Zur Online Ausgabe

LawThek VERLAG

USANCEN: TechGuard

Digitalisierung - Cybergovernance – Künstliche Intelligenz

00/23

AI kontrolliert einsetzen: Trustworthy AI, Controllable AI und Beschaffung sicherer AI

Datengesteuerte Anwendungen spielen eine immer wichtigere Rolle in unserem Leben und durchdringen immer mehr Aspekte unserer Routine. In den kommenden Jahren werden KI-basierte Systeme alltäglich werden ... SEITE 15

Willkommen bei Usancen:TechGuard!
Das Journal für Technologie und Cybersicherheit

Es ist uns eine große Freude, Ihnen die erste Ausgabe von „Usancen:TechGuard“ vorzustellen, einem Journal, das sich den Herausforderungen und Chancen in den Bereichen Technologie, Recht, Cybersecurity und digitale Transformation widmet. In einer Welt, in der technologische Fortschritte und Cyberbedrohungen Hand in Hand gehen, zielt „Usancen:TechGuard“ darauf ab, ein unverzichtbares Medium für Führungskräfte, Manager:innen und Expert:innen zu sein, die sich täglich mit diesen dynamischen und entscheidenden Themen auseinandersetzen.

Unsere erste Ausgabe: 00/2023

In unserer ersten Ausgabe decken unsere Autor:innen eine Vielzahl von Themenbereichen ab. Dazu gehören ein Beitrag zur Cyberforensik von Michael Veit, ein Beitrag zu Informationsquellen von Robert Redl, die Betrachtung der Frage wie Anwendungssicherheit durch einen sicheren Softwarentwicklungslebenszyklus verbessert werden kann von Stefan Jakoubi und Michael Koppmann, sowie Überlegungen zu unerwarteten Ereignissen von Barbara Flügge, die Aufbereitung der Frage, wie man AI kontrolliert einsetzen kann von Andreas Holzinger, Peter Kieseberg und Simon Tjoa, ein Beitrag zu Cyberversicherung und Homeoffice von Lisa Katharina Promok, Authentifikation in der digitalen Ära von Markus Vesely, neue Aspekte der Managementhaftung in Folge von NIS2 von Stefan Eder.

Dank an Unsere Wegbereiter

Unser besonderer Dank gilt den herausragenden Autor:innen dieser Erstausgabe sowie den Mitgliedern unseres Redaktionsbeirates. Ihre Expertise und ihr Engagement ermöglichen es uns, ein breites Spektrum an tiefgreifenden und einsichtreichen Beiträgen in gut verständlicher Ausdrucksweise abzudecken. Das entspricht unserem Anspruch, ein Forum für hochkarätige Fachdiskussionen und innovative Ideen zu sein.

Eine Welt voller Möglichkeiten:

Unsere Themenschwerpunkte

„Usancen:TechGuard“ deckt einen weiten Bereich von Themen, beginnend mit den neuesten Trends in der Cybersecurity und KI bis hin zu praxisnahen Fallstudien und strategischen Überlegungen zur digitalen Transformation, ab. Wir bieten Einblicke in die aktuellen Herausforderungen und Chancen im Kontext der aktuellen Technologien, Risikomanagement, Governance und Compliance. Unser Journal verbindet theoretische Erkenntnisse mit praxisrelevanten Lösungen, um unseren Leser:innen einen umfassenden Überblick über den jeweiligen Stand der Technik zu geben.

Informationsquellen und rechtlicher Rahmen: Zugänglichkeit und Verständlichkeit

Ein Hauptanliegen von „TechGuard“ ist es, die Fülle an Informationen und Ressourcen, die sich auf Risikomanagement im Kontext von KI und Cybersecurity erstrecken, sichtbar und zugänglich zu machen. Der aktuelle Stand der Technik ist schwer zu überblicken und ändert sich laufend. Der rechtliche Rahmen erstreckt sich über viele unterschiedliche Regelungen wie NIS2, DORA, den bevorstehenden AI-Act und andere Rechtsquellen. Die relevanten Regelungen sind weit gestreut und daher nicht für jedermann leicht zugänglich.

Wir wollen diese Quellen nicht nur sichtbar machen, sondern sie auch in einer Form aufbereiten, die für unsere Leserschaft gut verständlich ist. Unser Ziel ist es, auch durch das Bereitstellen von Leitfäden, Checklisten und anderen hilfreichen Informationen, eine Brücke zwischen den vielen Quellen und den praktischen Anforderungen derer zu schlagen, die sich täglich mit diesen Themen auseinandersetzen.

FORTSETZUNG NÄCHSTE SEITE »

HERAUSGEBER
LawThek Verlag

Zielgruppe und Einbindung der Leserschaft

„Usancen:TechGuard" richtet sich an ein breites Spektrum von Leser:innen, die sich mit Risikomanagement, Technologie und Sicherheit in ihren Organisationen befassen. Wir ermutigen unsere Leser:innen, aktiv am Dialog teilzunehmen, indem sie Feedback und Kommentare zu unseren Artikeln senden und werden immer wieder gerne Fragen mit unseren Autor:innen aufgreifen und dazu Rückmeldung geben. Ihr Input ist entscheidend für die ständige qualitative Weiterentwicklung unseres Journals.

Nachhaltigkeit und Zugänglichkeit: Unsere Publikationsstrategie

In Übereinstimmung mit den Prinzipien der Nachhaltigkeit und ESG fokussiert sich „Usancen:TechGuard" auf eine digitale Veröffentlichungsstrategie, unsere Artikel und das Journal sind auf unserer Landingpage **cybsec.lawthek.eu** publiziert. Für diejenigen, die eine gedruckte Version bevorzugen, bieten wir eine Print-on-Demand-Option an. Zusätzlich sind unsere Inhalte über die LawThek Plattform **(lawthek.eu)** und die RIS:App zugänglich.

Blick in die Zukunft: Engagement für Exzellenz

In den kommenden Ausgaben von „TechGuard" werden wir unser Themenspektrum kontinuierlich erweitern und vertiefen. Unser Engagement für qualitativ hochwertige, zitierfähige Inhalte bleibt unser oberstes Ziel. Wir sind bestrebt, eine Plattform zu schaffen, die nicht nur informiert, sondern auch inspiriert.

Die Rolle und Ziele unseres Redaktionsbeirats

Ein wesentlicher Pfeiler des Erfolgs von „Usancen:TechGuard" ist unser Redaktionsbeirat, dessen Hauptziel es ist, mitzuhelfen, ein wissenschaftlich fundiertes und hochqualitatives Journal zu schaffen. Der Beirat setzt sich aus erfahrenen Expert:innen zusammen, die sich der Verbreitung von Fachwissen verpflichtet fühlen und daher einerseits Schwerpunkte vorgeben und andererseits bei der Auswahl der Themen und der Artikel unterstützen und auch selbst mit Artikeln zum Inhalt unseres Journals beitragen.

Zusammenfassung und Einladung

Mit „TechGuard" betreten wir eine spannende neue Ära der Technologie- und Sicherheitsdiskussion. Wir laden Sie herzlich ein, Teil unserer wachsenden Community zu werden und mit uns gemeinsam die Zukunft der digitalen Welt zu gestalten. Senden Sie uns Ihre Beiträge, Anregungen und Fragen. Sie erreichen uns unter **redaktion@cybsec.net**

Impressum

Offenlegung gem. § 25 MedienG | Medieninhaber und Herausgeber Dr. Stefan Eder, Rechtsanwalt | Sitz Tuchlauben 8, 1010 Wien |
Grundlegende Richtung des Mediums (Blattlinie) **Darstellung praxisnaher Entwicklungen und Fragestellungen des Rechts- und IT-Sicherheitsbereich, insbesondere zu Legal-Tech und Rechtsinformatik**

Informationspflichten gem. § 5 ECG | Diensteanbieter LawThek Verlags GmbH | Anschrift Tuchlauben 8, 1010 Wien | Kontakt Telefon: +43 1 532 28 70 E-Mail: **info@lawthek-verlag.com** | Firmenbuch Landesgericht Wien, FN 581943z | Umsatzsteuer-Identifikationsnummer ATU78231478 | Bürgermeister der Stadt Wien | Anwendbare berufsrechtliche Vorschriften Gewerbeordnung 1994 | Zugehörigkeit Wirtschaftskammer Österreich

„Die Quellenangaben in den Artikeln befinden sich zum Zeitpunkt der Publikation auf aktuellem Stand (November 2023)."

Leserservice: Ihre Wünsche, Anregungen sowie Beschwerden senden Sie bitte an **info@lawthek-verlag.com**
Abonnement: Unser Kundendienst hilft Ihnen gerne: **info@lawthek-verlag.com.**

In manchen Beiträgen wurde teilweise auf geschlechtsspezifische Formulierungen verzichtet, um die Lesbarkeit und Verständlichkeit zu erhöhen. Die gewählte Form kann variieren und spiegelt individuelle Präferenzen des Autors wider. Dies dient keiner Diskriminierung, sondern soll eine inklusive Sprache fördern.
Bei Fragen oder Anregungen stehen wir zur Verfügung.

Inhaltsverzeichnis

Cyberforensik-Report: Bequemlichkeit spielt Cyberkriminellen in die Karten 6
Michael Veit, MBI

GEMEINSAM! EINFACH! SICHERER! 7
Mag. Robert Redl

Cybersicherheit im Teamwork für das digitale Zeitalter 12
Michael Veit, MBI

AI kontrolliert einsetzen – Trustworthy AI, Controllable AI und Beschaffung sicherer AI 15
Dr. Andreas Holzinger, DI. Peter Kieseberg, FH-Prof. Mag. Dr. Simon Tjoa

Anwendungssicherheit durch einen sicheren Softwareentwicklungslebenszyklus (SDLC) 18
Mag. Stefan Jakoubi, Dipl.-Ing. Michael Koppmann

Exemplarische Probleme aus der Cyberversicherung im Zusammenhang mit Homeoffice 20
Mag. Lisa Katharina Promok

Authentifikation in der digitalen Ära: Wie Privatpersonen und Unternehmen ihre digitalen Identitäten bewahren 28
Dr. Markus Vesely

Das unerwartete Ereignis 30
Dr. Barbara Flügge

Aktuelles aus den Gerichten 34
Benn-Ibler Rechtsanwälte

Paradigmenwechsel für die Verantwortung von Leitungsorganen durch NIS-2 36
Mag. Dr. Stefan Eder

Cybersicher mit fit4internet 40
fit4internet

Digitalisierungvorhaben EU 2023 und Ausblick 2024 42
Benn-Ibler Rechtsanwälte

Cyberforensik-Report: Bequemlichkeit spielt Cyberkriminellen in die Karten

AUTOR:IN
Michael Veit
Master of Business Informatics
Cybersecurity-Experte bei Sophos

Der aktuelle **Active Adversary Report** von Sophos deckt eine interessante Trendwende auf, die ein allgemein verbreitetes Problem in der IT-Sicherheit betrifft: Bequemlichkeit. In **früheren Falldaten** aus dem Report, der reale Cyberattacken analysiert, war die Ausnutzung von Sicherheitslücken die Hauptursache für Angriffe, dicht gefolgt von kompromittierten Zugangsdaten. In der ersten Jahreshälfte 2023 kehrt sich dieses Bild um, und zum ersten Mal standen mit 50% kompromittierte Zugangsdaten an erster Stelle der Ursachen. Die Ausnutzung einer Schwachstelle lag bei 23%. Auch wenn diese Momentaufnahme nicht umfassend belegen kann, dass Angreifer kompromittierte Anmeldeinformationen gegenüber Schwachstellen bevorzugen, lässt es sich nicht leugnen, dass die Nutzung illegal erworbener, gültiger Konten die Machenschaften der Angreifer erheblich erleichtert. Was die Kompromittierung von Anmeldedaten für die Cyberkriminellen noch einmal attraktiver macht, ist die in vielen Organisationen immer noch ganz fehlende oder nicht konsequent umgesetzte Multifaktor-Authentifizierung (MFA).

Bei der forensischen Aufarbeitung der Cyberattacken stellten die SophosLabs fest, dass MFA in 39% der bisher untersuchten Fälle nicht umfassend konfiguriert war. „Das Entmutigendste an dieser Statistik ist, dass wir als Branche wissen, wie man dieses Problem löst, aber zu wenige Organisationen diesen Bereich priorisieren“, so Michael Veit, Cybersecurity-Experte bei Sophos. „Das Problem ist also nicht die Technologie, sondern die Durchsetzung. Oftmals werden die Authentifizierungsanforderungen gelockert, um ein besseres Benutzererlebnis zu bieten. Das öffnet Angreifern Tür und Tor und wenn es um menschliche Gegner geht, bieten diese kleinen Risse bereits beste Chancen, um in Netzwerke einzudringen.“

Im Bereich MFA findet ein ständiger Wettlauf statt. Da Unternehmen stärkere Authentifizierungsmechanismen einführen, reagieren Kriminelle mit der Entwicklung von Techniken, die die eingesetzten Technologien umgehen. „Dieser Zyklus wird sich auf absehbare Zeit fortsetzen“, so Veit „Wir haben jetzt den Punkt überschritten, an dem einfache SMS-Codes, zeitbasierte Einmalpasswörter (TOTP) oder sogar Push-Based-Authentifizierung effektiv sind. Organisationen, die sich vor den neuesten Angriffstechniken schützen möchten, müssen auf Phishing-resistente MFA umsteigen. Und selbst hier sind die Kriminelle nicht untätig. Als Sophos X-Ops die Daten für den aktuellen Report analysierten, entdeckte das Team, dass eine der neuesten Social-Engineering-Taktiken zum Beispiel darin besteht, den Empfänger per SMS dazu zu bewegen, seinen Security Token zu deaktivieren.“

Moderne, phishing-resistente MFA-Technologien als Standardauthentifizierungsmodus für alle Dienste innerhalb einer Organisation inklusive entsprechender Schulungen sorgen aktuell für maximalen Schutz gegen kompromittierte Anmeldedaten. Dabei müssen die entstehenden **Kosten** auch an den Kosten einer potenziellen Sicherheitsverletzung und Wiederherstellung gemessen werden, die oft um ein Vielfaches teurer sind. Eine starke Authentifizierung allein kann jedoch nicht jeden Angriff stoppen, weshalb **mehrschichtige Verteidigung** und Telemetrieanalyse von entscheidender Bedeutung sind. Beides verschafft Unternehmen Zeit und Gelegenheit, einen aktiven Angriff zu erkennen und abzuwehren.

Darüber hinaus können viele Authentifizierungssysteme für den adaptiven Zugriff konfiguriert werden. Dieses Vorgehen auch Basis des **Zero-Trust-Ansatzes** ändert die Zugriffs- oder Vertrauensebene basierend auf Kontextdaten über den Benutzer oder das Gerät, das Zugriff anfordert. Außerdem wird der Zugriff auf Benutzer beschränkt, die ihn wirklich benötigen. Mit adaptiven Zugriffsauthentifizierungssystemen können Unternehmen Zugriffsrichtlinien für bestimmte Anwendungen oder Benutzergruppen anpassen und dynamisch auf verdächtige Signale reagieren.

GEMEINSAM! EINFACH! SICHERER!

AUTOR:IN
Mag. Robert Redl
VOICE Bundesverband der IT-Anwender e.V.
Knowledge- und Netzwerk Manager

Unternehmens- und länderübergreifende Zusammenarbeit (Community) als wesentlicher Erfolgsfaktor für Informationssicherheit!
Dies gilt für Unternehmen aller Größenordnungen, besonders aber für viele Mittelstandsunternehmen, die heute bei der Umsetzung notwendiger Maßnahmen oft noch keinen ausreichenden Reifegrad oder **Stand der Technik** erreicht haben.
Die organisatorischen und vor allem auch technischen Maßnahmen sind teilweise aufwendig und verlangen auch entsprechend adäquater Mittel.

Die wohl wichtigsten Aufgaben für Führungskräfte in den nächsten 9 Monaten werden folgende sein:
Gestaltung der entsprechenden Rahmenbedingungen (personelle und budgetäre Ressourcen oder Beschaffung qualifizierter Unterstützung)
Verpflichtende Ausbildung der Führungskräfte (auch für die Geschäftsleitung)
Überblick der relevanten Risken für das Unternehmen und den noch zu treffenden Maßnahmen (regelmäßige Berichtserstattung an die Geschäftsleitung)
Sich auf den Ernstfall vorbereiten! Dies bedeutet auch entsprechende Notfalls- und Krisenvorsorgen zu treffen und entsprechend zu üben!
Investitionen in ein Mindestmaß von Sicherheitstechnologien (Plattformen) für den Schutz von Geräten, Netzwerken und Informationen.

Nur noch knapp 320 Tage bis zum Inkrafttreten der NIS 2.0 Richtlinie, somit höchste Zeit den eigenen Reifegrad festzustellen und notwendige Maßnahmen zu setzen!
Dies sollte jedoch für jedes Unternehmen bereits heute eine Selbstverständlichkeit sein!
Zunehmend wird dies auch aufgrund der hohen wirtschaftlichen Vernetzung („Third Party Risk Management“) und der ständig wachsenden Bedrohungen (Vergrößerung der Angriffsflächen z.B. durch Vernetzung von Maschinen, Digitalisierung in der Produktion usw.)
Informationssicherheit muss Bestandteil der Unternehmensstrategie und jeder Produkt- und Dienstleistungsbereitstellung werden („Security by Design“).
Es gibt jedoch keinen 100% Schutz! Der Eintritt eines Cybervorfalls ist nur eine Frage der Zeit und ihr Vorbereitungsgrad entscheidet über die Überlebensfähigkeit Ihres Unternehmens, sowie leider auch oftmals die der Kunden und Partner.
Im Rahmen der VOICE-Veranstaltung Entscheiderforum 2023 gab es eine hochkarätige Gesprächsrunde zum aktuellen Status von Informationssicherheit.
Juhan Lepassaare (Executive Director der ENISA), Dr. Gerhard Schabhüser (Vizepräsident vom BSI) und Jimmy Heschl als Vertreter der Anwenderunternehmen gaben einen ersten kurzen Einblick in die aktuellen Entwicklungen. Die anschließende Podiumsdiskussion mit mehr als 150 IT-Verantwortlichen aus Anwenderunternehmen zeigte die vielfältigen Herausforderungen und Fragestellungen aus Sicht der Unternehmen.
Eine Reihe von Regularien, insbesondere aber die NIS 2 Richtlinie und der CRA (Cyber Resilience Act) sorgen für erhöhte Compliance- und vor allem auch Umsetzungsanforderungen in Unternehmen aller Größenordnungen.

Eine Präsentation im Rahmen des VOICE Informationssicherheitstdialogs von Jimmy Heschl brachte zwei wesentliche Aspekte auf den Punkt:

Insgesamt werden in der D-A-CH Region ca. 50.000 Unternehmen von der NIS 2.0 Richtlinie direkt betroffen sein. Die indirekten Auswirkungen gehen durch weitere Entwicklungen wie den CRA (Cyber Resilience Act) und die Verpflichtung von Unternehmen sich auch eines Mindestniveaus bei ihren Lieferanten (Produkten, Dientsleistungen) zu versichern noch weit darüber hinaus!
Die Zusammenfassung in einem sehr kurzen Satz lautete: **„Es gibt noch viel zu tun“!**
Bereits heute tragen Unternehmen aller Größenordnungen die Last von Aufwendungen aufgrund von fehlerhaften Produkten oder ungenügenden Dienstleistungen. Der CRA sollte diese Situation mittelfristig verbessern und hält gleichzeitig Unternehmen dazu an ein

FORTSETZUNG NÄCHSTE SEITE »

höheres Maß von Sicherheit bei ihren Produkten (insbesondere mit Softwarekomponenten) zu gewährleisten.

Die Frage ist jedoch vor allem das WIE!

Die nachstehenden Handlungsfelder geben einen groben Überblick über die wichtigsten Maßnahmen. Dahinter liegt jedoch eine große Anzahl von konkreten Aufgabenstellungen:

Abbildung 1. Handlungsfelder

Schrittweise werden von verschiedenen Institutionen (ENISA, ECCC, BSI, etc.) – Guidelines und Hilfsmittel veröffentlicht die Orientierung und Hilfestellung bei der Umsetzung der notwendigen Maßnahmen geben.

Besonders hervorzuheben in Österreich sind Einrichtungen wie KSÖ (Kuratorium Sicheres Österreich), die CSP-Plattform und Vorstellung von NCC (Nationales Koordinierungscenter für Cybersicherheit) als Bestandteil der ECCC-Initiativen auf EU-Ebene. Diese Plattformen und Einrichtungen unterstützen österreichische Unternehmen bei der Umsetzung und der Erreichung des durch NIS 2.0 vorgeschriebenen Sicherheitsniveaus.

Während sich die Angreifer laufend professionalisieren (Cybercrime as a Service, Arbeitsteilung und Spezialisierung auf bestimmte Aufgaben), agieren Unternehmen weitgehend auf sich alleine gestellt und erfinden das Rad ständig neu.

Es gibt zwar mittlerweile eine unübersehbare Anzahl von physischen und virtuellen Veranstaltungen, die Informationsangebote der Anbieter und verschiedener loser Austauschgruppierungen, diesen gelingt es aber keinesfalls die Themenstellungen strukturiert und in ihrer Gesamtheit zu erfassen.

Es gibt zwar verschiedene Initiativen und Organisationen, die zu manchen Themen Orientierungs- und Umsetzungshilfen bieten.

Vor allem fehlt es heute aber an einer zentralen Übersicht zu den vielfältigen Möglichkeiten und Maßnahmen.

Die Kernidee eines übergreifenden Communityansatzes für die D-A-CH Region ist relevantes Wissen und Lösungsbausteine einfacher zugänglich zu machen und so den Zeitaufwand und das Kostenniveau für das Erreichen eines angemessenen Sicherheitsstandards für Ihr Unternehmen zu senken/niedrig zu halten.

Im Rahmen der ÖSCS (Österreichs Strategie für Cybersicherheit) wurde ein laufend in Erweiterung befindlicher Maßnahmenkatalog implementiert der bestimmte Lösungsbausteine auch kostenlos zur Verfügung stellt. Einen Überblick zu wichtigen Maßnahmen und weiterführenden Inhalten (primär Österreich oder D-A-CH Region) stellt die CCA-Initiative (Cyber Security Austria) zur Verfügung.

Soweit kostenlos oder frei verfügbar finden sich

dort auch Hinweise auf weiterführende Informationsquellen. Eine erweiterte Sammlung von Informationen steht VOICE-Mitgliedern ab 2024 zur Verfügung.
Ein weiteres Beispiel ist die Initiative OPCYBRES die einen umfassenden Ansatz zur Erhöhung der Resilienz von Unternehmen darstellt.
Auf rechtlicher Seite bietet die Plattform Lawthek einen guten Überblick zu wichtigen Compliance- und rechtlichen Aspekten der Informationssicherheit. Ein besonderer Fokus liegt dabei auf Verantwortung und Themenstellungen für leitende Organe eines Unternehmens.
Um mit der CCA Plattform eine aktuelle Wissensbasis zu schaffen sind alle Organisationen und Unternehmen eingeladen entsprechende Wissens- oder Lösungsbausteine oder auch Herausforderungen aus ihrer Sicht einzubringen.
Im Rahmen des Communityaustausches (erweiterte Version von CCA) gibt es auch Informationen zu „leistbaren" Technologien und Produkten. Erste Termine dazu gibt es ab 2024.
Während die Anforderungen weitgehend klar sind stellt die Umsetzung notwendiger Maßnahmen für viele Unternehmen eine große Herausforderungen dar!

Einige Beispiele für nationale und internationale Erfolgsbeispiele (Lösungsbausteine) entstanden für bestimmte Branchen oder Zielgruppen:

- Definition von Mindeststandards für bestimmte Zielgruppen (z.B. DIN SPEC 27076) in Deutschland
- Cyber Risk Rating von KSÖ und KSV stellt einen guten Ausgangspunkt zur Beherrschung von Lieferantenrisken in Österreich dar. Ein laufendes Förderprojekt der EU erweitert diesen Ansatz für Europa
- Branchenspezifische Zusammenarbeit von Unternehmen (E-CERT, EE-ISAC) – z.B. in der Energiewirtschaft)

Meistens bildet der NIST-Standard, die ISO Normen 2700x für Informationssicherheit und ISO 31000 für Risikomanagement oder der BSI Grundschutz die Ausgangslage zur Ableitung wesentlicher Anforderungen. Teilweise gibt es auch ergänzende Informationen wie bzw. Konkretisierungen zu Teilbereichen. Einige Beispiele

- ENISA Dokumente (ENISA Threat Landscape, Risikokataloge)
- „Handreichungen zum Stand der Technik" vom BSI in Deutschland
- Templatesammlungen (tlw. kostenflichtig aber meist preiswert)
- Mindeststandards in Deutschland für Kommunen
- IKT Minimalstandard Schweiz
- Plattform Sichere Industrie
- Initiativen von Wirtschaftkammern und Verbänden

Es gibt zu Informationssicherheit eine nahezu unüberschaubare Anzahl von Informationsquellen. Ohne eine Verdichtung der Informationen und Fokussierung auf die wesentlichen Aspekte sind jedoch viele Unternehmen nicht in der Lage den notwendigen Informationssicherheitsstandard zu erreichen.
Dabei geht es längts um mehr! Informationssicherheit muss Bestandteil jedes wirtschaftlichen Handelns, inbesondere durch die voranschreitende Digitalisierung, werden. Gelingt dies nicht sind Unternehmen gefährdet Kunden zu verlieren, Umsatzeinbußen zu erleiden oder Produkte nicht mehr verkaufen zu können!
Es gibt aber keine einfache Antwort bezüglich vieler Themenstellungen:

- Wie kann ich als Geschäftsleitungsmitglied die neuen Complianceanforderungen erfüllen?
- Wie hoch muss der Securitystandard für mein Unternehmen sein?
- Welche Ressourcen sind notwendig?
- Wie kann ich den Reifegrad meiner Organisation ermitteln?
- Was bedeutet Stand der Technik?

Der bestehende Ressourcenmangel an qualifizierten Mitarbeitern und das intransparente Produkt- und Dienstleistungsangebot wird zu der wesentlichen Herausforderung für Mittelstandsunter-nehmen.

Nachfolgend werden 2 Communityansätze kurz dargestellt die hier eine Hilfestellung sein können.
Vereine und Communities bieten bei den genannten Themenstellungen ebenfalls Unterstützung. So hat beispielsweise der IT-Anwenderverband VOICE ein begleitendes

FORTSETZUNG NÄCHSTE SEITE »

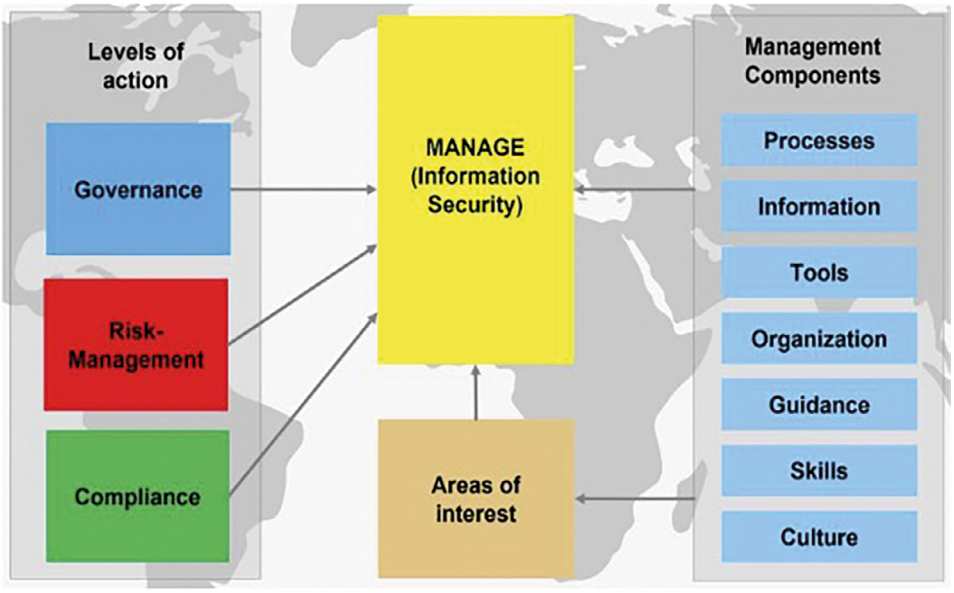

Abbildung 2. Managementframework

Veranstaltungsprogramm für 2024 vorgestellt, um vor allem auch Mittelstandsunternehmen zu unterstützen

Gemeinsam! Einfach! Sicher!

- Evaluierung und Diskussion von „Mindeststandards“
- Ableitung von konkreten Anforderungen für unterschiedliche Zielgruppen
- Definition von Handlungsfeldern
- Parameter die den Umfang des notwendigen Sicherheitsniveaus konkretisieren

Einige Beispiele für wesentliche Parameter zur Ableitung der unternehmensspezifschen Anforderungen sind:

- Unternehmensgröße
- Eigenbetrieb von wichtigen Applikationen bzw. Einsatz von Cloudservices
- Anforderungen durch Partner und Kunden
- Branchenspezifische Anforderungen (z.B. Kommunen und öffentlicher Bereich)

Der klassische Beratungsansatz kann jedoch nur noch eingeschränkt funktionieren. Es wird daher notwendig sein bei wesentlichen Lösungsbausteinen die entstehenden Kosten für Unternehmen zu minieren (kostenlose Angebote oder leistbare Angebote) und einen Überblick zu in der Praxis bewährten Lösungsansätzen zu bieten.
Jedenfalls ist für viele Unternehmen auch eine Neuausrichtung der gesamten Sicherheitsstrategie und Sicherheitsarchitektur notwendig (Tools, Prozesse,…) und die nachstehenden Aspekte sind gesamthaft zu betrachten. Dieses Managementframework ermöglicht Unternehmen eine effektive Umsetzung Ihrer Informationssicherheitsstrategie!

- Adäquates Risikomanagement und Business Continuity Management
- Auswahl von Managed Services
- Entscheidung einer Sicherheitsplattform bzw. Sicherheitstechnologien

Gleichzeitig ist der Stillstand bei all diesen Herausforderungen keine Option. Künstliche Intelligenz sorgt einerseits für automatisiertes Handeln in der Abwehr von Bedrohungen und gleichzeitig für neue Angriffsvektoren!
Zusammenfassend wollen wir Sie einladen sich der CCA-Initiative (Teilen von Wissen über Communitygrenzen) mit Ihrem Unternehmen anzuschließen oder Ihre Herausforderungen und Fragestellungen einzubringen.
Für IT-Anwenderorganisationen bietet die Mitgliedschaft in einem Verband mit hoher Kompetenz zu Informationssicherheitsthemen weiterführende Möglichkeiten.
Zu beiden Themenstellungen stehen Ihnen über die CCA-Plattform weitere Informationen zur Verfügung.

Wirken Sie mit und erhöhen Sie Ihre Informationssicherheit im Interesse Ihres Unternehmens, Ihrer Kunden und Partner!

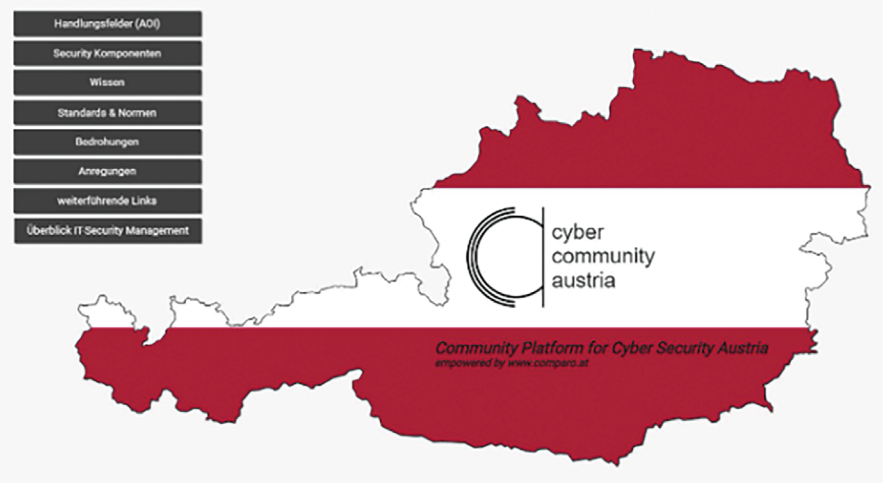

Abbildung 3. Cyber Community Austria

Linksammlung:

CCA-Sharpcloud: https://eu.sharpcloud.com/html/#/story/0991f317-112e-42e9-ba9a-ec6401083b26

OPSAM light: https://eu.sharpcloud.com/html/#/story/2a656360-a730-41b4-9ab0-aaa4b67472a1

ÖSCS: https://www.bundeskanzleramt.gv.at/themen/cybersicherheit/oesterreichische-strategie-fuer-cybersicherheit.html

BSI IT-Grundschutz: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

IKT Minimalstandard: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/ikt-minimalstandards.html

BSI Stand der Technik: https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/stand-der-technik-umsetzen_node.html

ENISA Threat Landscape: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

Sichere Industrie: https://www.sichere-industrie.de/

Cyber Risk Rating der KSÖ/KSV: https://cyberrisk-rating.at/

DINSPEC 27076: https://www.beuth.de/de/technische-regel/din-spec-27076/365252629

Cybersicherheit im Teamwork für das digitale Zeitalter

AUTOR
Michael Veit
Master of Business Informatics
Cybersecurity-Experte bei Sophos

Der Übergang in eine hybride Arbeitswelt mit immer mehr verbundenen Geräten und mobilen Mitarbeitern stellt IT-Abteilungen jeglicher Größenordnung vor beträchtliche Herausforderungen. Das gilt vor allem für das Thema IT-Sicherheit. Doch es gibt flexible Lösungen.

Die Problematik wird auch in der Studie „State of Cybersecurity 2023" von Sophos bestätigt. Immerhin glauben 56 Prozent der in Deutschland befragten Teilnehmer, dass die Cybergefahren zu fortgeschritten sind, um sie allein bewältigen zu können. Der Bedarf an Cybersecurity as a Service mit skalierbaren, zentral fernverwalteten und agilen Lösungen ist daher enorm, zusätzlich angefeuert durch den eklatanten Fachkräftemangel.

Obwohl der Zugriff auf Daten außerhalb des Büros schon immer mit Risiken verbunden war, hat die Häufigkeit dieser Praxis durch die Digitalisierungs- und Home-Office-Welle die Wahrscheinlichkeit eines erfolgreichen Angriffs und damit die monetären Anreize für Cyberkriminelle enorm erhöht. Zu diesem Ergebnis kommt auch das Bundeskriminalamt, das in seinem „Bundeslagebild Cybercrime" im August 2023 Ransomware weiterhin als primäre Bedrohung für Unternehmen und öffentliche Einrichtungen definiert.

Es geht darum, Cyberangriffe so früh wie möglich zu entdecken

Als Antwort auf diese Entwicklung starten viele Unternehmen konzertierte Anstrengungen, um ihre Abwehrmaßnahmen als Reaktion auf die hybride Arbeitswelt zu erweitern und zu synchronisieren. Dabei entsteht aktuell eine Verlagerung des grundsätzlichen Ziels beim Erstellen einer Cybersecurity-Strategie: Es geht nicht mehr primär darum, Bedrohungen nach dem Entdecken unschädlich zu machen, sondern das neue Hauptziel besteht darin, Bedrohungen so früh wie möglich in der Angriffskette zu stoppen, idealerweise bevor der Angreifer überhaupt umfänglich in Unternehmenssysteme eindringt. Die Schwierigkeit besteht darin, die Signale eines potenziellen Angriffs zu erkennen – laut State of Cybersecurity 2023 Studie von Sophos sehen 59 Prozent der in Deutschlang Befragten genau darin ein Problem. Doch es kann geholfen werden. Mittlerweile können speziell ausgebildete und international vernetzte Experten durch gezielte Bedrohungssuche mit Hilfe von Künstlicher Intelligenz Lücken oder Schwachstellen frühzeitig identifizieren und schließen, bevor ein Angreifer sie ausnutzen kann. Durch die zentrale Steuerung dieser Abwehrmaßnahmen können Unternehmen ihren Mitarbeitern optimalen Schutz bieten, egal ob im Büro, Zuhause oder unterwegs.

So bekannt das Problem, so aufwändig und schwierig ist allerdings die Lösung, da die Implementierung eines umfassenden Cybersecurity-Ökosystems zwei maßgebliche Komponenten benötigt: die vernetzte und intelligente Kontrolle aller Endgeräte, Server und Netzwerke eines Unternehmens sowie die Unterstützung durch erfahrene Cybersecurity-Experten, die aus Kosten und Verfügbarkeitsgründen nur die wenigsten Organisationen intern vorhalten können.
Dass diese Grundpfeiler für eine moderne Cybersecurity-Strategie oftmals noch Fehlanzeige sind, ist besonders besorgniserregend, wenn man bedenkt, dass 93% der Unternehmen laut der Sophos-Umfrage **„State of Cybersecurity in Business"** die Durchführung wesentlicher Sicherheitsmaßnahmen bereits als Herausforderung empfinden. Darüber hinaus sagen über die Hälfte der Befragten IT-Verantwortlichen, dass Cyber-Bedrohungen mittlerweile zu weit fortgeschritten sind, um sie als Unternehmen allein bewältigen zu können – eine ernüchternde Wahrheit.

Wie Unternehmen von Cybersecurity as a Service profitieren können

Die Lösung bietet sich in Form eines Cybersecurity-as-a-Service-Modells (CSaaS) in Kombination mit einem intelligenten Cybersecurity-Ökosystem an. In diesem Ökosystem kommunizieren alle relevanten Elemente, vom Endpoint bis zur Firewall, wodurch sowohl Prozesse automatisiert werden als auch einen großen Data Lake entsteht. Die Größe und der Umfang dieses Data Lake ist entscheidend, denn durch ihn ist die Analyse der Telemetriedaten nicht nur erheblich vereinfacht, sondern im Prinzip überhaupt erst möglich. So haben Unternehmen mit einem adaptiven Cybersecurity-Ökosystem in Kombination mit einem MDR-Service (Managed Detection and Response) eine flexible Möglichkeit, ihre Sicherheitsabläufe zukunftssicher zu gestalten und gleichzeitig starke Schutzschilde aufrechtzuerhalten.

Aktuelle Bedrohungslage in Europa

Im neuesten ENISA-Bericht, veröffentlicht im Oktober 2023, zur Cybersicherheit wird eine umfassende Analyse der Cyber-Vorfälle des Jahres 2023 vorgestellt. Welche Bedrohungstypen waren am aktivsten, und welche neuen Herausforderungen bringen diese für Unternehmen und Organisationen?

Abbildung 4. ENISA – https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

AI kontrolliert einsetzen – Trustworthy AI, Controllable AI und Beschaffung sicherer AI

Hintergrund

Datengesteuerte Anwendungen spielen eine immer wichtigere Rolle in unserem Leben und durchdringen immer mehr Aspekte unserer Routine. In den kommenden Jahren werden KI-basierte Systeme alltäglich werden und in Anwendungen zum Einsatz kommen, die wir täglich nutzen. Neben all den Chancen, die sie bieten, stellen diese Systeme jedoch auch eine Reihe von sicherheitsrelevanten Herausforderungen dar, insbesondere im Hinblick auf die mangelnde Transparenz, zu der auch das sogenannte Erklärbarkeitsproblem gehört. In den letzten Jahren und insbesondere seit Chat-GPT für Aufmerksamkeit in der Öffentlichkeit gesorgt hat, ist das Interesse an der Frage gewachsen, wie die Gesellschaft vor den Nachteilen und Gefahren geschützt werden kann, die sich aus dem allgegenwärtigen Einsatz von KI ergeben. Dieses Interesse hat dazu beigetragen, eine Diskussion anzustoßen, die in den letzten Jahren an Dynamik gewonnen hat. Darüber hinaus nähert sich der AI-Act der Europäischen Union, an dem schon seit geraumer Zeit gearbeitet wird, seiner Vollendung. Dieser wird nicht nur den Grundstein für einen gemeinsamen Markt für KI-basierte Systeme in der EU legen, sondern auch die Vorschriften für das Inverkehrbringen von KI festlegen, insbesondere im Hinblick auf KI-Anwendungen, die entweder verboten oder als sehr riskant eingestuft werden. Die vertreibenden Unternehmen müssen in der Lage sein, ein Risikomanagement durchzuführen, und sie müssen ihre KI so transparent wie möglich gestalten, um die aus ihnen resultierenden potenziellen Gefahren zu verringern.

Trustworthy Artificial Intelligence

Der Begriff der „Trustworthy AI" (vertrauenswürdige KI) wurde entwickelt, um die Entwicklung der KI besser mit Anforderungen an Sicherheit und Zuverlässigkeit in Einklang zu bringen. Der Begriff ist allerdings nicht einheitlich, es existieren hierzu unterschiedlichen Definitionen. Die beiden wichtigsten sind die der High-Level Expert Group (HLEG) der Europäischen Kommission[1] und die des National Institute of Standards and Technology [2] (NIST), die beide viele Gemeinsamkeiten, aber auch einige wichtige Unterschiede aufweisen.

Die sog. „key requirements" der HLEG-Definition umfassen dabei (1) Human Agency and Oversight, (2) Technical robustness & Safety, (3) Privacy & Data Governance, (4) Transparency, (5) Diversity, non-discrimination & fairness, (6) Environmental & social wellbeing and (7) Accountability. Die NIS-Definition betrachtet im Gegensatz dazu sieben sog., „characteristics": (1) Valid & reliable, (2) Safe, (3) Secure & resilient, (4) Accountable & transparent, (5) Explainable & interpretable,[3] (6) Privacy-enhanced und (7) Fair with harmful bias managed. Beide Definitionen gehen damit in eine ähnliche Richtung, aber die von der HLEG entwickelte Definition schließt auch das Wohlergehen von Umwelt und Gesellschaft (Nummer 6) als Anforderung ein. Dies muss diskutiert werden, da es sich nicht um eine technische, sondern um eine moralische oder philosophische Anforderung handelt, die es schwierig macht, Dinge wie vertrauenswürdige militärische Anwendungen zu definieren. Der wichtigste Unterschied zwischen den beiden Definitionen ist jedoch das Erfordernis der Erklärbarkeit, das ausdrücklich im fünften Merkmal der NIS-Definition genannt wird, zusammen mit mehreren anderen Anforderungen und Merkmalen, insbesondere denjenigen, die sich auf Voreingenommenheit, Nichtdiskriminierung, Rechenschaftspflicht und Transparenz beziehen. Diese Explizitheit der Forderung ist ein wichtiger Unterschied zwischen den beiden Definitionen, auch wenn die anderen Anfor-

FORTSETZUNG NÄCHSTE SEITE »

1 High-Level Expertgroup 2019. Ethics guidelines for trustworthy AI (released April 8, 2019) [Online]. European Union. Available: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

2 Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0)

3 Holzinger, A. (2018). Explainable AI. In Informatik-Spektrum, 41(2), S. 138ff. https://doi.org/10.1007/s00287-018-1102-5
Holzinger, A. (2018). Interpretierbare KI: Neue Methoden zeigen Entscheidungswege künstlicher Intelligenz auf. In c't Magazin für Computertechnik, 22, S. 136ff.

AUTOR:INNEN

Dr. Andreas Holzinger
Univ.-Prof. für Digitale Transformation, Leiter Human-Centered AI Lab
Universität für Bodenkultur (BOKU) Wien

DI. Peter Kieseberg
Senior Researcher
Fachhochschule St. Pölten

FH-Prof. Mag. Dr. Simon Tjoa
Institut für IT Sicherheitsforschung, Institutsleiter
Fachhochschule St. Pölten

Hauptanforderungen Controllable AI:

1. Wir müssen Kontrollen einrichten, die erkennen können, wenn ein KI-System übermäßig von dem Verhalten abweicht, das es zeigen soll.

2. Wenn ein solches unangemessenes Verhalten festgestellt wird, müssen wir Verfahren einführen, um das System neu zu kalibrieren oder es ganz abzuschalten.

derungen zumindest teilweise Explainability bedingen.

Darüber hinaus stellt die Gewährleistung von Sicherheit eine Herausforderung für viele Algorithmen des maschinellen Lernens dar. Dies liegt daran, dass Probleme mit der Emergenz und der Nicht-Erklärbarkeit es schwierig machen, normale Techniken für Sicherheitstests zu verwenden, insbesondere für solche, die komplexe neuronale Netzwerke mit Techniken des Reinforcement-Learnings aufweisen, wie z. B. ein „doctor in the loop"-Ansatz bei der Krebserkennung. Dennoch sind dies die spannenden Anwendungen für KI, die die technologischen Triebkräfte für die kommenden Jahre sein werden.

Controllable Artificial Intelligence

Die beiden genannten Definitionen für Vertrauenswürdigkeit von AI stehen in starkem Gegensatz dazu, wie wir den menschlichen Entscheidungsprozess behandeln: Da so viele unserer Entscheidungen das Ergebnis unbewusster Prozesse sind, können wir meist nicht sagen, wie wir zu spezifischen Schlussfolgerungen kommen. Trustworthy AI verlangt daher von KI mehr als wir das typischerweise von Menschen erwarten, denn bei Letzteren wollen wir in der Regel nur kontrollieren, ob ein Entscheidungsprozess im Großen und Ganzen korrekt ist, und falls nicht, sicherstellen, dass er entweder korrigiert wird oder dass die Person, die sich geirrt hat, Konsequenzen tragen muss. Dies können wir einfach in das Konzept der „kontrollierbaren KI"[4] (Controllable AI) umwandeln, mit den folgenden zwei Hauptanforderungen:

1. Wir müssen Kontrollen einrichten, die erkennen können, wenn ein KI-System übermäßig von dem Verhalten abweicht, das es zeigen soll.
2. Wenn ein solches unangemessenes Verhalten festgestellt wird, müssen wir Verfahren einführen, um das System neu zu kalibrieren oder es ganz abzuschalten.

Das grundlegende Konzept der kontrollierbaren künstlichen Intelligenz (Controllable AI) ist daher die Annahme, dass kein KI-System als zuverlässig angesehen werden sollte und dass es unbedingt notwendig ist, Methoden zu entwickeln, um Fehler zu erkennen und die Kontrolle wiederzuerlangen. In dieser Definition wird keine Erklärbarkeit gefordert, da nicht erklärt werden muss, wie und warum das System zu einer richtigen oder falschen Schlussfolgerung gelangt ist, sondern nur die Erkennung von Schlussfolgerungen, die zu weit vom richtigen Verhalten entfernt sind. Explainability ist eine Eigenschaft, die nicht erforderlich ist. Zum Vergleich: Viele Funktionen des menschlichen Verdauungssystems werden von Wissenschaftlern noch immer nicht vollständig verstanden, und vom Durchschnittsmenschen noch weniger. Andererseits sind viele größere Defekte für jedermann anhand der Reaktionen seines Körpers sofort erkennbar.

Die Ansätze für die Entwicklung einer kontrollierbaren KI sind vielfältig und müssen an die Anforderungen des jeweiligen Systems angepasst werden. Darüber hinaus ist es besonders wichtig, die Annahme von Fehlern in den Entwurf des Systems selbst einzubeziehen. Das bedeutet, dass kontrollierbare künstliche Intelligenz nicht nur eine Sammlung von Techniken ist, die auf das Endprodukt angewandt werden können, sondern vielmehr eine Entwurfsphilosophie für KI-Systeme, ähnlich wie „Privacy by Design" oder „Cyber Resilience".

AI und Security im Beschaffungsvorgang

Grundsätzlich müssen wir, wie oben schon angedeutet, davon ausgehen, dass mit der weitläufigen Einführung von AI in Systeme des täglichen Lebens, dies in vielen Fällen von Nicht-Expert*innen durchgeführt wird. Dies bedeutet, dass AI, ich welcher Form auch immer, ob als fertige API für einen bestimmten Zweck, als vortrainiertes Modell oder als extern angebundener Service, angekauft wird. Durch die Schwierigkeit des Security-Testings wird es nicht möglich sein, für jede Commodity-App weitreichende Tests durchzuführen, es wird daher auf Informationen von Lieferantenseite vertraut werden müssen. Die Berücksichtigung von AI-spezifischen Security-Anforderungen und Eigenheiten ist daher im Beschaffungsprozess zu berücksichtigen. Zu diesem Zweck wurde ein

4 Kieseberg, P. et al. (2023). Controllable AI-An Alternative to Trustworthiness in Complex AI Systems?. In International Cross-Domain Conference for Machine Learning and Knowledge Extraction, S. 1ff. Cham: Springer Nature Switzerland, 2023

Leitfaden entwickelt,[5] der eine Vielzahl wichtiger Fragen und Anforderungen in leicht verständlicher und nutzbarer Form berücksichtigt. Dieser Leitfaden dient dazu, auf der einen Seite den Beschaffungsprozess zu strukturieren und wichtige Fragen frühzeitig zu stellen, auf der anderen Seite die Kompetenz des Gegenübers auf Verkäuferseite abzuschätzen. Er ist nicht in der Lage zu bestimmen, ob ein bestimmtes System sicher ist oder nicht, oder ob die Anwendung von KI überhaupt die geeignete Antwort auf eine bestimmte Herausforderung ist. Der Leitfaden stellt dabei eine Reihe von Fragen zur Verfügung, die es ermöglichen, (1) festzustellen, ob ein Produkt auf grundlegenden Sicherheitsüberlegungen beruht, (2) wie wesentliche Fragen wie die Kontrolle über Daten und Modelle, Patching und ähnliches gehandhabt werden und (3) ob ein geeigneter Ansprechpartner zur Verfügung steht, der solche Fragen sinnvoll und korrekt beantwortet. Mit diesem Ansatz kann der Beschaffungsprozess sowohl in der ersten Auswahlphase als auch in einer anschließenden Überprüfungsphase deutlich schlanker und effizienter gestaltet werden. Zudem können ungeeignete Systeme und/oder Ansprechpartner frühzeitig aus dem Auswahlprozess ausgeschlossen werden.

Der Leitfaden ist in Abschnitte gegliedert, die als „Aspekte“ bezeichnet werden und sich jeweils auf einen bestimmten Themenbereich konzentrieren, der auf eine bestimmte Anwendung anwendbar sein kann oder auch nicht und mit einer Gruppe von Indikatoren verbunden ist. Diese umfassen bspw. Aspekte wie Datenschutz, Prüfung und Kontrolle sowie Kontrolle über den Quellcode. Für jedes Element wird eine Sammlung von Fragen und Unterfragen bereitgestellt, die wichtige Aspekte der Sicherheit und Kontrolle abdecken. Ein Ausschnitt aus einem dieser Fragenblöcke ist in Abbildung 1 dargestellt, wobei der Schwerpunkt auf der Verfügbarkeit des Quellcodes und/oder der Reproduzierbarkeit des erstellten Programms liegt. Andere Merkmale, insbesondere diejenigen, die sich auf die Kontrolle von Daten und Modellen konzentrieren, enthalten ein gewisses Maß an Redundanz, um die Nutzung zu verbessern und zu vereinfachen, ohne die Vorbereitungsphase für ein Interview wesentlich zu belasten.

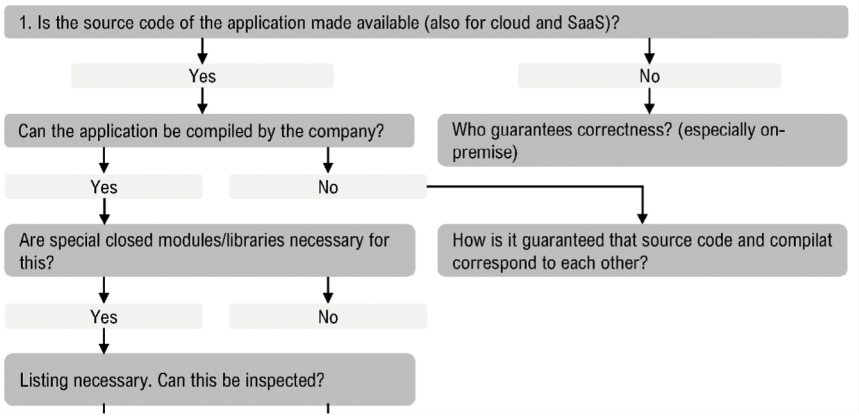

Abbildung 5. Beispielfragen zur Verfügbarkeit von Quellcode

Das Handbuch kann unter **www.secureai.info** kostenlos heruntergeladen werden und steht ohne Einschränkungen zur freien Verwendung zur Verfügung. Derzeit arbeiten wir an einer neuen Version, die bereits eine beträchtliche Menge an zusätzlichen Eingaben enthält, die aufgrund der wachsenden Fähigkeiten von Chatbots und anderen kürzlich entwickelten Apps sowie aufgrund von Verbesserungen in der Regulierungspolitik notwendig geworden sind. Da sich das KI-Gesetz jedoch derzeit noch im Entwurfsstadium befindet, gehen wir davon aus, dass diese speziellen Teile in naher Zukunft eine Reihe von Überarbeitungen erfahren werden.

Fazit und Ausblick

Grundsätzlich ergeben sich durch die immer ausgereifteren Methoden der AI viele neue Anwendungsgebiete und großer Nutzen für die Gesellschaft, allerdings muss AI kontrollierbar gemacht werden. Dies gilt nicht nur für die Erkennung von schlechtem Verhalten, sondern impliziert auch die Möglichkeit, auf gewisse Fähigkeiten der AI in einem System notfalls verzichten zu können. Derzeit arbeiten wir daran, den Ansatz der Controllable AI mit den neuen Regularien auf europäischer Ebene in Einklang zu bringen.

Auch in Bezug auf den Beschaffungsleitfaden arbeiten wir an einer neuen Version, die bereits eine beträchtliche Menge an Feedback berücksichtigt. Da sich der AI-Act jedoch derzeit noch im Entwurfsstadium befindet, gehen wir davon aus, dass diese gewisse Teile in naher Zukunft eine Reihe von Überarbeitungen erfahren werden.

5 Kieseberg, P., Buttinger, C., Kaltenbrunner, L., Temper, M., Tjoa, S. (2022). Security considerations for the procurement and acquisition of Artifi cial Intelligence (AI) systems. In 2022 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), S. 1ff. IEEE.

Anwendungssicherheit durch einen sicheren Softwareentwicklungslebenszyklus (SDLC)

AUTOR:INNEN
Mag. Stefan Jakoubi
Geschäftsleiter Professional Services
SBA Research

AUTOR
Dipl.-Ing. Michael Koppmann
Senior Information Security Consultant
SBA Research

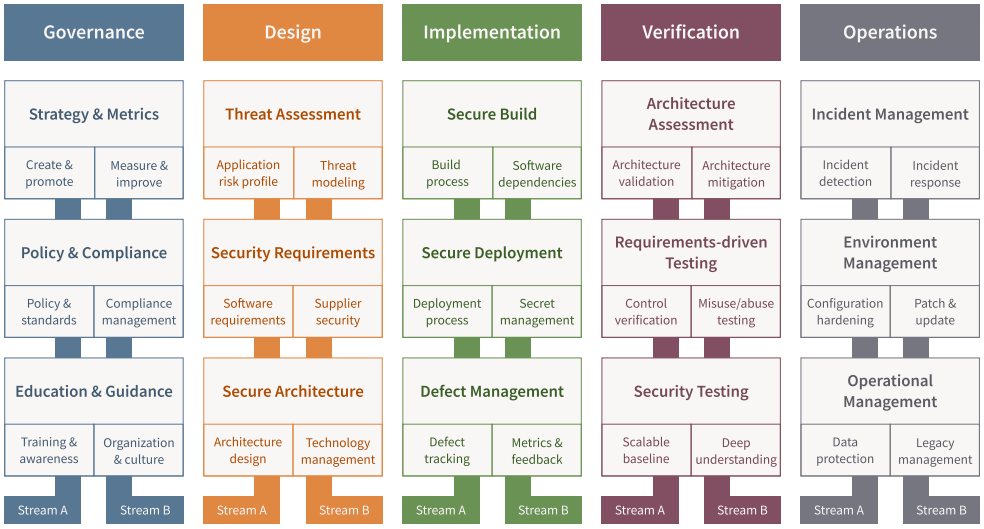

Abbildung 6. Diagrammdarstellung[3] des SAMM

Sicherheitsschwachstellen in Softwareprodukten namhafter Hersteller sind medial sehr präsent. Solche Neuigkeiten haben die Chance, bis in die Top-Managementebenen vorzudringen. Zu den gravierendsten und, durch ihre Tragweite, in höchsten Unternehmensebenen bekannten Schwachstellen zählten in den letzten Jahren „Log4Shell“[1] und der „Solarwinds-Hack“.[2] Die notwendigen akuten Notfallmaßnahmen verursachten Kosten in Höhe von Personenmonate bis -jahre (in entsprechend softwarelastigen Umgebungen).

Gegenmaßnahmen zu spezifischen Schwachstellen stellen meist gute Symptomlösungen dar, gehen aber der Ursache nicht auf den Grund. Möchte man in eine nachhaltige Grundlage für die Entwicklung sicherer Softwareanwendungen investieren, lohnt sich die Integration von Sicherheitsbewusstsein in alle Phasen des Software-Lebenszyklus. Sicherheit wird somit ein Kernbestandteil des Produkts, von der Zeit der initialen Planung, bis hin zur Auslieferung und weiterfolgenden Pflege und Wartung. Dieser Softwareentwicklungslebenszyklus ist in der Industrie als Software Development Life Cycle (SDLC) bekannt.

Für die Annäherung an einen SDLC empfehlen wir die Auseinandersetzung mit dem OWASP Software Assurance Maturity Model (SAMM[4]). Dessen Ziel ist es eine wirksame Methode zur Analyse und Verbesserung des sicheren Softwareentwicklungslebenszyklus zu bieten. Dabei unterstützt das SAMM den gesamten Software-Lebenszyklus und ist technologie- und prozessunabhängig. Das Modell ist entwicklungs- und risikoorientiert, um für eine große Anzahl verschiedener Unternehmen geeignet zu sein.

Alle Softwaresicherheitsaktivitäten werden in fünf sogenannte business functions gegliedert, die wiederum fünfzehn security practices beinhalten. Die konkreten Sicherheitsaktivitäten sind in den streams der security practices beschrieben. Jede Sicherheitsaktivität ist in drei Reifegrade eingeteilt, wobei jeder Reifegrad konkret mit Merkmalen beschrieben wird, sodass ein Benchmarking gut gelingt. Abbildung 6 zeigt das Model mit allen business functions, security practices und streams.

Die fünf business functions in aller Kürze zusammengefasst:

1) Governance: Strategische Aspekte des Sicherheitsprogramms, von Schutzbedarfsfeststellung über Maßnahmenmanagement, Metriken, Compliance bis zu Ausbildungen und Schulungen.

2) Design: Erstellen des Sicherheitsprofils über ein solides Bedrohungsmodell und die

1 https://www.bsi.bund.de/dok/log4j
2 https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/
3 https://owaspsamm.org/img/pages/SAMM_v2_diagram.svg
4 https://owaspsamm.org/

darauf basierende Ableitung von Sicherheitsanforderungen und der entsprechend sicher gestalteten Softwarearchitektur.
3) Implementation: Konkrete Umsetzung der „vorhergehenden sicheren Planungsphasen" vom Testen über das Bauen bis hin zur Verteilung der Software im Produktivsystem. Ein entsprechend laufendes Issue-Tracking-System ist der Schlüssel für kleine aber äußerst effektive Verbesserungszyklen.
4) Verification: Jegliche qualitätssichernden Maßnahmen von Assessments der Softwarearchitektur über automatisierte Verifikation von Testfällen bis hin zum klassischen Penetrationstest.
5) Operations: Sichere Ausgestaltung der Produktivumgebung inklusive Vorbereitungen auf den Sicherheitsvorfall oder auch -notfall.
OWASP stellt ein fertiges Exceldokument für ein Assessment (SAMM-Toolbox[5]) bereit. Im Zuge der Beurteilung wird für jede security practice ein Reifegradwert ermittelt, welcher für eine weiterführende Kommunikation grafisch aufbereitet ist. Dieses Dokument inkludiert aber auch eine Meilensteinplanung, mit der eine solide Aufteilung des Programmes für Anwendungssicherheit in mehrere Phasen – beispielsweise Halbjahre – auf einfache aber klar strukturierte Weise unterstützt wird. Unternehmen, die noch einen niedrigen SDLC-Reifegrad vorweisen, profitieren am meisten von einer strukturierten Einführung eines Programmes für Anwendungssicherheit. Ein solches Programm beinhaltet für gewöhnlich Interviews, Schulungen und Tests zu den Bereichen: Schutzbedarfsfeststellung, Compliance, Bedrohungsanalyse, Architekturanalyse, Automatisierung und Härtungsmaßnahmen, Penetrationstests, sowie Protokollierung und Überwachung des Softwarebetriebs.
In weiterer Folge wird somit das Verständnis über das eigene Unternehmen und interne Abläufe vertieft und klärt Fragen wie: Wie erschaffe ich eine gelebte Kultur für Anwendungssicherheit? Welche Sicherheitsanforderungen sollte meine Softwarearchitektur erfüllen? Wie bewerte ich gefundene Sicherheitsdefekte langfristig? Wie balanciere ich den Einsatz von automatischen Werkzeugen und manuellen Penetrationstests? Wie sollte ein formaler Prozess bei Cybersicherheitsvorfällen definiert sein?
Es empfiehlt sich, solche Assessments mit Hilfe von externen Berater:innen durchzuführen. Deren Mentoring erleichtert das Verständnis von Themen, zu denen bisher wenige Berührungspunkte bestanden haben. Somit kann der Fokus auf wesentliche Punkte entlang des strategischen Fahrplans gelegt werden.
Zusammenfassend ist ein Blick auf das OWASP SAMM sehr lohnend. Die Art und Weise, wie OWASP das Model dokumentiert, macht es nicht nur für Sicherheitsexpert:innen einfach, sich mit der Materie der Anwendungssicherheit beziehungsweise eines SDLC auseinanderzusetzen, und erlaubt somit die Zusammenarbeit über mehrere Abteilungen hinweg.

Exkurs OWASP

Das Open Worldwide Application Security Project (OWASP[6]) ist eine gemeinnützige Stiftung, die sich für die Verbesserung der Softwaresicherheit einsetzt. Durch diese Gemeinschaft mit über zehntausend Mitgliedern – aufgeteilt in hunderten lokalen Chaptern – entstanden unzählige Open-Source-Softwareprojekte und Ressourcen, die für alle frei zur Verfügung stehen.
Das OWASP-Top-10-Projekt[7] ist das bekannteste Werk, welches die zehn kritischsten Sicherheitsrisiken adressiert und mittlerweile nahezu Standard in Vertragswerken geworden ist.
Für fortgeschrittene Unternehmen, die bereits mit der sicheren Softwareentwicklung vertraut sind, ist der OWASP Application Security Verification Standard (ASVS[8]) ein Muss. Dieser Standard bietet eine Ansammlung an Anforderungen und Tests an die Anwendungssicherheit an. Entwickler:innen, Architekt:innen und andere Expert:innen können diese als Grundlage für ihre weiterführende Arbeit nutzen, um die Sicherheit der von ihnen betreuten Softwareprojekte zu verbessern.

5 https://github.com/owaspsamm/core/releases/download/v2.0.8/SAMM_spreadsheet.xlsx

6 https://owasp.org/
7 https://owasp.org/Top10/
8 https://owasp.org/www-project-application-security-verification-standard/

Exemplarische Probleme aus der Cyberversicherung im Zusammenhang mit Homeoffice

AUTOR:IN
Mag. Lisa Katharina Promok
Leiterin Forschungsinstitut für Privatversicherungsrecht Paris Lodron Universität Salzburg

I. Ausgangssituation

A. Arbeitsrechtliche Fragestellungen[1]

Der folgende Beitrag widmet sich der Versicherungsperspektive mit Fokus auf die Cyberversicherung. Die Erwähnung arbeitsrechtlicher Problemfelder dient nur der Sensibilisierung und lediglich als Hinweis, dass es sich in diesem Aufsatz keinesfalls um eine allumfassende Problemaufarbeitung iZm dem Terminus Homeoffice handelt. Die Fragestellungen werden unabhängig vom geltenden Arbeitsrecht und sonstigen Rechtsmaterien vorwiegend auf versicherungsrechtlicher Ebene untersucht.

II. Cybergefahren: Eine kurze Analyse

Wenn man über Cybergefahren spricht, bringt das Homeoffice mit Sicherheit ein zusätzliches Risiko aufs Tapet. Cybergefahren bzw Cyberrisks können vielfältig sein, darunter fallen klassische Cyberattacken, Data Breach, Phishing, DoS- und Fake President Fraud oder Ransomware, um nur einige zu nennen[2]. Vor Cyberattacken kann man sich rechtlich per se nicht schützen, doch durch den Abschluss einer Cyberversicherung könn(t)en die Folgen einer solchen minimiert werden. Je nach Ausgestaltung und Deckungsschutz der jeweiligen Cyberversicherungspolizze. Von der Arbeitgeberseite bzw Unternehmerseite aus betrachtet, bringt das Homeoffice jedenfalls zahlreiche Risiken in puncto Cybersecurity mit sich. Sowohl das Bundeskriminalamt (AUT) als auch das Bundesamt für Cybersicherheit (GER) hat seit Beginn der Pandemie eine Zunahme an Cyberkriminalität verzeichnet. Größtenteils handelt es sich um Frequenzschäden, bei denen vorrangig Datenschutzeingriffe erfolgen und daraus resultierend Kosten für IT-Forensik, Datenwiederherstellung und auch Betriebsunterbrechung entstehen. Vermehrt treten auch Cyberangriffe mit Lösegeldforderungen auf, die durchaus (existenzgefährdendes) Großschadenpotenzial bergen. Viele Unternehmen verfügen über Daten Back-ups, doch nicht nur die Unternehmen, auch die Cyberkriminalität wird professioneller und so gelingt es mittlerweile häufiger, gesamte

1 Weiterführende Gedanken dazu: In wie weit der Arbeitgeber den Arbeitnehmer bzw Dienstnehmer zur Verlegung der dienstlichen Tätigkeit in das Homeoffice verpflichten kann, ob und wenn ja, welche und wie Rahmenvereinbarungen zwischen Arbeitgeber und Arbeitnehmer abgeschlossen werden müssen, Spezialregelungen für Beamte (einzig das Beamten-Dienstrechtsgesetz BDG 1979 sah bereits vor dem Covid-19 Gesetz die Möglichkeit der Arbeitsausübung vom Wohnort aus, vor; siehe dazu § 36a BDG sowie § 5c VBG), der arbeitsrechtliche Terminus des Homeoffice, sozialrechtliche Folgen sowie die Rechtsfolgen bei unterlassener Homeoffice-Anweisung bzw Vereinbarung, sind allesamt interessante und aktuell dringliche Fragestellungen, denen es sich lohnt auf den Grund zu gehen, diese sind aber in weiterer Folge vom Arbeitsrecht zu beurteilen. Per 1.4.2021 trat das Homeoffice Maßnahmenpaket in Kraft, bis zu diesem Zeitpunkt regelte der österreichische Gesetzgeber Homeoffice nicht explizit, lediglich iZm der Covid-19 Pandemie wurden Regelungen dazu getroffen. Siehe auch näher dazu *Wetsch.* (2020). Rechtliche Rahmenbedingungen für die Arbeit im „Homeoffice". In Reichel, Pfeil & Urnik (Hrsg.), Die Arbeit ist immer und überall, S. 48f. Es handelt sich hierbei um kein eigenständiges, neues Gesetz, es werden lediglich bestehende Gesetze (AVRAG, ArbIG, ArbVG, DHG, ASVG/BKUVG und EStG; für weiterführende Informationen siehe dazu Felten, E. & Pfeil, W. 2020. In DRdA 4, S. 2f.) ergänzt bzw adaptiert. Diesem Maßnahmenpaket liegt prima vista kein umfassendes Gesamtkonzept zu Grunde. Das im Februar bzw April 2021 beschlossene Homeoffice-Gesetz entfaltet teilweise auch rückwirkende Geltung. Was Schäden an Arbeitsmitteln anbelangt, so soll ab April 2021 auch das Dienstnehmerhaftpflichtgesetz (DHG) im Homeoffice anwendbar sein. Schäden, die durch Kinder oder Haustiere des Arbeitnehmers verursacht werden, sind diesem zurechenbar. Ob und inwieweit dies auch auf Cyberrisiken anwendbar ist, bleibt fraglich bzw wird im Weiteren erörtert.

2 Weiterführend siehe dazu *Keltner, K.* (2018). Versicherbarkeit von Cyber Risiken und ausgewählte Abgrenzungsfragen der Sparten Cyber, Vertrauensschaden-, D&O- und Betriebshaftpflichtversicherung. In Berisha, Gisch & Koban (Hrsg.), Haftpflicht-, Rechtsschutz- und Cyberversicherung, S. 107ff.

Produktionskapazitäten konzernweit[3] anzugreifen[4]. Cyber-Bedrohungen[5], als weiter gefasster Begriff, unter den sich sämtliche idZ relevante Schadensszenarien und IT-Sicherheitsbedrohungen subsumieren lassen, nehmen somit tendenziell zu. Aufgrund dieser verzeichneten Zunahme wird häufig über den Nutzen von Cyberversicherungen diskutiert[6].

A. Die Cyberversicherung

Vom Verband der Versicherungsunternehmen Österreichs (VVO)[7] wurden im Jahr 2018 die sogenannten ABC 2018 Musterbedingungen für die Cyberrisiko-Versicherung erlassen sowie vom Gesamtverband der Deutschen Versicherungswirtschaft (GDV)[8] die AVB Cyber Bedingungen im Jahr 2017 ausgegeben. Die ABC 2018 (Österreich) orientieren sich an den AVB Cyber (Deutschland). In der Literatur existiert bis dato keine einheitliche Definition weder des Begriffs der Cyberrisiken noch der Cyberversicherung. Bis auf ein Urteil des LG Tübingen[9] sucht man Judikatur zum Thema Cyber im deutschsprachigen Raum vergebens. Die Cyberversicherung ist eine Kombination aus Sachversicherung und Haftpflichtversicherung. Dementsprechend inhomogen erfolgt die Verwendung des Begriffes Cyberversicherung. Auf Basis der Versicherungsfalldefinition in Art 1 der ABC 2018 spricht man von einer Cyberversicherung, wenn reine Vermögensschäden im Umfang der in Art 1 ABC 2018 beschriebenen Bestimmungen, die durch eine Informationssicherheitsverletzung verursacht worden sind, unter bestimmten Voraussetzungen gedeckt werden können. Es besteht prinzipiell die Möglichkeit eine Cyberversicherung als Privatperson abzuschließen, diese wird jedoch im Berufsleben keine Anwendung finden, da eine Versicherung zu privaten Zwecken, auch nur Risiken dieser Sphäre abdeckt. Sofern der Arbeitgeber eine Cyberversicherung abschließt, deckt diese nun Schäden iZm Homeoffice? Die Musterbedingungen sehen Homeoffice per se in keinem Artikel vor. Jedoch liegt bei Ausübung der Tätigkeit im Homeoffice regelmäßig eine Gefahrerhöhung iSd Art 6 ABC 2018 vor. Ein Umstand, den der VN[10] dem VU[11] unverzüglich melden muss, bei nichterfolgter Meldung kann der VU das Versicherungsverhältnis gem Art 6 2. ABC 2018 aufkündigen bzw ist gemäß den Voraussetzungen und Begrenzungen der §§ 23 bis 31 VersVG von der Verpflichtung zur Leistung frei. Lediglich die Musterbedingungen klammern Homeoffice gänzlich aus ihrem Regelungsgehalt aus. Am Markt – sowohl national als auch international – erhältliche Wordings gehen regelmäßig auf Homeoffice, Mobil Working oder Remote Access ein[12].

1. Gibt es eine Cyberversicherung für das Homeoffice?

Verbunden mit Homeoffice ergeben sich zahlreiche weitere Risiken, sowohl die

FORTSETZUNG NÄCHSTE SEITE »

3 An dieser Stelle beispielhaft zu erwähnen, ist der Cyberangriff im Jahr 2014 auf ein deutsches Stahlwerk. Die Angreifer beschädigten dabei einen Hochofen, verschafften sich Zutritt zu den Steueranlagen und manipulierten diese. Dadurch kam es zu Schäden an der Anlage, welche ein geregeltes Herunterfahren des Hochofens unmöglich machten; im Ergebnis wurde die gesamte Anlage schwer beschädigt und es entstand ein Schaden in Millionenhöhe; näheres dazu siehe Sicherheitsbericht des BSI – Cyber-Angriff auf deutsches Stahlwerk | Informatik Aktuell (informatik-aktuell.de) sowie Cyber-Angriff auf Stahlwerk: Hacker bringen Hochofen unter ihre Kontrolle - n-tv.de (Download am 30.4.2021).

4 *Malek & Zürn. (2021). Aktuelle Herausforderungen im Umgang mit Ransomare-Angriffen. In Die Versicherungspraxis 3(3)* Bundeskriminalamt, Überblick Kriminalitätsentwicklung 2020 (bundeskriminalamt.at) (Download am 30.4.2021).

5 Siehe auch *Pache, T.* (2019). Cyberversicherung für Vermittler. S. 3f.

6 Zu Cybergefahren siehe auch näher *Promok, L.* (2023). Cyberversicherung. S. 53f.

7 Der Verband der Versicherungsunternehmen Österreichs (VVO) mit Sitz in Wien vertritt die Interessen aller in Österreich tätigen privaten Versicherungsunternehmen und bietet seinen 126 Mitgliedern Unterstützung bei rechtlichen, steuerlichen, wirtschaftlichen und internationalen Angelegenheiten. Weitere Informationen dazu abrufbar unter https://www.vvo.at/vvo/vvo.nsf/sysPages/internationales.html (zuletzt aufgerufen am 7.11.2023).

8 Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat seinen Sitz in Berlin und es handelt sich dabei um die Dachorganisation der privaten Versicherer in Deutschland mit rund 460 Mitgliedern.

9 LG Tübingen, 26.05.2023 – 4 O 193/21.

10 Versicherungsnehmer.

11 Versicherungsunternehmen bzw Versicherungsunternehmer.

12 Zu den Charakteristika der Cyberversicherung siehe *Promok, S. 54f.*

Risiken des Privatbereichs als auch des beruflichen Alltags sind zu thematisieren.

a) Das versicherte Risiko – der Cyberangriff

Ein zentraler Begriff der Musterbedingungen ist die Informationssicherheitsverletzung[13]. Art 1 2.2. ABC 2018 definiert das versicherte Risiko. Eine Informationssicherheitsverletzung ist versichert, wenn sie durch Angriffe auf elektronische Daten, unberechtigte Zugriffe auf elektronische Daten, unberechtigte Eingriffe in *informationsverarbeitende Systeme,* eine Handlung oder Unterlassung die Datenschutzverletzung auslöste oder durch Schadprogramme hervorgerufen wurde. Eine Definition des Begriffes informationsverarbeitendes System wird weder in den ABC 2018 noch in den AVB Cyber[14] vorgenommen. Der Begriff ist weder ein Fachbegriff noch ein Rechtsbegriff und wird auch nicht anhand des allgemeinen Sprachgebrauchs definiert. Die Auslegung hat hier wohl anhand weiterer Regelungen zu erfolgen, möglichweise anhand der Obliegenheiten, die in Art 9 ABC 2018 umschrieben werden. Die Auslegung welche Szenarien versichert sind und welche nicht versichert sind, ist ebenfalls komplexer Natur. Eine systematische Auslegung empfiehlt sich mE hier nicht, denn braucht es wirklich immer einen zielgerichteten Angriff gegen die Funktionsfähigkeit des IT-Systems des VU? Soferne Fehler durch Angestellte erfolgen, oder ein Angriff von innen erfolgt, werden wohl besondere Regelungen notwendig sein. Art 2 2. ABC 2018 definiert den Risikoausschluss, für den Fall, dass Schäden infolge eines teilweisen oder gänzlichen Ausfalls oder einer Störung der Dienstleistung eines für den VU tätigen externen Dienstleisters entstehen. Besteht hier möglicherweise ein Widerspruch zu dem vorhin erwähnten versicherten Risiko?[15]

2. Obliegenheiten gem. § 6 Abs 2 VersVG, angepasste Sicherheitseinrichtungen und Stand der Technik

Kaum ein Versicherungsprodukt ist derart an den technischen Fortschritt geknüpft und somit auch dementsprechend fehleranfällig. Es erscheint - völlig zurecht - bloß ein Hinterherhinken der Bedingungen an den technischen Fortschritt vorzuliegen. Im Lichte dies § 6 Abs 2 VersVG[16] findet man in den Musterbedingungen unter Art 9 ABC 2018 termini wie: *Informationssicherheitsverletzung, technisch einwandfreier und betriebsfähiger Zustand, nicht über das technisch zulässige Maß, angepasste Sicherungseinrichtung, ausreichend komplexe Passwörter, zusätzlicher Schutz gegen unberechtigte Zugriffe, zusätzliche Schutzmaßnahmen, spezifische Sicherheitsrichtlinie, schutzbedürftige E-Mails.*[17] Die Auslegung dieser einzelnen Begriffe und die Auslegungsunterschiede bzw Differenzierungskriterien was den B2B oder B2C Bereich anbelangt, sind erörterungswürdig, doch werden an dieser Stelle ausgelassen. Problematisch ist jedenfalls, dass jeder Anwender/Leser, sei er nun Konsument[18] oder Unternehmer unterschiedliches (Vor) Wissen hat, einen unterschiedlichen Maßstab anlegt und die Begriffe somit anders interpretiert und sich damit einhergehend unterschiedlich in der virtuellen Welt verhält. Was kann man vom Endnutzer verlangen bzw welches Fehlverhalten ist diesem vorwerfbar? Mit sogenannten Stand der Technik Klauseln wird der *User* rechnen müssen. Der Stand der Technik ist ebenso ein auslegungsbedürftiger Begriff, der per se nicht definiert ist. Es kann sich hier aufgrund gesetzlicher Verweise eine Präzisierung ergeben oder der Stand

13 Siehe hierzu auch *Kath, W.* (2019). Die Cyberversicherung. In ZVers 3, S. 114.

14 Die vom Gesamtverband der Deutschen Versicherungswirtschaft (GDV) ausgegebenen allgemeinen Bedingungen für die Cyberrisiko-Versicherung (AVB Cyber) aus dem Jahr 2017. Dieses Bedingungswerk befindet sich aktuell in einer Überarbeitungsphase und wird voraussichtlich Ende 2023 bzw Anfang 2024 neu veröffentlicht.

15 Zum versicherten Risiko in der Cyberversicherung siehe auch *Promok, S. 56.*

16 § 6 (2) VersVG „Ist eine Obliegenheit verletzt, die vom Versicherungsnehmer zum Zweck der Verminderung der Gefahr oder der Verhütung einer Erhöhung der Gefahr dem Versicherer gegenüber - unabhängig von der Anwendbarkeit des Abs. 1a - zu erfüllen ist, so kann sich der Versicherer auf die vereinbarte Leistungsfreiheit nicht berufen, wenn die Verletzung keinen Einfluss auf den Eintritt des Versicherungsfalls oder soweit sie keinen Einfluss auf den Umfang der dem Versicherer obliegenden Leistung gehabt hat."

17 Siehe dazu auch *Kath, S. 122.*

18 Zwischenzeitlich gibt es Cyberversicherungspolizzen auch für Private, diese bilden allerdings einen geringen Prozentsatz des Marktes ab.

der Technik kann als nicht näher definierter unbestimmter Rechtsbegriff angesehen werden.[19] Der Stand der Technik ist keine Rechtsvorschrift, aber ist in der Praxis von großer Relevanz. Häufig beschreiben/determinieren technische Regelwerke den Stand der Technik; dies hat allerdings nicht zwingend so zu sein. In der Informationstechnik versteht man unter dem Stand der Technik, die zum jeweiligen Zeitpunkt aktuellen technischen Möglichkeiten zur Problem- oder Aufgabenlösung, auf der Grundlage des Stands von Wissenschaft und Forschung[20]. Dies resultiert aus der gebräuchlichen Begriffsverwendung in Literatur und Praxis[21]. Der Stand der Technik bedürfte durchaus einer weiteren Untersuchung, diese wird allerdings nicht vorgenommen, da dies den Rahmen eines Aufsatzes bei weitem sprengen würde.

Was die Obliegenheiten des VN anbelangt, so wird dieser, neben den bereits genannten, dem Versicherer mitteilen müssen, dass ein Teil der Belegschaft die geschuldete Dienstleistung im Homeoffice erbringt, da die Verlagerung der Tätigkeit ins Homeoffice eine Gefahrerhöhung gemäß §§ 23 Abs 2 und 27 Abs 2 VersVG nach sich zieht. Die Verlagerung ins Homeoffice stellt nicht nur eine unerhebliche Gefahrerhöhung gemäß § 29 VersVG dar.[22] Die Meldung darüber hat unverzüglich zu erfolgen, muss jedoch, sofern bei Abschluss der Cyberversicherung noch keine Mitarbeiter im Homeoffice gearbeitet haben und dies auch nicht angedacht war, nicht schon bei Vertragsabschluss[23] erfolgen. Generell ist in der Praxis der Trend zu mehr Eigenschäden[24] erkennbar. ME ist die Tendenz in puncto Eigenschäden mit vermehrten Homeoffice Tätigkeiten stark steigend.

19 Sie dazu *Saria, G.* (2007). Grundsätzliches zum „Stand der Technik" aus rechtswissenschaftlicher Sicht. S. 27ff.

20 Im englischsprachigen Raum wird hier gerne von „state of the art" gesprochen.

21 *Saria, S. 88.*

22 Siehe dazu auch OGH 14.6.2020 7Ob 285/99h; 5.5.2010, 7Ob 34/10s; siehe hierzu des weiteren *Kath,* ZVers 2019, 123.

23 Vgl § 16 VersVG.

24 Sogenannte Allrisk Cyberpolizzen decken lediglich Eigenschäden der Kunden ab, jedoch keine Drittschäden siehe dazu auch *Hillgraf, A.* (2019). Auf Sanierungskurs - auch in Cyber. In Zeitschrift für Versicherungswesen 18, S. 534.

Art 9 der Allgemeinen Bedingungen für die Cyberrisiko-Versicherung (ABC 2018) definiert die Obliegenheiten des Versicherungsnehmers vor Eintritt des Versicherungsfalls. Es handelt sich hierbei um die sogenannte Stand der Technik Klausel. Dieser Artikel umschreibt die technischen Anforderungen an den VN und verweist auf § 6 Abs 1, 1a und 2 VersVG. Es kommt somit bei Verletzung der geforderten Obliegenheiten zur Leistungsfreiheit des Versicherers. ME geht von Art 9 1. ABC 2018 die Verpflichtung aus, Softwareupdates sowie Treiber zu aktualisieren und Schutzmaßnahmen gegen Schadsoftware (Virenscanner) auf dem aktuellen Stand zu halten. Ein Mindestmaß an IT-Sicherheitsvorkehrungen wird jedem aktiven Nutzer zumutbar sein. Um bereits vorzugreifen, eine differenzierte Betrachtung des geschuldeten Verhaltens, ist durchaus sinnvoll. Ein Technologiekonzern, mit überdurchschnittlich besetzter IT-Abteilung wird mehr an Sicherheitsvorkehrungen leisten müssen bzw was digitale Sicherungsmaßnahmen anbelangt, größere Sorgfalt walten lassen müssen als der Zwei- Mann-Tischler-Betrieb. Den Zwei-Mann-Tischler-Betrieb wird man hier, trotz unternehmerischer Tätigkeit eher als Konsumenten behandeln und sein Handeln am B2C Maßstab messen. Man benötigt allerdings eine gewisse IT-Affinität und ein gewisses Maß an technischem Vermögen, was der durchschnittliche VN wohl hat, da bereits jedem PC-Nutzer bekannt ist, dass Updates notwendig sind, um digitale Sicherheit gewährleisten zu können. Dem durchschnittlichen Anwender ist bekannt, dass es Cyberattacken und Viren gibt und dass ein aktives Tun notwendig ist, um hier einfache Präventivmaßnahmen zu setzen.

3. Mehrfachversicherungen am Beispiel der D&O

Im Gegensatz zu den AVB Cyber regeln die ABC 2018 keine vorrangige Inanspruchnahme der Cyberversicherung. Für einen Vorrangschutz der Cyberversicherung spräche die Möglichkeit des sofortigen Tätigwerdens im Versicherungsfall, da gerade bei Cyberattacken jede Minute zählt um den Schaden möglichst geringhalten bzw beheben zu können. Eine vorrangige Deckung durch die Cyberversicherung wäre demnach nicht nur für den Versicherer, sondern auch den Versi-

FORTSETZUNG NÄCHSTE SEITE »

cherten von Vorteil und mE wünschenswert[25]. Außer Acht lassen, darf man in dieser Diskussion allerdings keinesfalls §§ 59 VersVG (Doppelversicherungsregime).

Greift eine Cyberversicherung bei Schäden im Fall der Homeoffice Anordnung seitens der Unternehmensleitung oder kann möglicherweise eine D&O[26] Versicherung als Ausfallsversicherung im Schadensfall herangezogen werden? A priori kann jedenfalls gesagt werden, die detaillierte Prüfung der jeweiligen Polizze bzw der einschlägigen Versicherungsbedingungen ist dringend empfohlen und bewahrt vor etwaigen Überraschungen.

Auf den Deckungsschutz der D&O-Versicherung möchte ich im Folgenden sogleich kurz eingehen. Bei der D&O-Versicherung handelt es sich um eine Passivversicherung, die nur im Schadensfall zum Tragen kommt, diese ist also was die Abwehr von Gefahren anbelangt, sinnbefreit. Im Schadensfall des Cyberangriffes wird die D&O meist keine Deckung gewähren, da der Versicherungsschutz der D&O laut A- 1 der Musterbedingungen[27] nur dann zur Anwendung gelangt, sofern ein Mitglied des Aufsichtsrates, Vorstandes oder der Geschäftsführung des Versicherungsnehmers oder einer Tochtergesellschaft (aktuell oder in der Vergangenheit für den VN tätig) aufgrund einer Pflichtverletzung während der Tätigkeitsausübung aufgrund gesetzlicher Haftpflichtbestimmungen für einen Vermögensschaden auf Schadenersatz in Anspruch genommen wird. Es kann also bereits an dieser Stelle die D&O-Versicherung zur Inanspruchnahme iZm einer Cyberattacke ausgeschlossen werden, da kein objektives Kriterium hierfür erfüllt ist[28].

Selbst wenn durch das Handeln eines Mitglieds des Vorstandes im Homeoffice (beispielsweise der illegale Download einer Musikdatei einer Filesharing-Tauschbörse[29], die bekanntermaßen gefährlich ist) eine Cyberattacke resultiert, kann die D&O-Versicherung mangels sämtlicher Tatbestandsmerkmale nicht zur Deckung herangezogen werden. Im soeben angesprochenen Fall, liegt weder eine Pflichtverletzung während der Ausübung der Tätigkeit vor, noch tritt aufgrund gesetzlicher Haftpflichtbestimmungen ein Vermögensschaden ein[30]. Zumal beinhalten D&O-Polizzen - wie auch die Musterbedingungen dies unter B4-1 AVB D&O Mehrere Versicherer, Mehrfachversicherung vorsehen - eine Subsidiaritätsklausel; eine Cyberversicherung würde in diesem Fall, immer vorrangig zur Deckung herangezogen werden, egal ob der Schaden in irgendeiner anderen Versicherung theoretisch mitabgegolten wäre[31].

Ein Szenario, dass mE in den Anwendungsbereich der D&O fällt, skizziert sich folgendermaßen: Der Geschäftsführer eines Unternehmens, der sich auch für die IT des Betriebs verantwortlich zeichnet, lässt nicht

25 Gegenteiliger Meinung *Kath, S. 125.*

26 Directors and Officers Liability Insurance. Vermögensschaden-Haftpflichtversicherung für fremde Rechnung für Organe und leitende Angestellte, Definition siehe *Ramharter, M. (2018). D&O-Versicherung : dogmatische Grundlagen und ausgewählte Praxisfragen. S. 6. Wien: Facultas.*, 6 sowie *Gruber, M., Mitterlechner, H., & Wax, T. (2012). D&O-Versicherung : mit internationalen Bezügen. S. 5f. München: Beck.*; *Hafner, M. & Perner, S. (2018). D&O-Versicherung: Struktur und Inhalt, In ZFR 8, S. 369*

27 Allgemeine Versicherungsbedingungen für die Vermögensschaden-Haftpflichtversicherung von Aufsichtsräten, Vorständen und Geschäftsführern (AVB D&O).

28 *Ramharter, S. 8.* sowie auch *Gruber, Mittlerlechner & Wax, S.8.*

29 Die Problematik von illegalen Downloads wird unter anderem hier angesprochen: online abrufbar unter https://www.arag.de/rechtsschutzversicherung/internet-rechtsschutz/tauschboersen-haftung-illegale-downloads/ sowie unter https://www.pwc.de/de/cyber-security/cyberangriffe-gegen-unternehmen-in-deutschland.pdf (Download am 17.3.2021).

30 Der Vollständigkeit halber sei darauf hingewiesen, dass wir uns möglicherweise im Anwendungsbereich des DHG befinden, da das DHG auch dann zum Zug kommt, wenn es sich - wie der OGH es formuliert – um „erlaubtes, übliches oder sozialadäquates Privatverhalten" handelt. Es gilt allerdings zu beachten, dass das DHG bspw auf Geschäftsführer einer GmbH keine Anwendung findet, da hierzu § 25 GmbHG die lex specialis darstellt; siehe hierzu *Reich-Rohrwig* in Straube/Ratka/Rauter, WK GmbHG § 25 (Stand 1.6.2015, rdb.at.). Das DHG kommt auch bei Vorständen von Aktiengesellschaften nicht zur Anwendung.

31 Zu den Musterbedingungen siehe *Fenyves, A., Koban, K. & Keltner, K.* (2020). Allgemeine Versicherungsbedingungen. S. 106ff.

die notwendige Sorgfalt walten, indem er alle Mitarbeiter anweist, keine Softwareupdates durchzuführen. In diesem Fall wird sich der Versicherer allerdings (zurecht) auf A-7.1 sowie A-7.6-8 AVB D&O berufen (Ausschlussgrüne aufgrund des vorsätzlichen Abweichens von geltenden Vorschriften oder sämtlicher Pflichtverletzungen). Dem für die IT des Unternehmens zuständigen Geschäftsführer[32] ist vorwerfbar, dass er sich mit Sicherheitsstandards auseinandersetzen und diese kennen muss, sowie für deren Einhaltung Sorge zu tragen hat[33].

4. Exemplarische Problemstellungen

- Fall 1)[34]

Der Arbeitgeber stellt dem Arbeitnehmer keinerlei technische Gerätschaften zur Verfügung, räumt dem Arbeitnehmer das Recht auf Ausübung der Tätigkeit im Homeoffice ein bzw fordert diesen dazu auf, seine Tätigkeit (idF möglich) vom Homeoffice aus fortzusetzen[35]. Der Arbeitnehmer verwendet ein privates Speichermedium und ist via VPN-Zugang ins Unternehmensnetzwerk eingewählt und schleust so Schadsoftware ein, wodurch der Betrieb des Arbeitgebers für 24 Stunden lahmgelegt wird, da wichtige Daten des Arbeitgebers vorrübergehend nicht mehr abrufbar sind.

- Fall 2)

Im Unterschied zu Fall 1 bekommt der Arbeitnehmer (im Folgenden AN genannt) sämtliche Ausstattung vom Arbeitgeber, der diesen auch unterweist und den Umstand dem Versicherer meldet, zur Verfügung gestellt. Der AN öffnet eine Phishing-Mail und schleust auf diese Art und Weise Schadsoftware ins Unternehmensnetzwerk ein, was wie in Fall 1 zu einer Betriebsunterbrechung aufgrund vorübergehend nicht verfügbarer Daten führt.

– Variante a) Der Arbeitgeber hat bereits sämtlich Sicherheitsvorkehrungen getroffen (Treiber aktualisiert, Virenschutz Software vorinstalliert, automatische Sicherheitsupdates veranlasst und für eine wöchentliche Datensicherung Sorge getragen, etc). Zusätzlich dazu hat eine Unterweisung des AN stattgefunden und es wird lediglich firmeneigenes sicheres und vorab geprüftes Material und Speichermedien zur Verfügung gestellt, doch es kommt durch Ransomware[36] Angriff in Form eines Trojaners zur Sperre der gesamten Unternehmens-IT und darüber hinaus wird eine Lösegeldforderung seitens der Angreifer gestellt.

– Variante b) Der vom Arbeitgeber unterwiesene Arbeitnehmer verwendet fahrlässigerweise ein privates Speichermedium und schleust so eine Schadsoftware ins Unternehmensnetzwerk ein.

Hinweis: In allen Fällen hat der Arbeitgeber eine Cyberversicherung abgeschlossen.
Um diese Problemstellungen lösen zu können und beurteilen zu können, ob eine Cyberversicherung im jeweiligen Fall Deckungsschutz bietet, empfiehlt sich ein Blick in die Musterbedingungen. Anhand derer erscheint folgende Conclusio plausibel.

Grundsätzliches: Der Versicherungsfall des Art 1 der Musterbedingungen ist jeweils erfüllt, da aufgrund der Beeinträchtigung der Verfügbarkeit von Daten eine Informationssicherheitsverletzung[37] vorliegt. Als Informationssicherheitsverletzung ist hier die Be-

32 Vor allem iZm Cybersecurity ist vielen Führungskräften das mögliche Ausmaß einer Cyberattacke und die weiteren nachteiligen Folgen für das Unternehmen oftmals nicht bewusst. Hier besteht Nachholbedarf in puncto Aufklärung und Präventionsmaßnahmen siehe dazu auch *Hillgraf, S. 534.*

33 Siehe *Fenyves, Koban & Keltner, S. 11.* Vgl Art A-7.1, A-7.6, A-7.7 und A-7.8 AVB D&O.

34 Das Einschleusen einer Schadsoftware (Virus) in das jeweilige Unternehmensnetzwerk mittels eines USB-Sticks, ist kein Spezifikum bzw spezifisches Problem des Homeoffice, diese Problematik besteht auch bei Ausübung der beruflichen Tätigkeit in den firmeneigenen Räumlichkeiten.

35 Der Arbeitnehmer trifft diese „Anordnung" auf Grundlage der Empfehlung der Bundesregierung (kein zwingender Charakter). Bis dato bestand/besteht keine Anordnung seitens der BReg die Tätigkeit des Arbeitnehmers ins Homeoffice zu verlagern. Auf arbeitsrechtlicher Ebene kann der AG den AN nicht zur Verlegung zwingen, dies muss in beiderseitiger Übereinstimmung erfolgen.

36 Zu Ransomware generell siehe auch *Keltner, S. 109.*

37 In den meisten Cyberversicherungspolizzen ist allerdings nicht nur das Vorliegen einer Informationssicherheitsverletzung relevant, sondern auch der Umstand wie diese zustande kam.

FORTSETZUNG NÄCHSTE SEITE »

einträchtigung von elektronisch verfügbaren Daten beschrieben, egal ob eine bloß vorübergehende Beeinträchtigung oder die komplette Löschung von Datensätzen vorliegt. Unter *elektronische Daten* fallen gem Art 1 2. ABC 2018 auch Software und Programme. Der Vorfall ereignet sich in allen Konstellationen während der Laufzeit des Versicherungsvertrages (Art 4).

– Spezifika ad Fall 1) Soferne der Arbeitgeber dem VU allerdings nicht gemeldet hat, dass Mitarbeiter ins Homeoffice entsandt wurden und dort private Endgeräte verwenden,[38] und auch keine Unterweisung stattfand bzgl allfälliger Präventionsmaßnahmen, wird der Cyberversicherer hier zurecht auf Leistungsfreiheit gemäß Art 9 ABC 2018 Obliegenheiten des VN vor Eintritt des Versicherungsfalles plädieren. Artikel 6 2. Gefahrerhöhung ermöglicht es dem Versicherer zudem die Kündigung.

– Ad Fall 2) Die Beurteilung dazu erfolgt analog wie in Fall eins. In diesem Fall wird der VU gegenüber dem Arbeitgeber ebenfalls nicht zwingend leistungspflichtig, da nur folgende Voraussetzungen erfüllt sind: aufrechter Versicherungsvertrag, Anzeige der Gefahrerhöhung, zur Verfügung Stellung von Infrastruktur, in welchem Zustand diese ist, geht aus dem Sachverhalt nicht hervor, hierbei wird es sich um einen Grenzfall handeln. Die Betriebsunterbrechung wird in den Musterbedingungen im Baustein B[39] behandelt und die besonderen Risikoausschlüsse des Art 19 4. ABC 2018 definieren den Ausschluss des Versicherungsschutzes, bei Verwendung von ungetesteten oder nicht freigegebenen informationsverarbeitenden Systemen (worunter der Stick im Sachverhalt fallen wird) Achtung: Auch nach Eintritt des Schadens ist der VN gemäß Art 10 zu einem aktiven Wohlverhalten[40] verpflichtet, ansonsten könnte der VU Leistungsfreiheit begehren.

– Variante b) IdF kann der VU jedenfalls zur Leistung herangezogen werden: technisch einwandfreie IT-Infrastruktur wird zur Verfügung gestellt, es erfolgen Sicherheitsunterweisungen sowie Präventionsmaßnahmen. Die obigen Ausführungen gelten analog. Achtung: Der VN sollte keinesfalls der Lösegeldforderung nachkommen, da weder Lösegeldforderungen noch Schäden die daraus resultieren nach den Musterbedingungen gedeckt sind und zu den Risikoausschlüssen Art 2 4. ABC 2018 des zählen.

a) Empfehlungen für Unternehmen: Vorgansweise im Ernstfall

Der Abschluss einer Cyberversicherung kann eine Risikominimierung für aus dem Homeoffice resultierende Cyberrisks mit sich bringen. Der Deckungsumfang ist für jedes Cyberversicherungsprodukt individuell einer detaillierten Prüfung zu unterziehen, um so den bestmöglichen Deckungsschutz im Schadenfall zu erhalten. Unternehmen sollten[41] klare Anweisungen für die Arbeitnehmer im Homeoffice definieren und Homeoffice Unternehmensleitlinien allen Mitarbeitern gegenüber transparent kommunizieren.[42] Awareness bei den Mitarbeitern schaffen, das Risikobewusstsein schärfen und auf die vergrößerte Gefahr einer Cyberattacke im Homeoffice hinweisen, sind kostengünstige und stark risikoreduzierende Aspekte iZm Cybersecurity. Soferne eine Cyberversicherung abgeschlossen wurde, ist der Arbeitgeber verpflichtet, die Homeoffice Tätigkeit der Arbeitnehmer gegenüber dem VU anzuzeigen. Auch nur leichte Fahrlässigkeit kann zur Verringerung des Versicherungsschutzes oder im Worst-Case Scenario zur Kündigung seitens des VU führen.

38 Die Prämie erhöht sich bei den gängigen Cyberversicherungsanbietern deutlich in einem so gelagerten Fall.

39 Die Musterbedingungen zählen vier Risikobausteine, diese sind frei wähl- und kombinierbar: A - Service und Kostenversicherung, B - Betriebsunterbrechungsversicherung, C - Datenwiederherstellungsversicherung sowie Baustein D – Haftpflichtversicherung. Siehe hierzu näher Keltner, S. 111.

40 ISv Mitwirkung an der Schadensbegrenzung, Unterstützung während der „Aufarbeitung“ und Leistung sämtlicher möglicher Maßnahmen, die der raschen Wiederherstellung des Ursprungszustandes dienen; analog zu & 3 Abs 3 VersVG.

41 Unabhängig vom seitens der Bundesregierung beschlossenen Homeoffice-Gesetz.

42 Ob hier gegebenenfalls der Aufsichtsrat oder der Betriebsrat involviert werden muss, bleibt an dieser Stelle außer Acht gelassen.

III. Auf den Punkt gebracht

Die im Jänner 2019 veröffentlichten Musterbedingungen haben bis dato zu keiner Konsolidierung des Cyberversicherungsmarktes geführt, der Markt zeigt sich immer noch sehr heterogen und diese Inhomogenität zeigt sich auch im Umgang mit technischen Obliegenheiten in den Cyberversicherungsverträgen. Die meisten Versicherungskonzepte enthalten mehr oder weniger umfangreiche Kataloge mit technischen Obliegenheiten, die auch iZm Homeoffice virulent werden. Es wird zwischen klassischen technischen Obliegenheiten (zB dem Schutz gegen Schadsoftware mit einem Virenscanner) und organisatorischen Maßnahmen (Patch-Management-Verfahren, Erstellen von Krisenplänen für den Eintritt des Schadensereignisses) differenziert. Zusammengefasst werden Anforderungen an das betriebliche Risiko-Management beschreiben. Generalklauselartig und wenig zufriedenstellend ist der Stand der Technik geregelt. Eine adäquate Cyberversicherung kann IT-Sicherheitsmaßnahmen komplettieren, dient aber nicht als Ersatz dafür, vor allem in gefahrerhöhenden Homeofficetätigkeiten empfiehlt sich eine detaillierte und differenzierte Lösung. Die exemplarischen Problemstellungen wurden anhand der Musterbedingungen gelöst. Die jeweilige Cyberversicherungspolizze kann von den Musterbedingungen abweichen und dadurch kann es zu variablen/ungleichen Lösungsansätzen kommen. Wie bereits angemerkt, empfiehlt sich ex ante die detaillierte Prüfung des jeweiligen Bedingungswerkes.

Authentifikation in der digitalen Ära

Wie Privatpersonen und Unternehmen ihre digitalen Identitäten bewahren

AUTOR:IN
Dr. Markus Vesely
CEO der A-Trust GmbH

Unser Alltag verlagert sich immer mehr in den Cyberspace. Das bedeutet, dass sich sowohl Personen als auch Unternehmen im digitalen Raum eindeutig identifizieren müssen, um rechtssicher handeln zu können. Wie funktioniert nun die digitale Authentifikation von natürlichen und juristischen Personen und wie kann deren jeweilige digitale Identität gewahrt werden?

Sowohl in der Wirtschaft als auch in der Verwaltung werden analoge Prozesse zunehmend durch digitale Alternativen ersetzt. Die aktuell geltende eIDAS-Verordnung sieht drei rechtsgültige Arten von elektronischen Signaturen vor: Simple (SES), Advanced (AES) und Qualified (QES).

Zwar sind **einfache elektronische Signaturen** (SES) wie eine manuell auf einem Desktop-Bildschirm ausgeführte oder eingescannte handschriftliche Unterschrift bereits seit Langem verfügbar, doch sie genügen im Fall komplexer, risikoreicher Transaktionen und Verträge bei Weitem nicht den Sicherheits- und Complianceanforderungen. Dafür braucht es die **fortgeschrittene elektronische Signatur** (AES) und die **qualifizierte elektronische Signatur** (QES). Sie sind mit den signierten Daten so verknüpft, dass diese nach dem Unterzeichnen nicht unbemerkt verändert werden können. Zusätzlich stellen sie sicher, dass die Signatur eindeutig der unterzeichnenden Person zugeordnet ist – so ist die Authentizität der Unterschrift gewährleistet.

Qualifizierte elektronische Signatur

Der Begriff „qualifizierte elektronische Signatur" fällt immer wieder in Zusammenhang etwa mit dem Vertragsmanagement eines Unternehmens oder der Verwaltung von Patient:innendaten in der Gesundheitsversorgung. Dies zeigt, dass die QES für den sicheren Umgang mit hochkritischen Daten geschaffen und gemäß §4 (1) SVG iVm. §886 AGBG auch immer dann gefragt ist, wenn eine der handschriftlichen Unterschrift rechtlich gleichgestellte Signatur in elektronischer Form benötigt wird.

Was unterscheidet nun eine QES von einer AES? Sie ist, einfach gesagt, eine AES, der ein qualifiziertes Zertifikat zugrunde liegt und die mit einer qualifizierten elektronischen Signatuerstellungseinheit erstellt wurde.

Für eine QES braucht es also eine qualifizierte Signaturerstellungseinheit – etwa ein bei einem Vertrauensdienstanbieter wie A-Trust befindliches Hardware-Sicherheitsmodul, das zum Beispiel für die Handy-Signatur bzw. nun ID Austria genutzt wird. In anderen Fällen sind eine Chipkarte (Bankomatkarte, e-card, ...), ein geeignetes Chipkarten-Lesegerät und eine zugehörige Software erforderlich, um eine QES zu erstellen. Somit stellt die qualifizierte elektronische Signatur aufgrund ihrer hohen Anforderungen an die Identifizierung der Unterzeichnenden die sicherste Form des digitalen Unterzeichnens dar.

Die wichtigsten Anwendungsfälle für die QES

Der wohl verbreitetste Use Case für die qualifizierte elektronische Signatur ist das **E-Government.** Sie ist außerdem bei der **elektronischen Vergabe öffentlicher Aufträge** erforderlich und wird auch oftmals verwendet, um die Echtheit, Herkunft und Unversehrtheit des Inhalts von **elektronisch übermittelten Rechnungen** zu gewährleisten. Dazu kommt die **europaweite Rechtssicherheit** von Dokumenten, die mit der Handy-Signatur bzw. ID Austria unterzeichnet werden: ein wichtiger Erfolgsfaktor in der digital vernetzten Geschäftswelt! Auch für **spezielle Branchenlösungen** ist die QES unerlässlich, wie etwa für die sichere Nutzung des Unified Patent Court (UPC).

Die qualifizierte elektronische Signatur kann allerdings nur von natürlichen Personen

durchgeführt werden. Wie können nun Unternehmen oder Behörden die größere Produktivität und Effizienz digitaler Authentifizierungslösungen nutzen?

Qualifiziertes elektronisches Siegel

Dafür ist das elektronische Siegel vorgesehen, der digitale Behörden- bzw. Firmenstempel. Technisch basiert es auf dem gleichen Verfahren wie eine elektronische Signatur, wobei die Verknüpfung des Unternehmens mit dem Zertifikat über eine zeichnungsberechtigte Person der jeweiligen Organisation erfolgt.

Laut eIDAS gibt es auch hier wie bei der elektronischen Signatur die drei Niveaus „einfach", „fortgeschritten" und „qualifiziert" und damit ebenfalls steigende Sicherheitslevels. Was das Siegel von der Signaturlösung nun unterscheidet, ist sein rechtlicher Wert: Denn als rechtliches Äquivalent zur handschriftlichen Unterschrift ist die qualifizierte elektronische Signatur eine Willenserklärung und die unterschreibende Person gibt mit ihr das uneingeschränkte Einverständnis zu einem Sachverhalt oder einer Vereinbarung. Damit ist die Schriftformerfordernis erfüllt, die es erlaubt, rechtlich bindende Verträge zu schließen.

Da das Siegel als digitaler Stempel eines Unternehmens oder einer Behörde, also einer juristischen Person, verwendet wird, gibt es jedoch keine eindeutige Verbindung zwischen einer konkreten Person und dem gestempelten Dokument, kann also nicht als Willenserklärung gelten. Hierfür wird zusätzlich die qualifizierte Signatur der jeweils zeichnungsberechtigten Personen benötigt. Wenn damit aber keine Verträge geschlossen werden können, wofür werden elektronische Siegel überhaupt gebraucht?

Vorteile eines qualifizierten elektronischen Siegels

Mit einem Firmen- oder Behördenstempel wird die Echtheit des digitalen Dokuments, die Authentizität seines Inhalts sowie seine Integrität bestätigt. Das Siegel ist daher geeignet, um binnen weniger Sekunden zeit- und ortsunabhängig die eindeutige Herkunft und Unversehrtheit von Zeugnissen, Bescheiden, Rechnungen oder Beglaubigungen zu bestätigen, und sichert den Beweiswert von Dokumenten.

Damit können sich Organisationen **vor Internetbetrug schützen,** eingescannte Papierdokumente nach Anbringen eines qualifizierten elektronischen Siegels und eines qualifizierten Zeitstempels **revisionssicher archivieren** oder ihre **Workflows vollständig und medienbruchfrei digitalisieren.** Als Beispiel eines konkreten Anwendungsfall ist die Eintragung aller Produkte mit Energielabel in die EU-Datenbank EPREL zu nennen, die nur mit der Verifizierung des Unternehmens durch ein qualifiziertes elektronisches Siegel möglich ist. Ein weiterer interessanter Use Case des qualifizierten Firmensiegels stellt die Erfüllung der Auflagen für E-Rechnungen zwischen Wirtschaftstreibenden gemäß §11 Abs. 2 des UstG. dar, demzufolge eine E-Rechnung nur dann als Rechnung gilt, wenn die Echtheit der Herkunft und die Unversehrtheit des Inhaltes gewährleistet ist.

Digitale Identität als Grundlage unserer Gesellschaft

Die eingangs erwähnte große Bedeutung des technologischen Wandels für unseren beruflichen und privaten Alltag macht klar, dass sowohl unsere Identität als Bürger:innen als auch die Identität unserer Unternehmen und Organisationen im digitalen Raum unbedingt hoch professionell gewahrt werden muss. Ohne eindeutige und sichere Authentifizierung durch einen Vertrauensdiensteanbieter wie A-Trust sind Betrug und Rechtsunsicherheit Tür und Tor geöffnet, mit negativen Auswirkungen auf die persönliche Sicherheit der Menschen wie auch auf die wirtschaftlichen Rahmenbedingungen. Deshalb sollten wir auf allen Ebenen und über alle Branchen hinweg zusammenarbeiten, um die digitale Ära möglichst sicher und erfolgreich zu gestalten.

Das unerwartete Ereignis

AUTOR:IN
Dr. Barbara Flügge
DoktorB
Senior Offer Creation & Resilience Strategist
digital value creators (DVC)

Zweifelsohne ist jeder Unternehmer auf sorgenfreies und risikoarmes Wachstum bedacht. Wachstum ist das optimale Ergebnis, wenn man zur richtigen Zeit am richtigen Ort die richtigen Entscheidungen getroffen hat. Externe und interne Risiken funken immer wieder dazwischen und unterbrechen die oftmals verzweifelte Suche nach der passenden Erfolgsformel, die zu Ihrem Unternehmen, Ihrem Business bzw. Ihrer Organisation passt. Der «Fit-Faktor», also wie sich Erfolg und Wachstum in Ihre Organisationen einfügen, hängt zunehmend auch an der Sichtbarkeit Ihres Unternehmens und Ihrer Marke. Konsequenterweise trägt Sichtbarkeit mit System und Stringenz zur Skalierbarkeit Ihres Angebots bei. In unseren Untersuchungen eines widerstandsfähigen und skalierbaren Angebots zeigt sich, dass es sieben performancekritische Handlungsfelder braucht. Der operative Betrieb und die IT sind das sog. Handlungsfeld Nummer 5. Digitalisierung ist sicherlich ein Erfolgsbaustein für jedwede Organisation und Verwaltung, ob Referent oder Verwaltungscoach. Digitalisierung ist elementarer Bestandteil unseres Denkens und unseres Handelns geworden: für Geschäftsnetzwerke, Angebotspräsentationen, Schulungen; voll automatisiert ist die Digitalisierung ein wichtiger Mitarbeitender geworden und mit ihm und dank ihm fertigen wir Alltagsgegenstände und Luxusartikel, lassen Häuser dank 3D-Technologie wachsen, prüfen Nachforderungen und vergleichen Referenzurteile in komplexen Mandantensituationen.

Wir sind nicht allein dort draussen. Eindringlinge und Störenfriede machen Organisationen jeglicher Grössenordnung das Leben schwer, im Betrieb, Verkauf, im Zulieferprozess und in der Kanzlei. Wir können uns sehr genau ein Bild davon machen, wie analoges Eindringen aussieht. Wir haben bildlich den Dieb, den mutwilligen Zerstörer vor Augen.
Nehmen wir als Beispiel ein Anwaltsbüro. Eindringlinge verschaffen sich Zugang zu dem Büro, den Unterlagen, Aktennotizen, entwenden Betriebsmittel. Sie durchsuchen, zerstören, nehmen mit. Wurde vorab gezielt sich auf das Eindringen vorbereitet, desto leichter fällt es den Eindringlingen das zu finden, was sie suchen bzw. desto gezielter lösen sie eine Aktion aus, die sie geplant hatten oder wofür sie beauftragt wurden. Dazu zählen etwa die Mitnahme von Unterlagen,

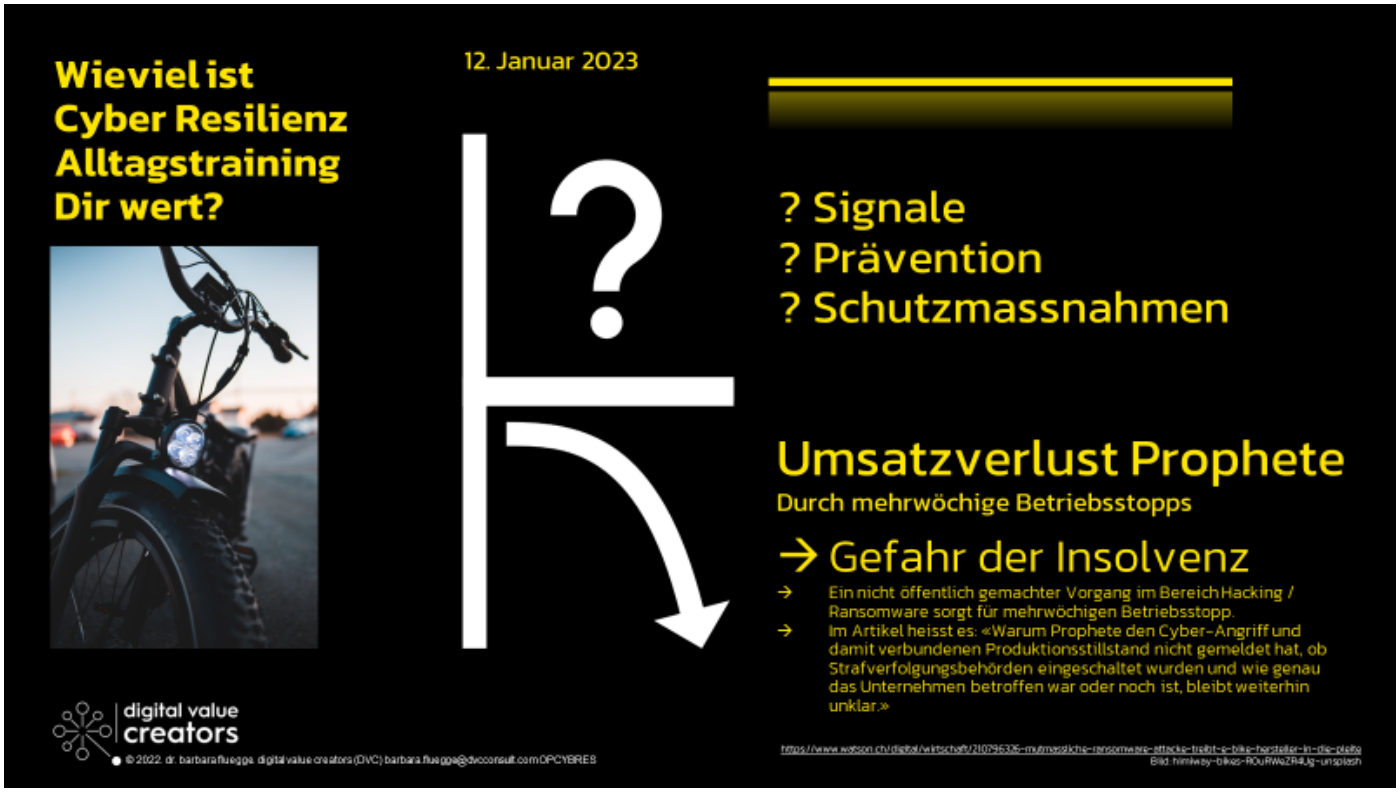

Abbildung 7. Eindringling

Datenträger, es geht darum Verwirrung zu stiften, um einen anwaltlichen Vorgang hinauszögern und einen Termin vor Gericht oder eine Aussage platzen zu lassen.

Wie gezielt und planvoll hat ein Eindringling vorzugehen, um das Erfolgserlebnis zu bekommen, was beabsichtigt war? Mit dem Einzug der Digitalisierung haben sich Eindringlinge neu ausgerichtet. Sie sind versierter geworden und nutzen weit mehr digitale Optionen für ihr bis dato genutztes Geschäftsmodell: 1) «Zugriff und Stören» und 2) «Zugriff und Zerstören». Längst geht es um die dritte Option 3) «Zugriff und Verdienen».

Big Game Hunting wurde bis dato als diejenigen Angriffe mit dem grössten Hackerrisiko bezeichnet, um grosse Unternehmen und Konzernstrukturen sowie bekannte Marken zu attackieren. Das Bild hat sich gewandelt. Der Mittelstand, der sich dank digitaler Tools seine Betriebsabläufe optimiert, sein Business international vertreibt und Mitarbeitende, die in Europa und in USA beispielweise ansässig sind, dockt sich digital im Durchschnitt mit mehr als 17 Zugangsstellen an andere bekannte und im Subunternehmergeschäft unbekannte Unternehmen an.

Das Cyberrisiko liegt zum einen so die Analyse von Crowdstrike und digital value creators (DVC) in wenig bis unzureichend geschützten Systemen und der Überwachung bzw. Sicherung oben genannter Zugangsstellen und zum anderen bei uns Menschen. Startups mit coolen Apps sind attraktiv und günstig für den Mittelstand und das Marketingbüro. Das Wissen und das konsequente Durchdenken eines Risikos könnte dafür sorgen festzustellen, wann und weshalb digitale Zugänge ververnachlässigt und Warnungen missachtet worden sind.

Analysen zeigen, dass es immer noch der Mensch ist, der den Hackern und Eindringlingen den roten Teppich ausrollt. Nehmen wir das Beispiel einer Marketingabteilung in einem Bundesministerium. Im analogen Minenfeld würde alles getan werden, um Eindringlinge durch Zugangskontrollen und eine Abfolge von Prüfungen abzuwehren, Unterlagen würden sicher aufbewahrt, auffällige Postsendungen vorab aussortiert werden. Und im digitalen Minenfeld? Wie bereiten Sie Ihre Organisation auf das digitale Minenfeld vor?
Das Mandat von Organisationen jeglicher Industrie- und Branchenzugehörigkeit, Grösse

FORTSETZUNG NÄCHSTE SEITE »

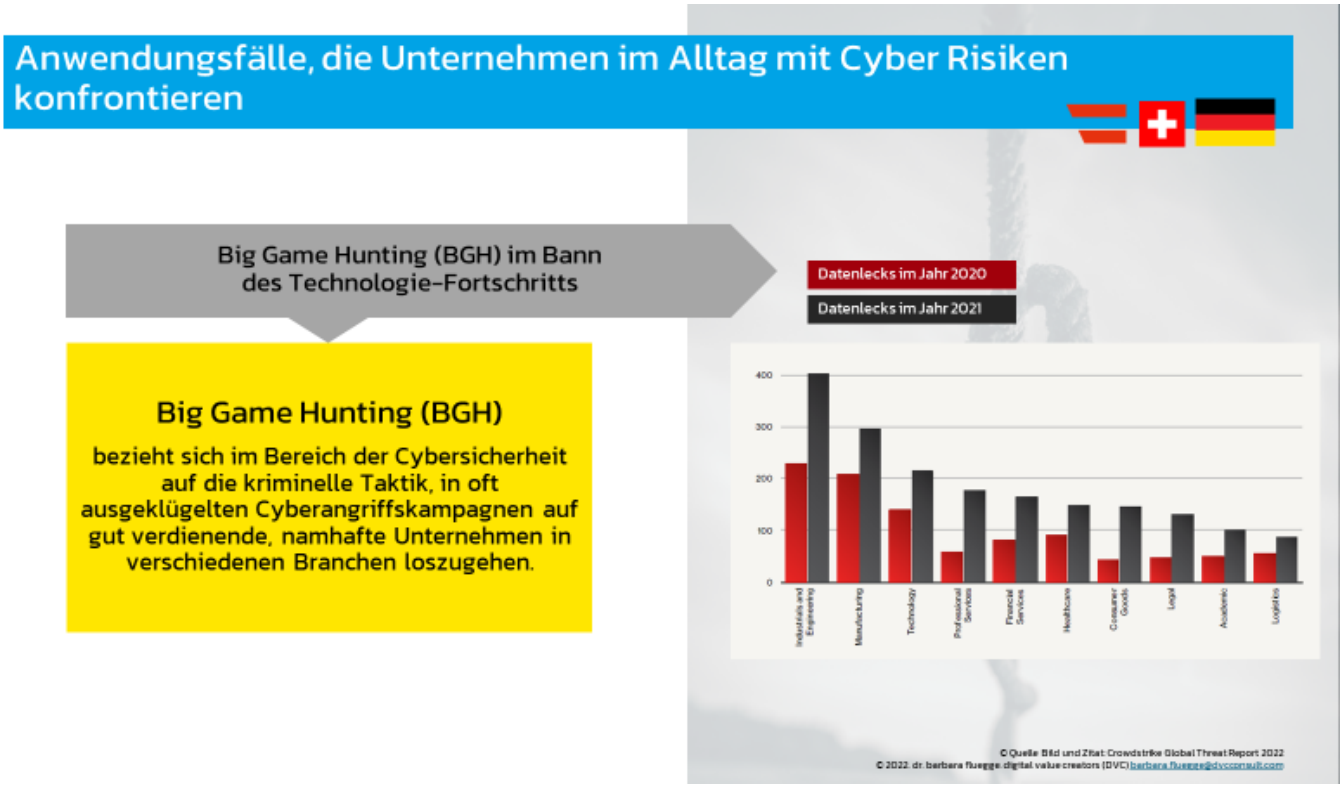

Abbildung 8. Big Game Hunting

und Geografie ist es, das Unternehmen, seine Belegschaft, die Finanzkraft und das Umfeld des Unternehmens zu schützen. Zu schützen vor den Gefahren, die im Cyber Bereich präsenter sind denn je, und damit die Existenz des Unternehmens gefährden. Dazu zählen vorherrschende und unentdeckte Gefahren aus dem digitalen und virtuellen World Wide Web, Anfälligkeit durch vernetzte und teils offene Software-Systeme, gehackte physische Sensoren, manipulierte mediale Inhalte und Finanzdaten und gesperrte funktionale Abläufe. Letzteres ist bekannt, etwa um Organisationen um Lösegeld für die Öffnung von Systemzugängen oder Zugang zu Dateninhalten zu erpressen.

Ein durchgetaktetes digitales Arbeitsumfeld also ist kein Garant dafür, dass das Unternehmen, sein Geschäftsziel und damit seine Existenz und die Belegschaft sicher sind. Es braucht eine Wahrnehmungsschärfung für Organisation und Mensch. Dies umfasst aus unserer Erfahrung sieben Organisationsbereiche – unabhängig von Industrie, Grösse und Geografie sind diese sieben Handlungsfelder relevant (siehe Bild 2). Damit liesse sich – so unsere Erfahrung – ein unerwartetes Ereignis in ein zu erwartetes Ereignis abfedern und damit gar nicht erst entstehen zu lassen. Das Risiko tritt also gar nicht erst auf. Gehen wir zurück zu dem Beispiel der Marketingabteilung. Digital werden die Presseabteilung im Ministerium, die Agentur, das Grafikteam, Fotografen und Rechercheabteilungen miteinander vernetzt. Eine Kampagne zum Thema Standortsicherung der Produktion im Österreich steht an. Es werden Poster und Druckmaterial digital gestaltet und mit dem Zahlenwerk versehen. Der digitale Eindringling, der auf die dritte Option seines Geschäftsmodells aus ist, wird nicht die Kampagne stören oder Dateien verschwinden lassen. Er wird sich auf die Zahlen, die in der Kampagne genannt werden, konzentrieren. Eine Manipulation, die weitreichende Konsequenzen hat. Denn genau diese Zahlen sind Gegenstand im Pressegespräch zu Wahlkampfzeiten im TV und online via YouTube. Die politischen Vertreter sollen öffentlich Rede und Antwort stehen. Der Supergau sind nicht erklärbare Zahlen, Fehler in den Herleitungen und die Breitbandwirkung in den sozialen Medien und bei den Wählern!
Wie liesse sich hier mit der Marketingabteilung und allen anderen arbeiten, um diese Gefahren abzuwenden? Braucht es umfangreichere Tools und Plausibilitätschecks? Sicherlich. Nur, diese allein genügen nicht.
Die Wahrnehmungsfähigkeit einer Organi-

Abbildung 9. 7 Handlungsfelder

sation, ihrer Struktur und bei uns Menschen gilt es zu schulen. Denn eine digitale Gefahr ist dann für uns real existent und trifft uns umso mehr, wenn sie durch unser Verhalten, unsere Handlung oder unser Nichtstun entstanden ist. Gefahrenquellen entstehen aus menschlicher und prozessualer Unachtsamkeit, die aus einer Nachlässigkeit heraus ein Risiko entstehen und wachsen lässt. Das Schutzschild der Organisation und das ist die gute Nachricht lässt sich konsequent auf- und ausbauen. Dazu statten wir – mit Blick auf das allgegenwärtige Gefahrenpotential – im Idealfall alle 7 Handlungsfelder in Organisationen mit einem Wahrnehmungsprogramm aus.

Dabei handelt es sich um ein Schulungsprogramm bestehend aus kognitiven, sozialen und digitalen Elementen. OPCYBRESTM steht für Operative Power durch Cyber Resilienz. Die ÖSCS-Initiative / das BKA sagt darüber: «OPCYBRESTM unterstützt die Umsetzung der Ziele der ÖSCS und trägt damit zu einer Erhöhung der gesamtstaatlichen Resilienz gegen Gefahren aus dem Cyberraum bei.» Testen Sie die Wahrnehmung Ihrer Organisation und spielen Sie die 7 Handlungsfelder mit uns durch.

Referenzliste:

digital value creators (DVC) (2022): OPCYBRESTM Schulungsprogramm online und vor Ort

Flügge, B. (2021). Mobility Moves Minds – build and grow again as business. Dean Publishing (Deutsche Ausgabe)

Aktuelles aus den Gerichten

Benn-Ibler Rechtsanwälte

ZUR LANGFASSUNG

Datenschutz am Arbeitsplatz

Die Einsichtnahme in E-Mails einer früheren Mitarbeiterin ist gemäß einer Entcheidung des österreichischen OGH unter bestimmten Voraussetzungen nach Art 6 Abs 1 lit f DSGVO zulässig. Dies gilt vor allem dann, wenn dies zur Wahrung eines berechtigten Interesses des Unternehmens erforderlich ist und die Interessen oder Grundfreiheiten der betroffenen Personen nicht überwiegen.

ZUR LANGFASSUNG

EuGH soll den Begriff des immateriellen Schadens der DSGVO klären

Der deutsche Bundesgerichtshof hat in einem Verfahren betreffend eine Person, deren personenbezogene Daten von dem Verantwortlichen unrechtmäßig durch Weiterleitung offengelegt wurden, die Frage der Festlegung der Kriterien betreffend den Anspruch auf Ersatz des immateriellen Schadens an den EuGH vorgelegt.

Unter anderem soll die Frage beantwortet werden, ob für die Annahme eines immateriellen Schadens bloße negative Gefühle wie Ärger, Unmut, Unzufriedenheit, Sorge und Angst, die an sich Teil des allgemeinen Lebensrisikos sind, genügen, oder, ob die Annahme eines Schadens einen über dieses Gefühl hinausgehenden Nachteil für die betroffene natürliche Person erforderlich macht.

ZUR LANGFASSUNG

Wann sind Äußerungen in privaten Chats vertraulich

Das deutsche Bundesarbeitsgericht (BAG) hat geurteilt, dass Mitglieder einer Chatgruppe den besonderen persönlichkeitsrechtlichen Schutz einer Sphäre vertraulicher Kommunikation nur dann in Anspruch nehmen können, wenn es berechtigte eine Vertraulichkeitserwartung gibt. Das ist wiederum abhängig vom Inhalt der ausgetauschten Nachrichten. Haben die Nachrichten den Inhalt beleidigender und menschenverachtender Äußerungen über Betriebsangehörige, bedarf es laut BAG einer besonderen Darlegung des Arbeitnehmers, warum er erwarten durfte, dass der Inhalt der Chatgruppe nicht an Dritte weitergegeben wird.

ZUR LANGFASSUNG

EuGH muss Gerichtsstand bei Software-Verträgen klären

Der österreichische oberste Gerichtshof (OGH) möchte vom Europäischen Gerichtshof (EuGH) wissen, wo der „Erfüllungsort“ iSd Art 7 Nr 1 lit b 2. Gedankenstrich der Verordnung Nr 1215/2012/EU über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (EuGVVO) bei Software-Dienstleistungsverträgen liegt.
Im Ausgangsfall entwickelte die in Wien ansässige klagende GmbH für die in Deutschland ansässige Beklagte eine Software. Vertragsgegenstand war die ursprüngliche und laufende Entwicklung sowie der laufende Betrieb der Software in Deutschland. Die Parteien vereinbarten weder Gerichtsstand noch Erfüllungsort.
Die Kernfrage ist, ob der „Erfüllungsort“ bei der Erbringung von Dienstleistungen der Ort ist, an dem der Dienstleister (in dem Fall die Klägerin) seine Tätigkeit hauptsächlich vorzunehmen hat.

Rechtsschutz-Deckung bei Data Breach

ZUR LANGFASSUNG

Der österreichische Oberste Gerichtshof (OGH) stellt klar, dass auch immaterielle Schäden vom Versicherungsschutz einer Rechtsschutzversicherung nach den Allgemeinen Bedingungen für die Rechtsschutzversicherung 2017 (ARB 2017) gedeckt sein können.

Betriebsratsvorsitzender kann kein Datenschutzbeauftragter sein

ZUR LANGFASSUNG

Die Stellung als Betriebsratsvorsitzender steht der Wahrnehmung der Aufgaben eines Datenschutzbeauftragten entgegen. Der Arbeitgeber sei deshalb berechtigt, die Bestellung zum Datenschutzbeauftragten zu widerrufen, so das deutsche Bundesarbeitsgericht (BAG).

Buchrezension Cyberversicherung

ZUR LANGFASSUNG

Der Tagungsband “Cyberversicherung” herausgegeben von Mag. Lisa Katharina Promok, erschienen 2023 bei Facultas, enthält die Abhandlungen der Tagung des Forschungsinstitutes für Privatversicherungsrecht zur Cyberversicherung im Herbst 2022 und bietet einen aktuellen Überblick über die Herausforderungen im Bereich der digitalen Sicherheit.

Zum Verhältnis von NIS 2 und DSGVO

ZUR LANGFASSUNG

Der Normenzweck und die Zielsetzungen der NIS 2 VO und der DSGVO überlagern sich im Bereich des Schutzes persönlicher Daten. In der DSGVO betrifft das insbesondere die Regelugen der Art. 32 und 33 DSGVO.

Die NIS 2 VO adressiert dieses Problem und sieht vor, dass die Regelugen der NIS 2 VO unbeschadet der Regelungen der DSGVO gelten (Art. 2 (12) NIS 2 VO), sodass diese beiden Regelungen gleichberechtigt nebeneinander bestehen.

Damit Doppelbestrafungen vermieden werden, regelt , dass wenn eine Datenschutzbehörde in der Folge eine Strafe in Bezug auf die angezeigte Verletzung verhängt, gemäß Art. 35 NIS2 keine weitere Strafe für denselben Sachverhalt im Sinne von Art. 34 der NIS 2 Vo verhängt werden darf. Sehr wohl können aber die in Art 32 und 33 NIS 2 VO angesprochenen Durchsetzungsmassnahmen verfügt werden.

Paradigmenwechsel für die Verantwortung von Leitungsorganen durch NIS-2

AUTOR:IN
Mag. Dr. Stefan Eder
Herausgeber, Partner bei Benn-Ibler und Gesellschafter bei Cybly GmbH

Cyberrisken stellen Leitungsorgane in Folge des hohen Gefahrenpotenzials und der Relevanz der möglichen Schäden vor neue – bisher so nicht bekannte – Herausforderungen. Durch die neue „NIS-2" Richtlinie der Europäischen Union wird nun das Thema des Umfangs der notwendigen Sorgfalt neu thematisiert.

Es ist mittlerweile allgemein bekannt, dass Cyberrisiken bestandsbedrohend für viele Unternehmen sein können. Die Anzahl der Angriffe ist so hoch, dass auch kaum ein Unternehmen sagen kann, dass es von solchen Versuchen verschont geblieben ist.
Diese Risikosituation führt schon für sich alleine gesehen dazu, dass Leitungsorgane in der Pflicht sind, diese Risiken zu beobachten und geeignete Maßnahmen zur Abwehr zu setzen. Bei Kapitalgesellschaften muss gemäß § 22 GmbHG bzw. § 82 AktG ein internes Kontrollsystem eingerichtet sein. Dies dient dem Schutz des Vermögens der Gesellschaft. Die dazu festgelegen Maßnahmen betreffen alle operativen Unternehmensbereiche und somit auch die Cybersicherheit. Zu beachten ist, dass dies eine kollektive Verantwortung der jeweiligen Organe ist und diese Verpflichtung per se nicht delegiert werden kann.

Für den Fall, dass Geschäftsführung bzw. Vorstand diesen Verpflichtungen nicht ordnungsgemäß nachkommen, **haften** sie gemäß den §§ 25 GmbHG bzw. 84 AktG **persönlich** für den dadurch entstehenden Schaden. Als Sorgfaltsmaßstab ist der eines ordentlichen (und gewissenhaften) Geschäftsmannes/Geschäftsleiters heranzuziehen. Der Gesetzgeber geht in dem Zusammenhang von einer objektiv sachlichen Herangehensweise auf Basis angemessener Information aus, wobei dies in Judikatur im Wege der Auslegung für den Einzelfall in Bezug auf die jeweils zu beurteilende Risikosituation weiter konkretisiert wird. In Folge der ebenfalls vorgesehenen Beweislastumkehr müssen die betroffenen Organe beweisen, dass sie ihren Verpflichtungen mit der notenwendigen Sorgfalt nachgekommen sind.

Die über die Jahre immer größer werdende Gefahr der Cyberrisiken haben auch die Organe der Europäischen Union erkannt. Nach längeren Konsultationen wurde dazu am 14.12.2023 Die Richtline (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau (sog. „NIS-2 RL") verabschiedet. Die NIS-2 RL ist am 16.1.2023 in Kraft getreten. Wie alle Richtlinien bedarf sie an sich der innerstaatlichen Umsetzung, die bis Ende 2024 vorgesehen ist.

Das wäre nun nicht weiters aufregend. Allerdings beinhaltet die NIS-2 RL neben einer Vielzahl von cyberspezifischen Regelungen unter anderem in den Art. 20 (Governance) und Art. 21 (Risikomanagementmaßnahmen) eine Festlegung welchen Sorgfaltsmaßstab Leitungsorgane in Bezug auf Cybersicherheit anzuwenden haben. Diese sind im Wesentlichen an den Standards orientiert, die man in der Literatur für ein Risikomanagementsystem generell bzw. spezifisch für Cyberrisiken (vgl. z.B. ISO 27001) finden kann.

Da, wie schon vorstehend dargestellt, in Bezug auf das interne Kontrollsystem und Risikomanagement bereits innerstaatliche Regelungen bestehen, bedarf es dahingehend keiner gesonderten Umsetzung, um die Pflicht von Leitungsorganen, auch gegen wesentliche Cyberrisken vorzusorgen, innerstaatlich gesetzlich festzulegen. Die detaillierte Ausgestaltung der einzelnen Pflichten wird der Gesetzgeber ins innerstaatliche Recht zu übernehmen haben, wobei schon die aktuelle Judikatur vergleichbare Sorgfaltskriterien für die Auslegung der §§ 25 GmbHG bzw. 84 AktG entwickelt hat. Die Indikation der Regelungen gemäß Art 20 und 21 NIS-2 RL bietet sich für die konkrete Auslegung der Pflichten der Leitungsorgane für die Risikovorsorge gegen Cyberrisiken durch innerstaatliche Gerichte daher an.

Das Argument, dass dies jede Kapitalgesellschaft betrifft, deren wirtschaftliches Bestehen von der Vermeidung wesentlicher Cybervorfälle abhängt, und nicht nur jene

(durchaus große Zahl von) Unternehmen, die direkt unter NIS-2 fallen, liegt auf der Hand. Sehen doch die §§ 22 GmbHG bzw. 82 AktG keine Einschränkung der Verpflichtungen der Einrichtung eines internen Kontrollsystems nach Tätigkeitsbereich der jeweiligen Kapitalgesellschaft vor.

Der Vorteil ist, dass es für Leitungsorgane nachvollziehbare Maßnahmen gibt, die in Bezug auf Cybersicherheit anzuwenden sind. Wobei auch auf die Verhältnismäßigkeit und Angemessenheit der Maßnahmen Bedacht genommen werden darf/soll.

Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen sind das Ausmaß der Risikoexposition der eigenen Einrichtung, deren Größe und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.
Was bedeutet das nun konkret in Bezug auf Cybersicherheit? Leitungsorgane müssen (in etwas verkürzter Form) …
… an Schulungen teilnehmen und allen Mitarbeitern Schulungen anbieten um (in Ihrem Verantwortungsbereich) ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen zu erwerben;
… sicherstellen, dass geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen im Unternehmen ergriffen werden, um die Risiken der genutzten Dienste zu beherrschen und die Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten;
… Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme, die Bewältigung von Sicherheitsvorfällen, die Aufrechterhaltung des Betriebs, wie Back-up-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement, Sicherheit der Lieferkette, Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen, Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit entwickeln (lassen) und für deren Umsetzung sorgen;
… weiters Vorsorge treffen, dass grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit, Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung, Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen, Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme im Unternehmen eingerichtet werden.

Wie gesagt, die Verpflichtung zur Risikovorsorge und Einrichtung eines internen Kontrollsystems, das sich auf wesentliche Cyberrisken erstreckt, bestand unabhängig von der NIS-2 RL schon bisher. Der **Paradigmenwechsel** liegt aber darin, dass nun eine detaillierte Umschreibung der zweckmäßigen Maßnahmen und Vorsorgen erfolgt ist. Auch der Schutz der z.B. in der Lieferkette vertraglich verbundenen Unternehmen ist nach aktuellem Verständnis schon bisher eine wesentliche Vertragspflicht (i.e. ein von einem Cybervorfall betroffenes Unternehmen muss auch jetzt schon seine Vertragspartner, die ans eigene System angeschlossen und daher gefährdet sind, unverzüglich verständigen und warnen). Das ergibt sich aus den vertraglichen Schutz- und Sorgfaltspflichten.

Festzuhalten ist auch, dass Cyberrisikovorsorge primär eine Managementaufgabe ist. Cybervorfälle können die verschiedensten Formen annehmen (von den allseits bekannten DDos-Attacken, über Pishing-Angriffe, Ausspähen von Passwörtern, Geheimnisverrat durch Mitarbeiter bis zum Ausnutzen von diversen systembedingten Schwachstellen, der Übermittlung „verunreinigter Daten“ u.v.a.m). Besonders wichtig ist daher die vorausschauende Risikoanalyse, das Ausarbeiten eines Notfallsplanes und eines Managementplans, wie den diversen Risiken laufend begegnet werden soll. Wie auch in der NIS-2 RL angesprochen kommt besonders der Schulung der Mitarbeiter eine zentrale Be-

FORTSETZUNG NÄCHSTE SEITE »

deutung zu (die Resilienz des Unternehmens ist nur so gut wie das schwächste Glied in der Kette der Abwehr und die bei weiten meisten Cybervorfälle sind menschlichen Fehlern geschuldet).

Leitungsorgane müssen sich nun übrigens nicht zu Cyberexperten ausbilden lassen. Diese Aufgabe kommt nach wie vor den verantwortlichen Mitarbeitern (CISO und Team oder externen Experten) zu. Leitungsorgane müssen sich aber zumindest soweit schulen, dass sie das Bedrohungsszenario und die Risikolage generell verstehen und somit die richtigen Maßnahmen in Form von grundsätzlichen Richtlinien und Maßnahmenkatalogen verabschieden können und deren Umsetzung und laufende Aktualisierung überwachen können (wie sie das auch in Bezug auf das finanzielle Management oder andere Risikobereiche tun müssen).
Diese Maßnahmen müssen auch mit den notwendigen finanziellen, technischen und organisatorischen Mitteln unterstützt werden. Die bislang weitgehende Ignoranz des Themas ist ein erheblicher Risikofaktor für Leitungsorgane.

Die Vorsorge muss der Risikolage adäquat sein. Das meint nicht nur die eigene Leistungsfähigkeit und Gefährdung, sondern auch die Angriffsmittel, die den Angreifern zur Verfügung stehen. Dazu sei darauf verwiesen, dass Cyberkriminalität organsiert vorgeht. Nicht umsonst spricht man von Cybercrime as a Service (CaaS). Diese systematisierte Vorgehensweise von Cyberkriminellen ist auch nicht neu, sondern hat sich über die zumindest letzten zehn Jahre sukzessive und stetig entwickelt. Das jährliche Schadensvolumen wird z.B. in Deutschland 2022 auf € 203 Mrd. geschätzt Verhältnismäßig auf Österreich umgelegt, geht es um einen zweistelligen Milliardenbetrag. Die Anzahl der Angreifer ist beträchtlich und diese gehen durchaus mehr und mehr unternehmerisch organsiert vor.

Die Verpflichtung zur Überwachung ausreichender Risikovorsorge trifft im Rahmen seines Tätigkeitsbereiches auch den Aufsichtsrat. Diesem kommt im Rahmen seiner Aufsichts- und Prüfpflicht die Verantwortung zu, die durch das Management gesetzten Maßnahmen zu hinterfragen. Der Aufsichtsrat muss sich dazu die notwendige Expertise sichern, bei größeren Unternehmen mit besonderer Exponiertheit für Cyberrisiken kann man sich die Frage stellen, ob es im Aufsichtsrat eines gesonderten Ausschusses bzw. besonderer Fachkenntnisse bedarf. Im Falle eines Schadens in Folge eines Cybervorfalles muss der Aufsichtsrat mögliche Ersatzansprüche gegen Vorstand bzw. Geschäftsführung prüfen und gegebenenfalls durchsetzen.

Auch der jeweilige Wirtschaftsprüfer wird wohl im Rahmen seiner Prüfung das innerbetriebliche Risikomanagement und das interne Kontrollsystem evaluieren und im Zweifel eine Warnung (Redepflicht) aussprechen.
Die Verpflichtungen, die sich aus der DSGVO im Kontext mit Sicherheitsverletzungen ergeben, bleiben im Übrigen unberührt bestehen (und sind wohl ins Risikomanagement entsprechend miteinzubeziehen).

Für Leitungsorgane ist auch wichtig zu beachten, dass die D&O Versicherungen dem Thema Cyberrisiko durchaus mit Vorsicht begegnen. Bei einer besonders groben Pflichtverletzung besteht daher jedenfalls die Gefahr, dass Deckung abgelehnt wird. Darüberhinaus überdenken Versicherungen aktuell Art und Umfang ihrer Versicherungsangebote betreffend Cybersicherheit, da das Verhältnis Prämie zu Risiko ein immer größeres Problem darstellt.

Was es Seitens der Leitungsorgane braucht, ist ein proaktives Herangehen und Beschäftigung mit der Problematik. Cyberrisiken werden nicht verschwinden, sondern vielmehr ein dauerhafter Bestandteil der Bedrohungslage bleiben. Die Herausforderung ist, dass diese Risikoproblematik nicht umfassend gelöst werden kann und sich ständig verändert und weiterentwickelt. Eine fortlaufende Optimierungsaufgabe für Leitungsorgane.

CYBLY

Ihr Partner für digitale Transformation

Die Cybly GmbH ist ein LegalTech Unternehmen und bietet prozessorientierte, integrierte IT-Lösungen in allen Bereichen mit juristischem oder rechtsinformativem Hintergrund. Cybly vereint zwei Dienstleistungen bzw. Marken unter einem Dach – die Rechtsdatenbank „LawThek“ und die maßgeschneiderten Softwarelösungen von „Legalnetics“ ergänzt durch ein umfassendes, kompetentes Beratungsservice.

Optimale Kundenzufriedenheit

Die Bedürfnisse unserer Kunden wollen wir mindestens erfüllen – im besten Fall übertreffen - und zukünftigen Anforderungen des Marktes gerecht werden.

Jetzt scannen

cybly.tech

Cybly GmbH

Tuchlauben 8, 1010 Wien

Strubergasse 28, 5020 Salzburg

E-MAIL: **vertrieb@cybly.tech**

TEL.: **+43 1 533 6980-840**

fit4internet

Digitalisierung und digitale Technologien sind aus unserem Berufs- und Alltagsleben nicht mehr wegzudenken. Neben all den Vorteilen und Erleichterungen können sie auch Risiken und Gefahren mit sich bringen. Sicherheit in der digitalen Welt hat sich als eines der wesentlichsten Themen etabliert.

Cybersicher mit fit4internet

Mit dem Digital Skills Barometer hat fit4internet, der Verein zur Steigerung der digitalen Kompetenzen in Österreich, in Kooperation mit Partnern aus Wirtschaft und Wissenschaft das – österreich- und europaweit – erste befragungsbasierte Erhebungsinstrument geschaffen, welches ein repräsentatives, fundiertes und über reine Selbsteinschätzung hinausgehendes Lagebild über die digitale Fitness der österreichischen Bevölkerung ermöglicht. Und während die Ergebnisse der kürzlich veröffentlichten Ausgabe für das Jahr 2023 hoffnungsvoll stimmen, da sich die Wissenslücken der Österreicher*innen im so bedeutenden Bereich „4. Sicherheit und nachhaltige Ressourcennutzung" reduziert haben, bleibt eines sicher: Eine solide digitale Grundkondition lässt sich nur durch ständiges Dranbleiben, kontinuierliches Weiterlernen und konstantes Training der eigenen digitalen Kompetenzen gewinnen und behalten. Bedarfsorientierte, zielgerichtete sowie zukunftssichere Maßnahmen für Re- und Up-Skilling sind für Entscheidungsträger*innen aus Wirtschaft, Politik, Wissenschaft und Zivilgesellschaft auf Basis des einmaligen, umfangreichen und detaillierten Lagebilds über die digitale Fitness der österreichischen Bevölkerung des Digital Skills Barometers wesentlich leichter einzuleiten.

https://www.fit4internet.at/view/verstehen-zahlendatenfakten

Sie möchten Ihre eigenen digitalen Kompetenzen im Bereich „Sicherheit in der digitalen Welt" auf die Probe stellen und erfahren, wie #digitallyfit Sie wirklich sind? Dann machen Sie – ganz schnell und unkompliziert – eine Selbstevaluation mit den CHECKs und QUIZzes von fit4internet. Mithilfe dieser kostenlosen Standortbestimmung können etwaige Lücken und Unsicherheiten identifiziert und passende Weiterbildungsmöglichkeiten gefunden werden.

https://www.fit4internet.at/page/assessment/sicherheit

Und wenn Sie wissen wollen, wie es um die digitalen Kompetenzen Ihrer Mitarbeiter*innen im Bereich Cyber-Security steht, dann können Sie über die f4i-DigComp-Portal-Lösung schnell und unkompliziert den Stand der digitalen Kompetenzen ganzer Abteilungen, Standorte oder sogar Regionen bestimmen. Anhand dieser Gruppenbezogenen Ergebnisse können Sie bedarfsorientiert Weiterbildungs- oder Qualifizierungsprogramme veranlassen.

https://www.fit4internet.at/view/portaluser

Zukunftssicher zertifiziert

Da bereits über 90% der aktuellen Arbeitsplätze digitale Kompetenzen voraussetzen, stellt sich die Frage, wie digitale Skills für alle Arbeitnehmer*innen rasch und nachhaltig etabliert werden können. Genau an dieser Stelle kommt fit4internet mit dem "Dig-CERT – Zertifikat für digitales Allgemeinwissen in Alltag und Beruf" ins Spiel: Im Zusammenspiel von Wissenschaft und Praxis entwickelt, ist das Dig-CERT das derzeit europaweit einzige inklusive und wissenschaftlich-methodisch entwickelte Zertifikat zur Anerkennung von digitalem Wissen auf Basis des DigComp 2.3 AT. Es bildet dabei jene digitalen Kompetenzen ab, über die alle Arbeitskräfte verfügen sollten – unabhängig von Branche, Funktion oder individuellem Bildungshintergrund. Mit dem Dig-CERT belegen Arbeitnehmer*innen ihr fundiertes digitales Wissen und somit ihre berufliche Anschlussfähigkeit. Zudem ermöglicht es bessere Berufs- und Aufstiegschancen, da vorhandene Potenziale sichtbar gemacht werden können. Orientiert am Nationalen Qualifikationsrahmen (NQR) werden die Ergebnisse je nach Wissensstand auf unterschiedlichen Kompetenzstufen in den einzelnen Kompetenzbereichen dokumentiert. Gleichzeitig dient das Zertifikat auch als Leitfaden für die individuelle berufliche Weiterentwicklung und fungiert ebenso als Orientierungshilfe für potentielle Arbeitgeber*innen – denen man damit auch gleich seine persönliche Bereitschaft zum stetigen Weiterlernen demonstriert. Zudem ist der national anerkannte Nachweis für digitale Wissenskompetenz durch seine Anbindung an den Europass (www.europass.at) auch international anschlussfähig – somit ist man also nicht nur #digtallyfit, sondern auch Europa-fit!

www.dig-cert.at

Digitalisierungvorhaben EU 2023 und Ausblick 2024

Data Governance Act (VO (EU) 2022/868)	Der DGA zielt darauf ab, die Weiterverwendung spezifischer Daten des öffentlichen Sektors zu erleichtern.
Digital Markets Act (VO 2022/1925 - DMA)	Die Verordnung regelt „Torwächter" also digitale Plattformen, die als Schlüsselzugangstore zu Verbrauchern dienen. Sie soll verhindern, dass mächtige Plattformen ohne Grenzen ihre eigenen Regeln durchsetzen können.
Digital Services Act (VO 2022/2065 - DSA)	Der Digital Services Act legt Sorgfaltspflichten und Haftungsausschlüsse für Vermittlungsdienste, insbesondere Online-Plattformen, fest. Er enthält auch Verfahren zur Meldung und schnellen Entfernung illegaler Inhalte sowie zusätzliche Pflichten für sehr große Plattformen.
DLT-Pilot-Regime (VO 2022/858)	Diese Regelung, die vorerst für drei Jahre gilt, ermöglicht eine Pilotphase für DLT-Finanzmarktinfrastrukturen (Distributed Ledger Technology). Dazu gehören die Einführung von DLT-Lizenzen und einer Regulatory Sandbox für Handlung und Abwicklung von DLT-Finanzinstrumenten.
DORA-RL (RL 2022/2556)	Die DORA-RL beinhaltet Anpassungen in verschiedenen Rechtsvorschriften im Einklang mit der DORA-Verordnung.
DORA-Verordnung (VO 2022/2554)	Die DORA-Verordnung legt einheitliche Anforderungen an Netzwerk- und IT-Sicherheit in Finanzunternehmen fest. Dazu gehören IKT-Risikomanagement, Meldung von Vorfällen, Tests und Informationsaustausch.
Maschinen-VO (VO 2023/1230)	Diese Verordnung definiert Anforderungen an die Konstruktion und den Bau von Maschinenprodukten, insbesondere im Hinblick auf grundlegende Gesundheits- und Sicherheitsanforderungen. Sie schreibt eine zwingende Zertifizierung für bestimmte Maschinenkategorien vor.
MiCA-Verordnung (VO 2023/1114):	Die MiCA-Verordnung bringt EU-weit einheitliche Vorschriften für Emittenten von Kryptowerten und Krypto-Dienstleister. Sie gilt nur für Kryptowerte, die nicht als Finanzinstrumente, Einlagen oder strukturierte Einlagen betrachtet werden, und beinhaltet Zulassungsverfahren.
NIS-2 (RL 2022/2555)	Die NIS 2-Richtlinie schreibt EU-weite Vorgaben für die Cybersicherheit von Einrichtungen fest, ua Anforderungen an das Risikomanagement inklusive Verantwortlichkeit der Leitungsorgane.
Resilienz-Richtlinie (RL 2022/2557)	Diese Richtlinie verpflichtet kritische Einrichtungen zur Durchführung von Risikobewertungen und zur Ergreifung von Maßnahmen zur Gewährleistung der Resilienz. Besondere Aufsicht besteht über kritische Einrichtungen von europäischer Bedeutung.
Chip-Gesetz (VO 2023/1781)	Das Chip-Gesetz fördert politikgesteuerte Investitionen in Halbleiterproduktion in Europa. Es schafft einen investitionsfreundlichen Rahmen für Produktionsstätten und ermöglicht die Früherkennung von Halbleiter-Engpässen.
Produktsicherheits-Verordnung (VO 2023/988)	Diese Verordnung ersetzt die Produktsicherheitsrichtlinie und verlangt für Produkte angemessene Cybersicherheitsmerkmale.
Konnektivitäts-Verordnung (VO 2023/588)	Die Konnektivitäts-Verordnung legt die Einrichtung des Programms der Union für sichere Konnektivität für den Zeitraum 2023-2027 fest.
Verbraucherkreditvertrags-Richtlinie (RL 20233/2225)	Diese Richtlinie passt die alte Verbrauchskredite-Richtlinie an ein durch die Digitalisierung verändertes Marktumfeld an.
Verordnung zur Rückverfolgung von Geld- und Kryptowertetransfers (VO 2023/1113)	Verordnung ersetzt die Geldtransfer-Verordnung und erweitert ihre Anwendbarkeit auf Kryptowerte. Sowohl Zahlungsdienstleister als auch Anbieter von Krypto-Dienstleistungen werden verpflichtet, Angaben weiterzuleiten. Gilt auch für Transaktionen über EUR 1.000 von sogenannten nicht betreuten Geldbörsen (un-hosted wallets).

Viele weitere Vorhaben befinden sich derzeit noch im Gesetzgebungsprozess – einige davon bereits sehr weit fortgeschritten.

Kommissions-Vorschlag vom 21.4.2021 Aktueller Stand: Politische Einigung von Rat und Parlament erzielt (Dezember 2023)	**Gesetz über künstliche Intelligenz (AI Act):** Das Gesetz über künstliche Intelligenz legt verschiedene Bestimmungen für den Bereich der KI fest, darunter das Verbot bestimmter Praktiken, besondere Anforderungen für Hochrisiko-KI, Vorschriften für die Inverkehrbringung von KI-Systemen, Risikomanagement, Datengovernance, technische Dokumentation, Transparenz, menschliche Aufsicht, Qualitätsmanagement, Zulassungsverfahren und KI-Reallabore.

Cyber Resilience Act: Der Cyber Resilience Act legt Cybersecurity-Vorschriften für das Inverkehrbringen von Produkten mit digitalen Elementen, grundlegende Anforderungen an ihre Konzeption und Entwicklung, sowie Vorschriften für den Umgang mit Cyberschwachstellen, die damit verbundene Marktüberwachung und die Pflichten der Wirtschaftsakteure fest.	**Kommissions-Vorschlag vom 15.9.2022** **Aktueller Stand: Erste Lesung**
Ecodesign for Sustainable Products Regulation: Die Ökodesign-Verordnung legt Anforderungen an bestimmte Kategorien von Produkten fest. Diese umfassen Haltbarkeit, Zuverlässigkeit, Wiederverwendbarkeit, Reparierbarkeit, Energieeffizienz, Recycling und die Verringerung des CO2-Abdrucks.	**Kommissions-Vorschlag vom 31.3.2022** **Aktueller Stand: Erste Lesung**
EU-Cybersolidaritätsgesetz: Das EU-Cybersolidaritätsgesetz schlägt Maßnahmen zur Stärkung der Solidarität und Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen vor. Dies beinhaltet die Einrichtung eines europäischen Cyberschutzschilds, eines Cybernotfallmechanismus, den Aufbau einer EU-Cybersicherheitsreserve, Vorsorgemaßnahmen und die finanzielle Förderung der gegenseitigen Amtshilfe, mit einem Budget von 1,1 Mrd EUR.	**Kommissions-Vorschlag vom 19.4.2023** **Aktueller Stand: Erste Lesung**
MWSt-im-digitalen-Zeitalter-Richtlinie: Die MWSt-im-digitalen-Zeitalter-Richtlinie führt digitale Meldepflichten ein, macht die elektronische Rechnungsstellung bei grenzüberschreitenden Umsätzen verpflichtend, aktualisiert MWSt-Vorschriften für Plattformen und führt eine einzige EU-weite MWSt-Registrierung ein.	**Kommissions-Vorschlag vom 8.12.2022** **Aktueller Stand: Zustimmung des Parlaments erfolgt**
Produkthaftungs-RL: Die neue Produkthaftungsrichtlinie sieht vor, dass Software als Produkt betrachtet wird. Sie vereinfacht die Beweisführung, nimmt Sicherheitsanforderungen (insbesondere Cybersicherheit) in die Fehlerbeurteilung auf und betrachtet die Lernfähigkeit als Teil dieser Beurteilung.	**Kommissions-Vorschlag vom 28.9.2022** **Aktueller Stand: Erste Lesung**
Richtlinie zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz (RL über KI-Haftung): Die Richtlinie zur Anpassung der Vorschriften über außervertragliche zivilrechtliche Haftung an künstliche Intelligenz eröffnet die Möglichkeit, den Beklagten KI-Anbieter zur Offenlegung von Beweismitteln zu zwingen. Sie behandelt außerdem vermutetes Verschulden und einen vermuteten Kausalzusammenhang im Zusammenhang mit der Beweislast.	**Kommissions-Vorschlag vom 29.9.2022** **Aktueller Stand: Erste Lesung**
VO über europäischen Raum für Gesundheitsdaten: Die Verordnung über den europäischen Raum für Gesundheitsdaten ergänzt die DSGVO in Bezug auf elektronische Gesundheitsdaten. Sie gibt Personen mehr Kontrolle über ihre elektronischen Gesundheitsdaten und fördert die europaweite Nutzung und den Austausch von Daten für Forschung.	**Kommissions-Vorschlag 4.5.2022** **Aktueller Stand: Erste Lesung**
Data Act: Der Data Act soll regeln, wer die in den Wirtschaftssektoren der EU erzeugten Daten nutzen darf und Zugriff darauf hat. Nutzer sollen Zugang zu den von ihren Geräten erzeugten Daten haben, um sie an Dritte für anschließende Dienste weitergeben zu können. Es soll einen Schutz von KMU vor missbräuchlichen Vertragsklauseln in Verträgen über die gemeinsame Datennutzung (Wiederherstellung einer ausgewogenen Verhandlungsmacht) und Schutzmaßnahmen gegen unrechtmäßige Datenübermittlungen geben.	**Kommissions-Vorschlag vom 23.2.2022** **Aktueller Stand: Entscheidung des Parlaments in 1. Lesung (9.11.2023)**
VO zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO: Damit soll es zu einer Harmonisierung der Verfahrensvorschriften in grenzüberschreitenden Fällen, insb der Anforderungen hinsichtlich Zulässigkeit grenzüberschreitender Beschwerden, Verfahrensrechte betroffener Personen und einer verbesserten Zusammenarbeit der Datenschutzbehörden kommen.	**Kommissions-Vorschlag vom 7.3.2023** **Aktueller Stand: Erste Lesung**
VO zur Schaffung eines Rahmens für eine europäische digitale Identität: Damit soll ein Recht auf eine EU-weit gültige digitale Identität (Menschen und Unternehmen) geschaffen werden.	**Kommissions-Vorschlag vom 3.6.2021** **Aktueller Stand: Allgemeine Ausrichtung des Rats vom 6.12.2022**
RL zur Ausweitung und Optimierung des Einsatzes digitaler Werkzeuge und Verfahren im Gesellschaftsrecht: Mit dem Vorschlag wird die Menge der in Unternehmensregistern und/oder im BRIS verfügbaren Gesellschaftsdaten erhöht und deren Zuverlässigkeit verbessert und die direkte Verwendung von Gesellschaftsdaten ermöglicht, die in Unternehmensregistern verfügbar sind, wenn grenzüberschreitende Zweigniederlassungen und Tochtergesellschaften errichtet werden und andere grenzüberschreitende Tätigkeiten und Situationen vorliegen.	**Kommissions-Vorschlag vom 30.3.2023** **Aktueller Stand: Erste Lesung**
Änderung des Rechtsakts für Cybersicherheit (ENISA-VO) im Hinblick auf verwaltete Sicherheitsdienste: Diese Ergänzung des Rechtsakts für Cybersicherheit gibt der Kommission die Befugnis, europäische Systeme für die Cybersicherheitszertifizierung für „verwaltete Sicherheitsdienste" (zB Penetrationstests oder Sicherheitsaudits) einzuführen.	**Kommissions-Vorschlag vom 19.4.2023** **Aktueller Stand: Erste Lesung**