantwortung nachkommt, **angemessene Maßnahmen** zur Erhöhung der eigenen IT-Sicherheit zu ergreifen. Ein Versicherer wird einen Schaden nur dann ersetzen oder zuvor absichern, wenn die getroffenen Maßnahmen für die jeweilige Organisation als angemessen angesehen werden können und somit das Risiko von Sicherheitsvorfällen nachweislich minimiert wurde. Wird jedoch festgestellt, dass der Antragsteller unzureichende Vorkehrungen getroffen hat, muss die Organisation damit rechnen, dass die in der Policy vereinbarten Leistungen im Schadensfall verweigert oder erheblich reduziert werden. Versicherungsnehmer sollten daher unbedingt ihrer Verantwortung für den **Stand der Technik** nachkommen.

Exkurs: „Damoklesschwert“ Haftung

Dass sich Aufgaben delegieren lassen, die Haftung jedoch nicht, sollte schon seit Verabschiedung der DSGVO im Jahr 2018 und den damit verbundenen möglichen Bußgeldern hinlänglich bekannt sein. Doch auch im Kontext möglicher IT-Sicherheitsmängel und der IT-Compliance **besteht eine „Managerhaftung“**, die für Kapitalgesellschaften im § 43 GmbHG sowie § 76 Abs. 1 AktG und § 93 AktG verbrieft vorliegt. Sie ergibt sich aus dem vom Gesetzgeber – nicht zuletzt mit dem seit 2020 rechtsformübergreifend geltenden § 1 des Gesetzes über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen (StaRUG) – geforderten Risikomanagement. Geschäftsführer, Vorstände, Aufsichtsräte sowie Beiräte sind also gut beraten, den „Stand der Technik“ dauerhaft im Unternehmen sicherzustellen und Informationssicherheit als Ganzes, nicht nur als Kostenfaktor, zu verstehen.

3. Anforderungen
und angemessene Maßnahmen

Was muss ich tun?

Was aus heutiger Sicht als **angemessene organisatorische und technische Maßnahmen** bezeichnet werden kann, lässt sich nicht in allgemein gültiger Weise festlegen. Wie das Wort „angemessen" bereits andeutet, hat jede Organisation die konkrete Umsetzung individuell für sich festzulegen. So kann erst die Durchführung einer Risikoanalyse in einer Organisation Aufschluss über die Angemessenheit einer Maßnahme geben. Bei dieser Untersuchung werden Eintrittswahrscheinlichkeiten und wirtschaftliche Aspekte betrachtet und gegeneinander abgewogen. Auf jeden Fall hängen die zu treffenden Vorkehrungen von den spezifischen Anforderungen einer Organisation und den damit verbundenen Risiken für die IT- und Informationssicherheit ab.

Organisatorische Maßnahmen sind jedoch nur ein Teil der Umsetzung von IT-Sicherheitsanforderungen und können den Einsatz von technologisch ausgereiften Sicherheitslösungen nicht ersetzen. Sie tragen vielmehr dazu bei, dass die eingesetzten Produkte und Services optimal strukturiert und konfiguriert sind.

Einige Beispiele für angemessene organisatorische Maßnahmen:

- Die **Einführung eines Information Security Management System** (ISMS), worin auch ganz grundlegende Rollen und Verantwortlichkeiten festgelegt werden.
- Ein **belastbares IT-Notfallmanagement**, um Ausfallrisiken zu minimieren und Störungen schneller beheben zu können. Hierzu gehört u.a. die Minimierung von Datenverlusten mittels einer regelmäßig überprüften und entkoppelten Datensicherung.
- **Physische Sicherheitsaspekte**, die nur Berechtigten Zugänge und Zugriffe auf interne Perimeter und die eigene IT-Infrastruktur erlauben.
- Die **Schulung und Sensibilisierung der Mitarbeiter** zu Themen wie Informationssicherheit und Datenschutz.
- Eine **regelmäßige Überprüfung und Aktualisierung der IT-Sicherheitsrichtlinien und -verfahren**, um sicherzustellen, dass diese dem aktuellen Stand entsprechen.

4. Technische
Maßnahmen

Wie kann ich mich schützen?

Wie sollen Verantwortliche vorgehen, um die individuell passenden technischen Maßnahmen auswählen zu können? Die Handreichung vom TeleTrusT-Verband bietet einen umfassenden Überblick über die Technologien, die dem derzeitigen Stand der Technik entsprechen. Die Autoren lassen aber offen, welche Maßnahmen davon eine Organisation konkret ergreifen sollte. Ein Zero Trust Security-Konzept und die Beobachtung von Angriffsvektoren geben eine erste Orientierung. Eine darauf aufgebaute IT-Security-Strategie trägt dazu bei, dass Unternehmen und Organisationen den individuellen Schutzbedarf besser erkennen und sich adäquat absichern können. Dabei geht es nicht ausschließlich um die komplexen Herausforderungen bei der Einhaltung rechtlicher Rahmenbedingungen. Auch geopolitische Veränderungen und Ereignisse (Pandemie, Krieg) sowie deren direkte Auswirkungen bzw. Herausforderungen auf die Arbeitswelt (Stichwort: Homeoffice) spielen eine tragende Rolle. Nicht zuletzt verdeutlichen moderne Bedrohungen wie Advanced Persistant Threats (APTs), Zero Days, Ransomware oder Phishing, wie wichtig ein zuverlässiger Schutz der IT-Infrastruktur ist. Schließlich sollte Organisationen jeder Branche und Größe immer daran gelegen sein, mit sinnvollen technischen Maßnahmen ein angemessenes Schutzniveau zu erreichen.

Das Zero Trust Security-Modell von ESET (siehe Abbildung 6) bietet IT-Verantwortlichen ein modular aufgebautes Sicherheitskonzept zur Orientierung. Je nach Ausgangslage – beispielsweise die Anzahl und Art der eingesetzten Geräte, die genutzten Technologien oder das vorhandene Budget – werden verschiedene Schutzlevel beschrieben, in die sich Organisationen oder Verantwortliche einordnen können. Gleichzeitig ergibt sich hieraus der Bedarf an Sicherheitslösungen, die zur Erreichung des jeweiligen Schutzlevels notwendig sind. Aus diesem Grund sprechen wir von einem Reifegradmodell, wobei die Umsetzung stufenweise möglich und für jede Organisationsgröße sinnvoll ist.

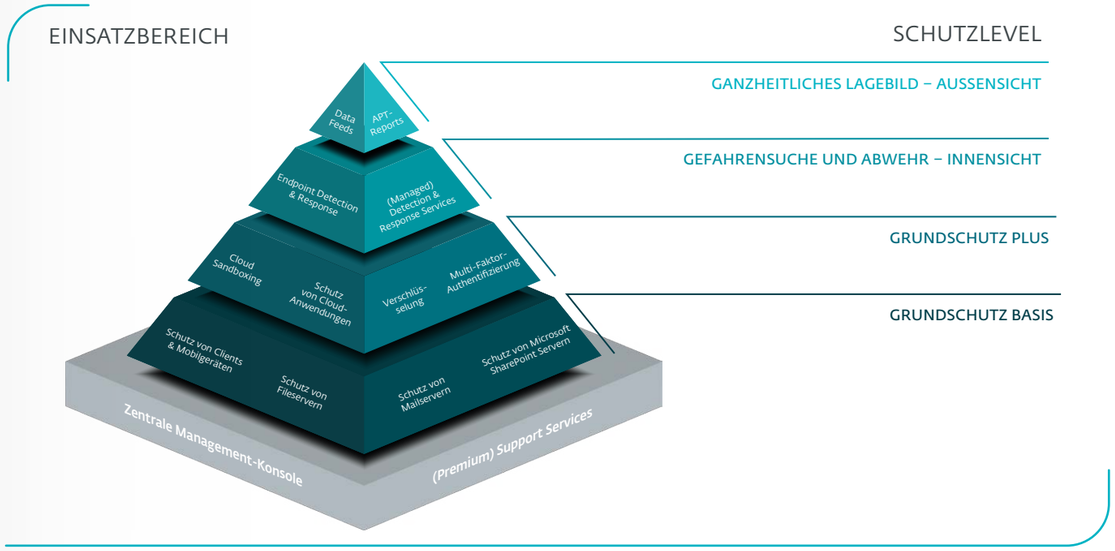

Abb. 6: Zero Trust Security-Ansatz von ESET

4.1. Grundschutz Basis

Ein Überblick über alle genutzten Endpoints und deren Schutzstatus ist unerlässlich für eine zuverlässige Absicherung von IT-Infrastrukturen. Ein zentrales Security Management verschafft diesen auf Knopfdruck – unabhängig von Unternehmensgröße oder Anzahl der eingesetzten Geräte. Es gewährleistet zudem durch Reporting-Funktionen und Policy-Optionen eine umfassende Kontrolle der gesamten IT-Sicherheit. Genauso wichtig ist eine zuverlässige Sicherheitslösung zum Schutz aller eingesetzten Clients, Mobilgeräte und Server. Damit kann zumindest der Basisschutz für einen unterbrechungsfreien Arbeitsalltag erreicht werden.

Beispielrechnung:

Auch für Unternehmen mit wenigen Arbeitsplätzen ist das Schutzlevel **Grundschutz Plus** für weniger als 8€ netto pro Monat und Gerät realisierbar. Je nach Lizenzgröße, -modell und -laufzeit auch deutlich darunter! Im Vergleich dazu stellen Unternehmen ihren Mitarbeitern Obst und Gemüse im gleichen Wert zur Verfügung. Bei einem erfolgreichen Cyberangriff vergeht ihnen allerdings schnell der Appetit.

4.2. Grundschutz Plus

In den meisten Fällen sind die Anforderungen an die Umsetzung geeigneter technischer Maßnahmen zur Erreichung eines angemessenen Schutzniveaus deutlich höher. Daten- bzw. Passwortdiebstahl, Ransomware, APTs und Zero Day-Bedrohungen stellen Organisationen jeder Größe vor immense Herausforderungen. Dem steigenden Risiko durch derartige Gefahren muss auch die IT-Sicherheit innerhalb von Organisationen Rechnung tragen, um dem Anspruch der Angemessenheit zu genügen. Ein möglicher Ansatzpunkt für ein gesteigertes Schutzniveau liegt in der Härtung der eingesetzten Endgeräte. Diese beginnt mit Lösungen für die Verschlüsselung und Multi-Faktor-Authentifizierung, die sowohl in der DSGVO als auch der NIS-2-Richtlinie explizit genannt werden. Darüber hinaus gilt es die Infrastruktur vor Ransomware, APTs und Zero Day-Bedrohungen zu schützen. Der Einsatz von Cloud Sandboxing ist dafür das geeignete Mittel und schont zugleich die ohnehin meist knappen Ressourcen auf Endgeräten. Unbekannte, potenziell schädliche Samples werden dabei nicht auf dem Endgerät selbst, sondern in einer Cloud-Umgebung umfassend analysiert und bewertet. Mit einem zusätzlichen Schutz für Cloud-Anwendungen sind schließlich optimale Bedingungen für eine sichere cloudbasierte Zusammenarbeit und Kommunikation z.B. mit Microsoft 365 oder Google Workspace geschaffen. Damit können die Mitarbeitenden flexibel und ortsunabhängig arbeiten und halten zugleich der steigenden Anzahl an Einfallstoren durch diese agileren Arbeitsmodelle stand.

4.3. Gefahrensuche und Abwehr – Innensicht

Haben Organisationen entsprechend der Stufe Grundschutz Plus ihre Endpoints gehärtet, kann eine Vielzahl an Bedrohungen bereits abgewehrt werden. Je nach gesellschaftlicher Relevanz eines Unternehmens und der Risikobewertung kann eine Endpoint bzw. Extented Detection and Response-Lösung (EDR/XDR) die Wahrscheinlichkeit eines Sicherheitsvorfalls weiter minimieren. Hiermit können beispielsweise Schwachstellen, Fehlverhalten von Mitarbeitern oder unerwünschte Anwendungen umgehend als Anomalie identifiziert werden und lassen sich im Bedarfsfall direkt beheben. Zudem erkennen EDR-/XDR-Lösungen Datenschutzvorfälle und halten Schäden so gering wie möglich. Dieser Prozess muss mit höchster Sorgfalt und ohne Unterbrechung des laufenden Geschäfts erfolgen.

Doch nicht jede Organisation besitzt ausreichende Ressourcen, um entsprechende Analysen durchzuführen. In diesem Fall kann der operative Betrieb einer EDR-/XDR-Lösung von externen Experten oder Dienstleistern übernommen werden. Diese sogenannten Managed Detection and Response (MDR) Services erleben aktuell einen wahren Boom.

4.4. Ganzheitliches Lagebild – Außensicht

Nachdem Organisationen mit den bisher beschriebenen Sicherheitslösungen den Blick auf die eigenen Systeme gerichtet und deren Sicherheit gestärkt haben, besteht der nächste Schritt in einem Perspektivwechsel, bei dem man den Blick nach außen auf den globalen Cyberraum wirft. Nur so ist es möglich, Risiken für die eigene Organisation rechtzeitig vorauszusehen und seine Schutzmechanismen danach auszurichten. Ein solches Frühwarnsystem ist sehr wertvoll für Organisationen, die ein eigenes Security Operation Center (SOC) bzw. Security Information and Event Management (SIEM) betreiben oder aufgrund ihrer Branchenzugehörigkeit einem besonderen Risiko gezielter Angriffe ausgesetzt sind. Hier kommen sogenannte Threat Intelligence Services ins Spiel, die aufkeimende oder geplante Angriffe frühzeitig aufdecken und Aufschluss unter anderem über Angriffsvektoren, Verbreitungen, Akteure und Vorgehensweisen geben. In der Regel erhalten Unternehmen die externen Informationen aus diesen zusätzlichen Quellen in Form von APT-Reports oder Data Feeds. Während bei den APT-Reports die Informationen von Experten aufbereitet in Berichten zur Verfügung gestellt werden, erhalten Organisationen mit den Data Feeds die Rohdaten, die sie in ihre bestehenden SIEM-Systeme integrieren können. Hierbei sind eine gesicherte Reputation, schnelle Verfügbarkeit und eine extrem niedrige Fehlalarmrate unerlässlich.

5. Handlungs-empfehlungen

Wie gehe ich vor?

Alle Empfehlungen für den Einsatz von Sicherheitslösungen sind individuell nach den jeweiligen Anforderungen und dem tatsächlichen Bedarf zu bewerten. Von Organisation zu Organisation unterscheiden sich die vorherrschenden Systeme bzw. die zugrunde liegende Infrastruktur. Wenn es also um die Frage nach geeigneten technischen Maßnahmen geht (siehe „4. Technische Maßnahmen" auf Seite 19), besteht der erste Schritt darin, eine Bestandsaufnahme der eingesetzten Systeme zu machen, die geschützt werden sollen. Anschließend können sich Verantwortliche an den Zero Trust Security-Stufen orientieren, um das passende Schutzniveau und damit die notwendigen Lösungen zu identifizieren. Dazu gehört eine Abwägung der Verhältnismäßigkeit von Faktoren wie Kosten der Umsetzung und Eintrittswahrscheinlichkeit eines Vorfalls. Darüber hinaus helfen die folgenden Handlungsempfehlungen Verantwortlichen, ein angemessenes Schutzniveau in ihrer Organisation zu gewährleisten.

Vorbereitung ist alles – Seien Sie gerüstet für den Worst Case! Ein Notfallplan mit detaillierter Ausarbeitung verschiedener Szenarien zur Aufrechterhaltung des Betriebs, zu umfassendem Backup-Management, Wiederherstellungsmaßnahmen nach einem Notfall sowie zum Aufbau eines Risikomanagements sind unerlässlich. Holen Sie sich außerdem Expertenmeinungen bezüglich Cyberversicherungen und sinnvollen Policen ein und schließen Sie ein passendes Modell ab.

Up(-To-)Dates – Verwalten Sie Ihre eingesetzten Sicherheitslösungen von einer zentralen Management-Konsole aus. Damit behalten Ihre IT-Teams immer den Überblick zu den aktuellen (Versions-)Status der vorhandenen Clients, Server und Mobilgeräte, können Updates automatisiert ausrollen und minimieren das Risiko von Gefahren durch die Ausnutzung von Schwachstellen. Ideal ist der ergänzende Einsatz eines Patch & Vulnerability Managements.

Datenhoheit ist Gold wert – Die Kontrolle der Daten muss bei Ihnen liegen. Sorgen Sie dafür, dass die Datacenter ausschließlich lokal oder innerhalb der EU liegen bzw. gehostet werden, um den bestmöglichen Sicherheitsstandard zu gewährleisten.

Weniger ist mehr – Auch so könnte das Credo von Zero Trust Security-Konzepten lauten. Vergeben Sie innerhalb Ihrer Organisation jedem Mitarbeitenden ausschließlich die für die tägliche Arbeit zwingend notwendigen Berechtigungen und Freigaben. Darüber hinaus bieten solche Konzepte eine Orientierungshilfe, wie man das eigene Netzwerk unter Berücksichtigung individueller Anforderungen optimal schützen kann.

Datenschutz geht alle an – spätestens mit Inkrafttreten der DSGVO. Sie nennt die Verschlüsselung von Daten explizit als geeignete Schutzmaßnahme für die Verarbeitung und Speicherung personenbezogener und sensibler Dateien. Mit einer geeigneten Lösung sind selbst bei Verlust oder Diebstahl eines Geräts die darauf gespeicherten Daten geschützt. Zudem entfällt die öffentliche Meldepflicht binnen 72 Stunden bei Geräteverlust, weil die gespeicherten Daten für Unbefugte nicht zugängig sind.

Vertrauen ist gut, Kontrolle ist besser – Sichern Sie Logins und Zugriffe mit einer Multi-Faktor-Authentifizierung. Schützen Sie darüber kollaborative Arbeiten und die Kommunikation innerhalb Ihrer Organisation mit dedizierten Security-Lösungen.

Fokus auf das Daily Business – Entlasten Sie Ihre Mitarbeiter. Dank ausgeklügelter Technologien wie Cloud Sandboxing oder Algorithmen zur Anomalieerkennung (EDR-/XDR-Lösungen) werden potenzielle Bedrohungen aufgespürt, analysiert und gegebenenfalls beseitigt – noch bevor diese auf den Endpoints Ihrer Mitarbeiter Schaden verursachen können.

Hilfe annehmen ist keine Schwäche – schon gar nicht, wenn es um die Sicherheit Ihrer Organisation geht. Egal, ob Ihnen fachliche oder zeitliche Ressourcen fehlen – greifen Sie auf das Wissen von Sicherheitsexperten zurück! Eine wertvolle Unterstützung bieten dabei Managed Detection und Response (MDR) Services, die eine optimale Einrichtung und Nutzung der EDR-/XDR-Sicherheitslösungen im Hinblick auf aktuelle Anforderungen Ihrer Organisation gewährleisten.

Geld schließt Einfallstore – Planen Sie ausreichend Budget für Ihre IT-Security und den Einsatz angemessener technischer Maßnahmen ein. Sinnvolle Investitionen in die Sicherheit der Infrastruktur können ungeplanten Kosten oder Störungen im Alltag durch Vorfälle vorbeugen.

Lieferant oder Kunde? – Hauptsache sicher! Treffen Sie präventive, umfassende Maßnahmen für die Zusammenarbeit mit Dritten. So lassen sich Supply Chain-Angriffe minimieren. Erstellen Sie Richtlinien, wie gemeinsame Zugänge auf Systeme abzusichern und anzuwenden sind. Sensibilisieren Sie Ihre Geschäftspartner und Stakeholder für Cybersecurity, z.B. mit einem Cyber Security Awareness Training.

Abb. 7: Zero Trust Security-Modell als Orientierungshilfe, ESET Umfrage zum Stand der IT-Sicherheit 2023

Fazit

Die Einhaltung der Maßnahmen im Rahmen von **Stand der Technik** stellt die Grundvoraussetzung von IT-Sicherheit dar, um Cyberangriffe überhaupt erfolgreich abwehren zu können. Das gilt unabhängig von der Rechtslage sowie der möglichen Zugehörigkeit eines Unternehmens zur Kritischen Infrastruktur. Organisationen müssen **angemessene Maßnahmen** ergreifen, um ihre IT-Systeme abzusichern und das Risiko von Angriffen zu minimieren. Bei der Frage nach konkreten strategischen und technischen Lösungen können Konzepte wie das **Zero Trust Security-Modell** weiterhelfen. Eine Cyberversicherung bietet optional zusätzlichen Schutz. Hier gilt es, die notwendigen Deckungsvoraussetzungen zu erfüllen und die Policen genau zu prüfen. Ziel muss es sein, ein ausgewogenes Verhältnis zwischen Risikominimierung und praktikablen Lösungen zu finden, um einen effektiven Schutz vor Cyberangriffen zu gewährleisten.

Kontaktdaten

Michael Schröder
Manager of Security Business Strategy
ESET Deutschland GmbH
Spitzweidenweg 32
07743 Jena
+49 3641 3114 220
partner@eset.de

Stefan Sander
Rechtsanwalt, Fachanwalt für IT-Recht
SDS Rechtsanwälte Sander Schöning PartG mbB
Villenstraße 7
47229 Duisburg
+49 203 39208900
info@sds.ruhr

Sprechen Sie uns an!

ESET – Informationssicherheit
für Organisationen jeder Größe

Qualitätsmanagement – Made in EU:

- überall verfügbar – vollautomatischer Schutz der gesamten Organisation
- volle Kontrolle über Ihre Daten dank transparenter (Sample-)Analysen innerhalb der EU
- einzigartige Geschwindigkeit bei der Analyse von eingehenden Warnmeldungen
- zuverlässig und sicher – alle Anforderungen von Datenschutzbestimmungen (bspw. DSGVO) bequem erfüllen
- große Flexibilität in puncto Lizenzform, Hardwareeinsatz und Anforderungen an die Infrastruktur

Vorteile für Einrichtungen:

- passgenaue IT-Sicherheit für alle Unternehmensgrößen und -anforderungen
- Mitarbeiter entlasten und (Hardware-)Ressourcen schonen
- Compliance und Sicherheitsstandards erweitern
- Verwaltung aller Schutzlösungen für alle gängigen Betriebssysteme via ESET PROTECT (cloudbasiert oder On-Premises)
- Lizenzvielfalt – Kombination beliebiger Betriebssysteme (Windows, macOS, Linux) und Geräte (Clients, Server, Mobilgeräte) entsprechend der Bedürfnisse

47% der Verantwortlichen kämpfen noch immer mit fehlenden Budgets und/oder Personal.
Dagegen glauben immerhin 75%, dass IT-Security inzwischen
den richtigen Stellenwert einnimmt!

Quelle: ESET Umfrage Stand der IT-Sicherheit 2023

Danksagung
Nachfolgend möchten wir uns bei den Personen bedanken, ohne die die Erstellung eines solchen Whitepapers nicht möglich gewesen wäre. Für ihre bedingungslose Unterstützung, den zugelieferten Input, die grafische Aufbereitung sowie das Lektorat schulden wir nachfolgenden Personen daher unseren größten Respekt und die verdiente Anerkennung:

Ivonne Biereye | Ildiko Bruhns | Stephanie Clarke | Michael Klatte | Alexander Opel | Hannes Reichel | Thorsten Urbanski | Antonia Volke | Maik Wetzel

Quellenverzeichnis

Abbildungsverzeichnis

Literaturverzeichnis

1 BSI-Gesetz – BSIG, Gesetz über das Bundesamt für Sicherheit in der Informationstechnik vom 14. August 2009, https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/BSI-Gesetz/bsi-gesetz_node.html

2 Netz- und Informationssystemsicherheitsgesetz – NISG, Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen, Fassung vom 26.07.2023, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536

3 Nationale Cyberstrategie – NCS, Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken, https://www.ncsc.admin.ch/ncsc/de/home/strategie/cyberstrategie-ncs.html

4 IT-Sicherheitsgesetz 2.0, Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 23. April 2021, https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html

5 NIS-2-Richtlinie, Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555

6 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679

7 BSI-KritisV, BSI-Kritisverordnung vom 1. Januar 2022, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/BSI_Kritis_VO.html

8 Bericht des Rechnungshofes: Koordination der Cyber-Sicherheit vom 22. April 2022, https://www.parlament.gv.at/dokument/XXVII/III/623/imfname_1439169.pdf

9 Informationssicherheitsgesetz – ISG, Bundesgesetz über die Informationssicherheit beim Bund vom 18. Dezember 2020, https://fedlex.data.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2020/2696/de/pdf-x/fedlex-data-admin-ch-eli-fga-2020-2696-de-pdf-x.pdf

10 Handreichung zum „Stand der Technik", Bundesverband IT-Sicherheit e.V. (TeleTrust), https://www.stand-der-technik-security.de/startseite/

11 Benutzerleitfaden zur Definition von KMU, Europäische Kommission, https://www.bafa.de/SharedDocs/Downloads/DE/kmu_handbuch_eu.html

ÜBER ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Unternehmensgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihr Netzwerk mithilfe von Cloud Sandboxing frei von Zero Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungsprodukte unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen.

Unsere XDR-Basis mit Endpoint Detection and Response-Lösung, Frühwarnsysteme (bspw. Threat Intelligence) und dedizierte Services ergänzen das Angebot im Hinblick auf Forensik sowie den gezielten Schutz vor Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste Technologien, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

3 VON ÜBER 400.000 ZUFRIEDENEN KUNDEN

BVB 09 CHAMPION PARTNER

Seit 2019 ein starkes Team auf dem Platz und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Security made in EU
Trust Seal www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel „IT Security made in EU" verliehen

ISO 9001 SGS
ISO/IEC 27001 SGS

Unsere Lösungen sind nach den Qualitäts- und Informationssicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2013 zertifiziert

ESET IN ZAHLEN

110.000.000+
Geschützte Nutzer weltweit

400.000+
Geschützte Unternehmen

195+
Länder & Regionen

13
Forschungs- und Entwicklungszentren weltweit

welivesecurity by ESET

ESET Digital Security Guide

ESET Deutschland GmbH | Spitzweidenweg 32 | 07743 Jena | Tel.:+49 3641 3114 200

ESET.DE | ESET.AT | ESET.CH

Digital Security
Progress. Protected.

↗ ESET.DE/STAND-DER-TECHNIK