AUSGABE 3 / 25. SEPTEMBER 2025

Aus der Produktfamilie Deutscher AnwaltSpiegel

CyberSecurityQuarterly

Das Online-Magazin für Datensicherheit in Unternehmen

→ unter anderem mit folgenden Themen:

Prof. Dr.
Thomas Wegerich
Herausgeber
CyberSecurityQuarterly

Liebe Leserin, lieber Leser,

es ist ein zweischneidiges Schwert: Die rasante Entwicklung der künstlichen Intelligenz (KI) eröffnet vielfache Möglichkeiten mit Blick auf die präventive und reaktive Cybersicherheit. In den Händen von Cyberkriminellen ist KI allerdings ein mächtiges Angriffswerkzeug, das zu ganz neuen Bedrohungslagen führt. Bodo Meseke und Michael Ritter kennen sie alle. Das sollten Sie auch.

Der Cyber Resilience Act (CRA) ist eine zentrale europäische Produktsicherheitsverordnung, die den regulatorischen Rahmen für Produkte mit digitalen Elementen festlegt. Der CRA tritt in weiten Teilen erst Ende 2027 in Kraft. Unternehmen sind jedoch gut beraten, sich jetzt schon mit dem neuen Recht zu beschäftigen. Sonst, so unsere Autoren Olga Stepanova und Dr. Hauke Hansen, droht ein böses Erwachen, was den Produktvertrieb in der EU betrifft. – Prädikat: lesenswert.

Wir bleiben in der EU und bei der Produktsicherheit: Durch das New Legislative Framework bilden Cybersicherheitsanforderungen künftig den Kern der Produktsicherheit. Carsten Hösker und Florian Wegmann haben für Sie zusammengestellt, welche Auswirkungen das in der Praxis für Unternehmen und deren Berater hat.

Ihr

Thomas Wegerich

Besuchen Sie unsere Website:
www.cybersecurity-quarterly.de

Künstliche Intelligenz als Angriffswerkzeug für Cyberkriminelle

Wir sehen einen Quantensprung, der alles bisher Dagewesene in den Schatten stellt

Von Bodo Meseke und Michael Ritter

Künstliche Intelligenz (KI) hat zahlreiche Bereiche unseres Lebens längst durchdrungen, auch wenn dies aus Anwendersicht nicht immer klar erkennbar ist. Sowohl im privaten als auch im geschäftlichen Umfeld nehmen die Nutzung und Bedeutung von KI-gestützten Systemen rasant zu, wobei ihre Einsatzmöglichkeiten noch längst nicht erschöpfend erforscht sind. Eines ist jedoch bereits heute deutlich sichtbar: KI in ihrer heutigen Form stellt einen Quantensprung dar, der alles bisher Dagewesene in den Schatten stellt.

KI revolutioniert Chancen und Risiken in der Cybersicherheit, indem sie zugleich mächtige Abwehr- und Angriffswerkzeuge liefert und Unternehmen zu adaptiven, prozessintegrierten Sicherheitsstrategien zwingt.

Bodo Meseke
EY GmbH & Co. KG Wirtschaftsprüfungsgesellschaft, Eschborn
Partner, Forensic & Integrity Services
bodo.meseke@de.ey.com
www.de.ey.com

Michael Ritter
EY GmbH & Co. KG Wirtschaftsprüfungsgesellschaft, Eschborn
Manager, Forensic & Integrity Services
michael.ritter@de.ey.com
www.de.ey.com

Aus Sicht der Cybersicherheit bietet sich hier ein sehr komplexes Bild. Auf der einen Seite schickt sich KI an, sowohl die präventive als auch die reaktive Cybersicherheit inklusive Spezialgebieten wie eDiscovery, IT-Forensik und Cyber-Incident-Response grundlegend zu revolutionieren. Auf der anderen Seite bringt KI aber auch völlig neue Gefahren mit sich, und das auch abseits der Tatsache, dass die KI-Systeme selbst ein Angriffsziel mit teils völlig neuen Angriffsvektoren darstellen.

In den Händen von Kriminellen ist KI bereits heute ein mächtiges Angriffswerkzeug, das die Bedrohungslandschaft grundlegend verändert. Diese Veränderungen beschränken sich dabei nicht allein auf die Cybersicherheit, sondern haben Auswirkungen auf die gesamte Unternehmenssicherheit und teils sogar deutlich über diese hinaus.

In diesem Artikel werfen wir einen Blick auf die Schattenseiten der KI – und speziell auf die Angriffsstellen, die es Cyberkriminellen ermöglichen, aktuell verfügbare beziehungsweise kurzfristig zu erwartende KI-basierte Technologien zur Begehung von Straftaten zu verwenden.

KI als Angriffswerkzeug

KI-Systeme stellen Kriminellen völlig neue Werkzeuge für die Begehung von Straftaten zur Verfügung. Neuere Ansätze wie Agentic AI und Reasoning, ganz zu schweigen von Techniken, die aktuell noch nicht (fertig) entwickelt sind, werden diese die Problematik noch massiv verstärken. Die Folge ist nicht nur eine beträchtliche Vereinfachung wirksamer Cyberattacken, sondern die Entwicklung völlig neuer krimineller Strategien und Taktiken.

Die Anbieter populärer KI-Systeme versuchen, hier Gegenmaßnahmen zu ergreifen, allerdings bisher nur mit eher mäßigem Erfolg. Generative KI ist ein klassisches Dual-Use-Produkt, und es ist oftmals schwer bis unmöglich, an einem Prompt die dahinterstehende Motivation abzulesen. Dazu kommt, dass zahlreiche KI-Komponenten von Trainingsdatenbeständen über Software bis hin zu fertigen Modellen als Open Source verfügbar und den Angreifern damit frei zugänglich sind. Eventuell implementierte Schutzmechanismen gegen Missbrauch können hier in der Regel leicht entfernt werden.

Social Engineering

Generative KI (GenAI) ist in der Lage, in zahlreichen Sprachen äußerst authentische und überzeugend formulierte Texte für unterschiedlichste Szenarien zu erstellen. Dabei kann der Kontext exakt vorgegeben werden, beispielsweise bezüglich Zielgruppe, Branche oder gewünschtem Effekt. Auch der imaginäre Autor kann in jedem Detail definiert werden, bis hin zu Qualifikation, Erfahrung, Alter und Charakter.

Gefälschte Texte lassen sich daher problemlos und mit hoher Qualität auf spezifische Berufsgruppen, Branchen oder Unternehmenstypen zuschneiden. Ein Fertigungsingenieur spricht anders als ein Fondsmanager, und in einem Logistikunternehmen werden andere Metaphern verwendet als in einem medizinischen Labor. Hochwertige GenAI-Systeme können diese und andere Faktoren oft auf sehr überzeugende Weise simulieren. Passendes gefälschtes Bild- und Videomaterial kann generative KI direkt mitliefern.

Hier ein paar Beispiele:

- Phishing-Mails
- gefälschte Profile in Jobportalen, Karriere- und sozialen Netzwerken
- gefälschte Geschäftskorrespondenz
- gefälschte Webpräsenzen und Firmenprofile
- gefälschte Produktseiten, Projektbeschreibungen, Flyer oder Produktpräsentationen

Gleichzeitig eignet sich generative KI auch zur schnellen und zielgerichteten Recherche über spezifische Berufe, Rollen, Branchen und teilweise sogar Unternehmen. Moderne Chatbots können ihre Nutzer sogar gezielt darin coachen, eine bestimmte Rolle einzunehmen.

Diese Fähigkeiten machen generative KI zu einem idealen Werkzeug für nahezu alle Aspekte des Social Engineering. Grundsätzlich ist all dies auch ohne Einsatz von KI möglich. Damit das Ergebnis überzeugend wirkt, müssen die Täter dann allerdings über erhebliches Wissen und spezifische Erfahrung verfügen. Die enorme Breite und Tiefe an Trainingsdaten neuerer großer Sprachmodelle macht dies in vielen Fällen weitgehend überflüssig.

Deep Fake – Fälschung von Bild-, Audio- und Videoinhalten

Ein weiteres Beispiel für den Einsatz generativer KI durch Kriminelle sind Deep Fakes. Die Möglichkeiten zur Generierung und Manipulation von Bildern, Video und Audiodaten sind bereits jetzt sehr beeindruckend, und diese Disziplin der KI entwickelt sich in rasantem Tempo weiter.

Momentan gibt es nur wenige bekannte Fälle, bei denen Deep Fakes eine kritische Rolle bei Cyberangriffen beziehungsweise Betrugsversuchen im Unternehmensbereich gespielt haben. Ein sogenannter Fake-President-Angriff mit Hilfe gefälschter Stimmen ist bereits erfolgt, solche Taten stellen aber aktuell noch die Ausnahme dar.

Angesichts der erheblichen Summen, die gerade im Bereich Waren- und Finanzbetrug auf dem Spiel stehen, verbunden mit stetig wachsenden Möglichkeiten der Automatisierung von Angriffen, steht zu erwarten, dass sowohl die Qualität als auch die Quantität entsprechender Betrugsversuche massiv zunehmen werden. Das lässt sich bereits heute im Bereich der Endverbraucher feststellen, wo KI aktuell bereits in großem Stil eingesetzt wird, beispielsweise im Kapitalanlagebetrug, bei Erpressungen oder bei der Diskreditierung von Personen und Organisationen.

KI in der Schwachstellenanalyse

Andererseits gibt es auch eine Reihe von Fällen, in denen KI erfolgreich zum Auffinden von Schwachstellen genutzt worden ist. Dabei gibt es unterschiedliche Ansätze, die jedoch noch nicht alle vollumfänglich verfügbar sind:

- Auffinden von Schwachstellen in Software durch Analyse des Quellcodes oder des Binärcodes
- Analyse der Schnittstellen und Abhängigkeiten einer Software, um potentiell verwundbare Komponenten zu identifizieren (Lieferkettenangriff)
- Analyse von Quellcode-Repositories auf vertrauliche Informationen wie Zugangsdaten oder API-Schlüssel
- Analyse von Binärcode auf fest codierten Zugangsdaten
- Analyse von Webseiten auf Sicherheitslücken und versehentliche Preisgabe vertraulicher Informationen
- Analyse von grafischen Benutzeroberflächen auf mögliche Schwachstellen

KI in der Programmierung von Schadcode

Die Anwendungsentwicklung mittels KI ist längst Realität, auch wenn die diesbezüglichen Möglichkeiten aktueller KI-Systeme medial teils stark übertrieben dargestellt werden. Gerade bei der Entwicklung kleinerer Anwendungen oder spezifischer Funktionen ist KI aber bereits heute ein sehr mächtiges Werkzeug. Entwicklungsprozesse lassen sich hier oft von Stunden oder Tagen auf Minuten verkürzen. Leider lässt sich dies nicht nur für die Entwicklung nützlicher Anwendungen nutzen, sondern auch für die Entwicklung von Schadcode.

Eine Besonderheit KI-gestützter Anwendungsentwicklung ist, dass der menschliche Programmierer keine tiefergehenden Kenntnisse der eingesetzten Technologien mehr benötigt, seien es Programmiersprachen, Algorithmen oder Schnittstellen (APIs) zu spezifischen Zielsystemen.

Fazit

Auch in den Händen von Cyberkriminellen ist KI ein mächtiges und aktuell noch nicht komplett verstandenes Werkzeug. In diesem Artikel haben wir lediglich eine kleine Auswahl heute bereits verfügbarer beziehungsweise kurzfristig zu erwartender Möglichkeiten zusammengefasst. Bereits jetzt ist sehr viel mehr denkbar, und aktuelle Entwicklungen wie Agentic AI, Reasoning und hocheffiziente, lokal ausführbare KI-Modelle erweitern die Anwendungsmöglichkeiten zusehends, was natürlich auch für kriminelle Aktivitäten gilt.

Dieser technische Fortschritt ermöglicht und bedingt weitreichende Veränderungen in Sachen Strategie und Taktik krimineller Organisationen und Einzeltäter. Um diesen neuen Herausforderungen effektiv und effizient zu begegnen, müssen Unternehmen ihre eigenen Strategien und Taktiken grundlegend verändern:

- **Adaptionsfähigkeit:** Moderne Sicherheitsstrategien müssen darauf ausgelegt sein, sich nicht nur ständig an Veränderungen anzupassen, sondern diesen aktiv vorzugreifen. Die Idee, sich mittels statistischer Extrapolation auf zukünftige Bedrohungen vorzubereiten,

war schon früher eher problembehaftet. In der momentanen Bedrohungslage werden solche Ansätze zunehmend gefährlich.

- **Neubetrachtung der Sicherheitstools:** Klassische Werkzeuge der Cybersicherheit sollten regelmäßig auf ihre aktuelle und zukünftige Wirksamkeit untersucht werden. Die Einfachheit, mit der Kriminelle heute nahezu perfekt designte und formulierte Phishing-Mails generieren können, muss nicht nur aktiv in Awareness-Kampagnen berücksichtigt werden, sondern führt insgesamt zu Veränderungen bei der Logik der Phishing-Abwehr.
- **Integration in Unternehmensprozesse:** Die Erkennung gefälschter Inhalte und der dahinterstehenden Betrugsversuche wird für Mensch wie auch Maschine immer schwieriger. Es wird damit zunehmend wichtiger, Geschäftsprozesse in Bezug auf solche Betrugsversuche auch abseits der eigentlichen Cybersicherheit resilient zu gestalten und Schutzmaßnahmen direkt in diesen Prozessen zu verankern.

Unternehmen können sich angesichts einer komplexen Sicherheitslage und einer sich stetig beschleunigenden technischen Entwicklung nicht länger auf altbewährte Strategien, Werkzeuge und Konzepte verlassen. Umgekehrt werden Unternehmen, die aktiv auf die neue Lage reagieren und ihre Sicherheitsstrategie und die dazugehörigen Taktiken und Technologien laufend an aktuelle und zukünftige Entwicklungen anpassen, einen erheblichen Wettbewerbsvorteil gewinnen können. ←

Hinweis der Redaktion: Weiterführende Informationen finden Sie in dem aktuellen EY-Whitepaper: **Künstliche Intelligenz und Cyber Incident Response: Chancen, Risiken und Anwendungsgebiete** **(tw)**

Cybersicherheit vs. Datenschutz – Wer hat Vorfahrt?

Dr. Axel Freiherr von dem Bussche, Partner bei Taylor Wessing, im Gespräch mit Dr. h.c. Marit Hansen, Landesbeauftragte für Datenschutz in Schleswig-Holstein

© alindiyani - stock.adobe.com

Cybersicherheit und Datenschutz gehören untrennbar zusammen – technische Maßnahmen müssen beide Ziele gleichermaßen berücksichtigen.

Dr. Axel Freiherr von dem Bussche, LL.M. (L.S.E.), CIPP/E
Taylor Wessing Partnerschaftsgesellschaft mbB, Hamburg
Partner
a.bussche@taylorwessing.com
www.taylorwessing.com

Dr. h.c. Marit Hansen
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel
Landesbeauftragte für Datenschutz Schleswig-Holstein
mail@datenschutzzentrum.de
www.datenschutzzentrum.de

Am 12.09.2025 führte Dr. Axel Freiherr von dem Bussche, LL.M. (L.S.E.), CIPP/E, Partner bei Taylor Wessing am Hamburger Standort der Großkanzlei, ein Gespräch mit Dr. h.c. Marit Hansen, der Landesbeauftragten für Datenschutz Schleswig-Holstein. Das Thema lautete „Cybersicherheit vs. Datenschutz – Wer hat Vorfahrt?“. Wir dokumentieren dieses Interview in voller Länge.

Dr. Freiherr von dem Bussche: *Heute haben wir ein besonders spannendes Thema auf der Agenda: „Cybersicherheit vs. Datenschutz – Wer hat Vorfahrt?“. Dieses Spannungsverhältnis wollen wir beleuchten. Wir freuen uns, dass wir mit Frau Dr. h.c. Marit Hansen über dieses Thema sprechen können. Sie sind nicht nur Datenschutzexpertin, sondern auch eine ausgebildete Informatikerin. Sie haben in der Vergangenheit auch andere Stationen durchlaufen. Sie waren nämlich Mitglied in der Datenethikkommission der Bundesregierung und Expertin in der Arbeitsgruppe der Agentur der Europäischen Union für Cybersicherheit (ENISA). Was hat Sie am meisten geprägt?*

Dr. h.c. Marit Hansen: Gleich am Anfang meiner Karriere bei dem Landesbeauftragten für Datenschutz Schleswig-Holstein im Jahre 1995 sprach ich mit meinem damaligen Chef Dr. Helmut Bäumler und erzählte ihm, dass es Internetbrowser gibt, mit denen man Inhalte anzeigen lassen könne. Mein Chef kannte das Wort „Browser“ nicht. Mit seinem polizeirechtlichen Hintergrund fragte er sofort nach: „Inhalte anzeigen? Direkt bei der Polizei?“ (schmunzelt). Dieses Missverständnis zwischen Recht und Technik hat mich dazu gebracht, dass man immer wieder überlegen muss, ob man einander versteht.

Ein ganz besonderes Erlebnis war die Arbeit in der Datenethikkommission der Bundesregierung. Es handelte sich um eine Runde aus interdisziplinär aufgestellten Spezialisten, die trotz ihrer Spezialisierung die Fähigkeit hatten, einander zuzuhören, voneinander zu lernen und sich auf ein gemeinsames Ergebnis zu einigen.

Dr. Freiherr von dem Bussche: *Wie sind Sie zu Ihrem jetzigen Amt gekommen?*

Dr. h.c. Marit Hansen: Es bedarf einer Kandidatur. Mein fachlicher Hintergrund ist Informatik, das ist untypisch für eine Datenschutzbeauftragte. Ich habe zuvor als stellvertretende Landesbeauftragte für Datenschutz Schleswig-Holstein gearbeitet. Im Jahr 2015 bin ich vom Schleswig-Holsteinischen Landtag gewählt worden, meine Wiederwahl war 2020. Einerseits kann man als Behördenleiterin fachlich nicht überall tief einsteigen, andererseits bestehen größere Einflussmöglichkeiten. Die Datenschutzkonferenz (das Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder; „DSK“) für fast eineinhalb Jahre zu leiten, hat mir ebenfalls große Freude bereitet.

Dr. Freiherr von dem Bussche: *Bevor wir zu unserem Gesprächsthema kommen, stelle ich die unausweichliche Frage: Was bedeutet KI für Ihr Amt? Steht nun der große Wandel bevor?*

Dr. h.c. Marit Hansen: Art. 74 der Verordnung über künstliche Intelligenz („KI-VO“) sieht neue Aufgaben für die Behörden vor. Abseits von dieser formalen Betrachtung hat sich die Welt durch KI insgesamt verändert. Diese Disruption ist gesamtgesellschaftlich spürbar. Wir merken die Verwendung von Large Language Models (LLMs) auch bei eingehenden Beschwerden. Typische Charakteristika: keine Tippfehler, formal korrekt, standardisiert. Referenzen auf Urteile oder Artikel in Gesetzen können auch schon einmal halluziniert sein.

Dr. Freiherr von dem Bussche: *Erhalten Sie qualitativ besser formulierte Beschwerden, oder nehmen Sie auch quantitativ eine Steigerung wahr?*

Dr. h.c. Marit Hansen: Auch in quantitativer Hinsicht. Mehrere meiner Kollegen verzeichnen einen Anstieg in Höhe von 50%. Wir haben einen Anstieg von etwas über 25%. Wir wissen jedoch nicht, ob nur KI dafür ausschlaggebend ist.

Dr. Freiherr von dem Bussche: *Die Formulierung unseres Themas „Cybersicherheit vs. Datenschutz – Wer hat Vorfahrt?“ ist ein wenig plakativ. Was halten Sie von diesem Titel?*

Dr. h.c. Marit Hansen: Ich mag provokante Titel (lacht). Die Headline beschreibt das Spannungsverhältnis gut. Ich würde nur der Formulierung widersprechen, dass einer Vorfahrt haben muss. Das Spannungsverhältnis ist mit einem Hausbau vergleichbar: Man kann zum Beispiel nicht zunächst den Maurer beginnen lassen und zu einem späteren Zeitpunkt den Architekten einschalten. Es müssen alle Akteure von Beginn an eingeplant werden, damit das Haus nicht zusammenstürzt.

Dr. Freiherr von dem Bussche: *Ein klassischer Fall eines solchen Spannungsverhältnisses kommt in unserer Praxis insofern vor, als bei der Implementierung von Cybersicherheitsmaßnahmen auch personenbezogene Daten verarbeitet werden. Dies betrifft beispielsweise die Überwachung von Postfächern, um Cybercrime zu verhindern. Diese Verarbeitung von personenbezogenen Daten bedarf einer datenschutzrechtlichen Rechtsgrundlage. Wir erleben häufig, dass Mandanten freudig ihre Pflicht zur Implementierung von Cybersicherheitsmaßnahmen erfüllen, aber zugleich dabei, mangels explizit bemühter DSGVO-Rechtfertigungsgrundlage, versehentlich gegen Datenschutzrecht verstoßen. Sobald wir dies in unserer Beratung mitteilen, sind die Mandanten perplex. Wie bewerten Sie dies?*

Dr. h.c. Marit Hansen: Früher gab es noch nicht spezielle Regelwerke wie beispielsweise die sich in der Umsetzung befindende NIS2-Richtlinie oder den Cyber Resilience Act. Stattdessen galt „nur“ die Datenschutz-Grundverordnung („DSGVO“), die in ihren Vorschriften wie zum Beispiel in Art. 5 Abs. 1 lit. f und 32 DSGVO „Sicherheit“ nennt. Schon in diesem Zusammenhang hat es viele überrascht, dass für die Implementierung von technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO immer dann eine Rechtsgrundlage erforderlich ist, wenn damit personenbezogene Daten verarbeitet werden – und das ist oft der Fall. Da hilft jedoch zum Beispiel Art. 6 Abs. 1 lit. c DSGVO weiter, der auf die Erfüllung einer rechtlichen Verpflichtung abstellt. Mit den neuen Rechts-

normen wird es aber expliziter. So nennt beispielsweise die NIS2-Richtlinie ausdrücklich Art. 6 Abs. 1 lit. c DS-GVO in Erwägungsgrund 109, 121.

Dr. Freiherr von dem Bussche: *Mich hat eine solche klare Bezugnahme positiv überrascht. Hier sehen wir das von Ihnen beschriebene Miteinander von Cybersicherheit und Datenschutz. Das ist durchaus neu.*

Dr. h.c. Marit Hansen: Ja, ich finde es gut. Erwägungsgrund 121 der NIS2-Richtlinie nennt zudem konkrete Maßnahmen zur Gewährleistung der Cybersicherheit. Da muss man genau hingucken und darf nicht Hochglanzprospekten glauben, die nur eine bestimmte Maßnahme als den letzten Schrei der Cybersicherheit bezeichnen. Es kommt auch immer auf das Wie an. So können die in Erwägungsgrund 121 genannten Maßnahmen beispielsweise Speicherfristen betreffen. Die früher vertretenen Aufbewahrungsfristen von sieben Tagen für Protokollierungsdateien mit IP-Adressen im Unternehmen reichen zumeist nicht mehr aus, da sich Ransomware-Angriffe über drei Monate oder länger hinziehen können. Eine Beschränkung einer Aufbewahrung auf eine Woche würde einer vollständigen Aufklärung entgegenstehen. Bei Ransomware-Angriffen hieße dies, dass man den Ursprungspunkt, also den „Patient Zero", in der Regel nicht identifizieren könnte.

Dr. Freiherr von dem Bussche: *Also gibt es nun eine gewisse Klarstellung. Diese darf jedoch nicht als Freifahrtschein verstanden werden.*

Dr. h.c. Marit Hansen: Genau. Es gilt nämlich für alle Maßnahmen das Gebot der Erforderlichkeit und der Verhältnismäßigkeit. Dabei hilft wieder der Blick in Erwägungsgrund 121 der NIS2-Richtlinie, der davon spricht, bei den Cybersicherheitsmaßnahmen gleichzeitig das Datenschutzrisiko einzudämmen, zum Beispiel durch Weitergabebeschränkungen, Verschlüsselung oder Pseudonymisierung der verarbeiteten Daten. Als weiteres Gesetz macht auch der Cyber Resilience Act das diskutierte Spannungsverhältnis deutlich. Der Cyber Resilience Act schreibt sogar als Konzeptionsgrundsatz „Security-by-Design" für Produkte mit digitalen Elementen vor. Dies betrifft alles, was vernetzbar ist und somit auch IoT-Produkte. Der Cyber Resilience Act listet auf, was „Security-by-Design" bedeutet – neben Vertraulichkeit, Integrität und Verfügbarkeit gehört auch die Datenminimierung dazu, die wir aus dem Datenschutz kennen.

Dr. Freiherr von dem Bussche: *Ein weiteres relevantes Gesetz ist der Data Act, der – insbesondere mit Blick auf die erwähnte Datenminimierung – indes dazu auffordert, aus dem Vollen zu schöpfen. IoT-Provider stehen dann womöglich vor der Herausforderung, die KI-VO, die DSGVO, den Data Act und den Cyber Resilience Act beachten zu müssen, wobei sogar ein Gesetz zur Ausschöpfung der Daten auffordert und ein anderes Gesetz wegen „Security-by-Design" die Datenminimierung beschwört. Die von Ihnen beschriebene Komplexität wird also nicht nachlassen.*

Dr. h.c. Marit Hansen: Ja, aber ich verspreche mir viel davon, wenn die Hersteller und Anbieter ihre Systeme gleich datenschutzkonform und sicher gestalten. Rechtskonformität by Design, darin erwarte ich Fortschritte. Für Standardanwendungen wird man sich auch immer wieder auf passende Blaupausen zurückziehen können. Wer jedoch innovative Wege gehen möchte, muss selbst stimmige Lösungen entwickeln.

Dr. Freiherr von dem Bussche: *Gut, dann können wir feststellen, dass wir Cybersicherheit und Datenschutzrecht sehr wohl versöhnt bekommen. In unserer Praxis wird das Spannungsverhältnis zwischen Cybersicherheit und Datenschutz auch im Fall von Data-Breaches gemäß Art. 33 DSGVO deutlich. Cyber-Breaches gehen nämlich oft mit Data-Breaches einher. Müssen diejenigen, die freiwillig einen Cyber-Breach anzeigen, ein datenschutzrechtliches Bußgeld fürchten?*

Dr. h.c. Marit Hansen: Gemäß § 43 Abs. 4 BDSG gilt der Grundsatz der Selbstbelastungsfreiheit. Derjenige, der sich selbst anzeigt, soll somit nicht noch ein datenschutzrechtliches Bußgeld erhalten. Dies muss jedoch ohnehin nicht befürchtet werden, wenn man sich bei der Meldung des Data-Breaches gegenüber den Aufsichtsbehörden kooperativ verhält.

Dr. Freiherr von dem Bussche: *Die wichtige Botschaft lautet also, dass man mit den Aufsichtsbehörden kooperieren sollte – dann muss man auch kein Bußgeld fürchten!*

Dr. h.c. Marit Hansen: Grundsätzlich ja. Allerdings muss die Kooperation proaktiv und ohne Trickserei erfolgen. Ungünstig ist zum Beispiel, wenn die Aufsichtsbehörde von dem Data-Breach längst auf anderem Wege erfahren hat.

Dr. Freiherr von dem Bussche: *Wir haben umfassend über die enorm zunehmende Komplexität gesprochen, die aus dem Zusammenspiel der vielen Regelwerke folgt. Dies überfordert viele Unternehmen. Gibt es aus Ihrer Sicht im Rahmen der Sanktionierung „mildernde Umstände" für Unternehmen, welche plötzlich alles auf einmal umsetzen müssen und deshalb verzweifelt sind?*

Dr. h.c. Marit Hansen: Das kommt auf den Einzelfall an. Es wird beispielsweise berücksichtigt, wer zeigt, dass er zur Einhaltung der Anforderungen gewillt ist und sich nicht bis zum Wirksamwerden davor drückt, um sodann auf Rücksichtnahme zu hoffen. Nichtstun reicht also nicht.

Dr. Freiherr von dem Bussche: *Zum Abschluss habe ich eine Frage, deren Antwort insbesondere Unternehmen, Datenschutzbeauftragte und Leiter von Rechtsabteilungen interessiert: Wie sollte man sich für die nächsten zehn Jahre wappnen?*

Dr. h.c. Marit Hansen: Es wird eine ganze Menge passieren. Zwar kann ich nicht in die Glaskugel schauen. Ich bin mir allerdings sicher, dass die Geschwindigkeit sich nicht verringern wird. Daher empfehle ich einen Fokus auf Risikomanagementsysteme, um effektiv und dauerhaft die Risiken beherrschen zu können. Man kann sich auch vertrauensvoll an die Aufsichtsbehörden wenden. Bei Sicherheitsfragen hilft außerdem das Bundesamt für Sicherheit in der Informationstechnik weiter. ←

Produkthaftung im digitalen Zeitalter

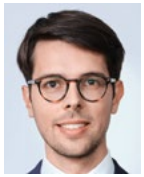
Cybersicherheit als Kernanforderung der Produktsicherheit

Von Carsten Hösker, LL.M., und Florian Wegmann, LL.M.

Die EU hebt die Produkthaftung ins digitale Zeitalter – und verschiebt die Risiken deutlich zu Lasten des Produktverantwortlichen.

Carsten Hösker, LL.M.
BLD Bach Langheid Dallmayr, Köln
Rechtsanwalt, Fachanwalt für Versicherungsrecht, Partner

carsten.hoesker@bld.de
www.bld.de



Florian Wegmann, LL.M.
BLD Bach Langheid Dallmayr, Köln
Rechtsanwalt, Fachanwalt für Versicherungsrecht

florian.wegmann@bld.de
www.bld.de

Die Europäische Union justiert den Rechtsrahmen für Produktsicherheit seit einiger Zeit neu. Im Gefüge des New Legislative Framework entsteht ein dichtes Netz aus Rechtsakten, die sich aus unterschiedlichen Blickwinkeln mit Cybersicherheitsanforderungen beschäftigen. Damit rücken vor allem vernetzte und digital gesteuerte Produkte in den Mittelpunkt.

Cybersicherheitsanforderungen zielen im Kontext der Produktsicherheit vielfach zunächst auf den Schutz des Produkts selbst vor Angriffen Dritter ab. Produktsicherheit hingegen betrifft den Schutz vor Gefahren, die von dem Produkt ausgehen. Beides lässt sich im digitalen Alltag aber nicht mehr trennen: Eine lückenhafte Cybersicherheit kann unmittelbar zur Beeinträchtigung der Produktsicherheit führen, jedenfalls dann, wenn sie Angriffe auf beziehungsweise Eingriffe in sicherheitsrelevante Funktionen des Produkts zulässt.

Neuer Produkt- und Fehlerbegriff

Um das Produkthaftungsrecht dem digitalen Zeitalter anzupassen, hat der europäische Gesetzgeber die neue Produkthaftungsrichtlinie [**Richtlinie (EU) 2024/2853**] erlassen, die die Mitgliedstaaten bis Ende 2026 in nationales Recht umzusetzen haben. Die Richtlinie reformiert den Produktbegriff, wobei die wichtigste Änderung darin zu

sehen ist, dass nunmehr auch ausdrücklich Software unter den Produktbegriff fällt, und zwar unabhängig von der Art ihrer Bereitstellung oder Nutzung. Umfasst ist Software, die auf einem Gerät gespeichert (sogenannte Embedded Software), aber auch solche, die über ein Kommunikationsnetz oder eine Cloudtechnologie abrufbar ist oder die durch ein Software-as-a-Service-Modell bereitgestellt wird.

Zur Beurteilung der Fehlerhaftigkeit eines Produkts sind künftig insbesondere „einschlägige sicherheitsrelevante Cybersicherheitsanforderungen" zu berücksichtigen. Welche Anforderungen das im Einzelnen sind und welchen Rechtsnormen diese Anforderungen zu entnehmen sind, hängt vom jeweiligen Produkt ab. Ein genereller Maßstab ist den Anforderungen aus der Produktsicherheitsverordnung [**Verordnung (EU) 2023/988**] zu entnehmen, die „angemessene Cybersicherheitsmerkmale fordert, die erforderlich sind, um das Produkt vor äußeren Einflüssen, einschließlich böswilliger Dritter, zu schützen". Diese Anforderung stellt eine unter herkömmlichen Zurechnungsregeln besondere, im Kontext von Cybersicherheit aber letztlich zwingende Haftungsregelung dar. Der vorsätzliche Eingriff eines außenstehenden Dritten markiert in der allgemeinen Zivilrechtsdogmatik bislang vielfach die Grenze der Zurechnung, jedenfalls bedarf es einer besonderen Rechtfertigung, einen solchen Eingriff dem „Ersttäter" – im hiesigen Kontext also dem Hersteller des Produkts, das eine Sicherheitslücke aufweist – zuzurechnen. Im Sinne der Rechtssicherheit wäre es für Unternehmen daher umso wichtiger, den einschlägigen Rechtsnormen konkret entnehmen zu können, wann ein Produkt über die notwendigen Cybersicherheitsmerkmale verfügt, um nicht als fehlerhaft angesehen zu werden. Wer sich die einschlägigen Anforderungen zu Gemüte führt, stellt fest, dass der europäische Gesetzgeber den Herstellern von Produkten lediglich Zielvorgaben macht, den Weg zum Ziel aber im Wesentlichen nicht beschreibt. In der Cyberresilienz-Verordnung [**Verordnung (EU) 2024/2847**] heißt es allgemein, dass Produkte mit digitalen Elementen so konzipiert sein müssen, dass sie ein „angemessenes Cybersicherheitsniveau" gewährleisten. Wann von einem angemessenen Cybersicherheitsniveau auszugehen sein soll, wird in einem Katalog mit weiteren Unterzielen definiert, die, soweit sie auf das betreffende Produkt anwendbar sind, gewährleistet sein müssen. So sollen Produkte – um nur zwei Beispiele zu nennen – „ohne bekannte ausnutzbare Schwachstellen" beziehungsweise mit „möglichst geringer Angriffsfläche" bereitgestellt werden.

Der europäische Gesetzgeber arbeitet also mit einer Vielzahl unbestimmter Rechtsbegriffe, die Auslegungsschwierigkeiten mit sich bringen, hat aber zugleich erkannt, dass es absolute Cybersicherheit nicht geben kann, so dass – immerhin – der Rückschluss vom Cybersicherheitsvorfall allein auf einen Produktfehler nicht möglich sein wird.

Auswirkungen auf die Lieferkette

Die Schärfe der Cybersicherheitsanforderungen schlägt auch auf die Lieferkette durch. Um im Schadensfall Ansprüche möglichst erfolgreich durchsetzen, aber auch – aus Sicht des zu Unrecht in Anspruch Genommenen – abwehren zu können, sollten die jeweiligen Pflichten und Verantwortlichkeiten in Bezug auf Cybersicherheitsanforderungen klar definiert und voneinander abgegrenzt werden. Beispielhaft zu nennen sind Regelungen zu SBOM-Pflichten (Software Bill of Material) und Schwachstellenmanagement, definierte Patch-SLAs (Service Level Agreements), koordinierte Offenlegung, Logging- und Forensic-Readiness, daneben Audit- und Informationsrechte, Benachrichtigungspflichten bei Sicherheitsvorfällen, transparente Updategovernance und klare Zuweisung von Verantwortlichkeit für Drittkomponenten.

> „Wer jetzt nicht aufklärt, ordnet und vertraglich vorsorgt, riskiert, dass der nächste Angriff nicht nur zum IT-, sondern auch zum Haftungsfall wird."

Hersteller wollen – um Regresslücken zu vermeiden – die für sie geltenden strengen Haftungsmaßstäbe möglichst vertraglich „flow-down" an Zulieferer weiterreichen. Lieferanten verfolgen naturgemäß das gegenteilige Ziel, nämlich die eigene Haftung gegenüber den Herstellern des Gesamtprodukts weitgehend zu beschränken. Unter versicherungsrechtlichen Gesichtspunkten sollten Zulieferer digitaler Komponenten darauf achten, keine Zusagen zu treffen, die über die gesetzliche Haftung hinausgehen, jedenfalls nicht ohne vorherige Einbindung ihres Produkthaftpflichtversicherers. Denn Standardpolicen decken regelmäßig nur die gesetzliche Haftung. Wer darüber hinausgehende Garantien – etwa „vollumfängliche Cyber-

resilienz“, Updateerfolgspflichten oder weitgehende Freistellungserklärungen – abgibt, riskiert unter Umständen gefährliche Deckungslücken. Unternehmen sind daher gut beraten, vor Beginn einer neuen Geschäftsbeziehung eine sorgfältige Vertragsprüfung unter Berücksichtigung der genannten versicherungsrechtlichen Implikationen durchführen zu lassen.

Herausforderungen in der Rechtsdurchsetzung

Auch die Rechtsdurchsetzung wird nach der neuen Produkthaftungsrichtlinie neu vermessen. Die Richtlinie senkt – getrieben von der sicherlich zutreffenden Annahme, dass die Darlegung eines vermeintlichen Produktfehlers im Vergleich zur alten Welt tendenziell komplexer wird – die Hürden für Geschädigte: Plausible Anhaltspunkte und erste Beweismittel können genügen, damit Gerichte die Offenlegung relevanter Unterlagen anordnen. Das ist dem deutschen Zivilprozess bislang fremd und trägt Züge der im US-amerikanischen Zivilprozess gängigen Discovery. Der deutsche Gesetzgeber hat mit dem neuen § 273a ZPO, der am 01.04.2025 in Kraft getreten ist, bereits eine Vorschrift zur Offenlegung von Geschäftsgeheimnissen geschaffen, die im Kontext künftiger Produkthaftpflichtfälle besonders relevant werden dürfte. Flankiert wird die Offenlegungspflicht von einer (teilweisen) Beweislastumkehr, wenn die technische oder wissenschaftliche Komplexität die Beweisführung erheblich erschwert.

Bejaht ein Gericht einen Produktfehler, stellt sich für den Hersteller die Frage, ob ihm der Entlastungsbeweis gelingt. Hier hat der europäische Gesetzgeber kaum zu überwindende Anforderungen postuliert: Liegt eine Sicherheitslücke vor, die nicht der Nutzer selbst dadurch verursacht hat, dass er notwendige Updates nicht installiert hat, gelingt eine Entlastung nur dann, wenn die Sicherheitslücke nach dem objektiven Stand der Wissenschaft und Technik zum Zeitpunkt des Inverkehrbringens oder der Inbetriebnahme des Produkts oder in dem Zeitraum, in dem sich das Produkt unter der Kontrolle des Herstellers befand, nicht erkannt werden konnte. Der objektive Stand von Wissenschaft und Technik stellt das denkbar höchste Anforderungsprofil dar, das über fortschrittliche, industrieübliche Standards hinausgeht und die „reine Lehre“ einschließt. In der Rechtsverteidigung wird elementar sein, darauf zu achten, dass Gerichte die Frage des Produktfehlers („angemessenes Cybersicherheitsniveau“) nicht mit der Frage der Vermeidbarkeit („Stand von Wissenschaft und Technik“) in unzulässiger Weise vermischen. Will ein Gericht die Frage klären, ob ein Produktfehler vorliegt, indem es nach der Vermeidbarkeit der Sicherheitslücke fragt, liegt eine unzulässige Vermischung der Ebenen des Fehlers und der Entlastung jedenfalls nicht fern.

All das macht aber auch deutlich: Erfolgreiche Rechtsverteidigung beginnt nicht erst im Prozess, sondern im Lifecycle: Wer auf saubere technische Dokumentation, Risikobeurteilung, Test- und Freigabeverfahren, Updatepolicy und insgesamt eine gute Lieferketten-Due-Diligence achtet, erhöht seine Chancen auf eine erfolgreiche Rechtsverteidigung. Abzuwarten bleibt, ob Haftpflichtversicherer künftig die entsprechende Dokumentation angesichts ihrer zunehmenden haftungsrechtlichen Bedeutung zur versicherungsvertraglichen Obliegenheit erheben mit der Folge, dass ihre Einhaltung allein schon zum Erhalt des Versicherungsschutzes geboten ist.

Fazit

Das Fazit fällt nüchtern aus: Die EU hebt die Produkthaftung ins digitale Zeitalter – und verschiebt die Risiken deutlich zu Lasten des Produktverantwortlichen. Die Cybersicherheitsanforderungen bilden den neuen Kern der Produktsicherheit; sie schärfen Haftungstatbestände und verlängern Risiken in die Nutzungsphase hinein. Für die Industrie heißt das: Rechtsverteidigung wird komplexer und Lieferkettengovernance wichtiger. Wer jetzt nicht aufklärt, ordnet und vertraglich vorsorgt, riskiert, dass der nächste Angriff nicht nur zum IT-, sondern auch zum Haftungsfall wird. ←

Der Cyber Resilience Act und seine Umsetzung im Unternehmen

Von der Theorie zur Praxis

Von Olga Stepanova, LL.M. (Berkeley), und Dr. Hauke Hansen

Unternehmen müssen sich trotz zahlreicher neuer Digitalgesetze frühzeitig und umfassend auf die Anforderungen des Cyber Resilience Act (CRA) vorbereiten, um die IT-Sicherheit und Marktfähigkeit ihrer digitalen Produkte in der EU ab 2027 sicherzustellen.

Olga Stepanova, LL.M. (Berkeley)
ByteLaw, Frankfurt am Main
Rechtsanwältin, Partnerin, Fachanwältin für IT-Recht, CIPP/E, zert. Datenschutzbeauftragte (TÜV)
stepanova@byte.law
www.byte.law

Dr. Hauke Hansen
FPS, Frankfurt am Main
Rechtsanwalt, Partner, Fachanwalt für IT-Recht, zert. Datenschutzbeauftragter (TÜV)
hansen@fps-law.de
www.fps-law.de

Der Cyber Resilience Act („CRA“) stellt eine zentrale europäische Produktsicherheitsverordnung dar, die den regulatorischen Rahmen für die Cybersicherheit von Produkten mit digitalen Elementen festlegt. Er reiht sich ein in eine Serie jüngst verabschiedeter europäischer Digitalgesetze, die auf eine Stärkung der IT-Sicherheit abzielen. Allerdings scheint sich der CRA im Schatten der übrigen Digitalgesetze zu bewegen, obwohl er bereits in Kraft getreten ist. Der Fokus der meisten Unternehmen liegt auf dem NIS2-Umsetzungsgesetz (NIS: Schutz von Netzwerk- und Informationssystemen), dessen Verabschiedung nach Bundestags- und Bundesratsbefassung für Ende 2025/Anfang 2026 erwartet wird, und dem Digital Operational Resilience Act („DORA“), der seit dem 17.01.2025 anwendbar ist und von der Finanz- sowie Versicherungswirtschaft einen einheitlichen – gesteigerten – IT-Sicherheitsstandard fordert.

Im Spannungsfeld zwischen Data Act, KI-Verordnung und den klassischen Fragen der DSGVO müssen sich betroffene Unternehmen zusätzlich mit dem CRA auseinandersetzen. Da ein erheblicher Teil der Anforderungen des CRA erst Ende 2027 umfassend anwendbar sein werden, liegt bei vielen Unternehmen der Fokus auf der etwaigen Erfüllung der noch vorher für sie verpflichtend werdenden Gesetze. Angesichts begrenzter personeller und finanzieller Ressourcen sowie einer zunehmenden Digitalrechtsumsetzungsfatigue erscheint dies nachvollziehbar. Dennoch ist in Anbetracht langer Entwicklungszyklen eine frühzeitige Auseinandersetzung mit den Anforderungen des CRA erforderlich, um sicherzustellen, dass die eigenen Produkte ab Ende 2027 in der Europäischen Union vertrieben werden können. Daneben müssen Hersteller schon ab dem 11.09.2026 Meldepflichten für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle mit Auswirkungen auf die Sicherheit von Produkten mit digitalen Elementen beachten. Um die kurze Frist von 24 Stunden für eine Frühwarnung einhalten zu können und währenddessen kurzfristig die richtigen Instanzen im Unternehmen einzubinden, ohne dass es zu Stillstand oder Fehlentscheidungen kommt, müssen Eskalationsprozesse bestehen, die nicht nur formal existieren, sondern auch gelebt werden. Sofern schon eingeübte Eskalationsprozesse für den Umgang mit Meldungen und Benachrichtigungen bei Datenpannen existieren, können die CRA-Meldepflichten hieran angelehnt werden.

Anforderungen nach dem CRA

Der CRA folgt in Anlehnung an die DSGVO und andere Digitalgesetze wie DORA und NIS2 dem sogenannten risikobasierten Ansatz. Danach muss ein Unternehmen, das CRA-regulierte Produkte vertreibt, einen umfassenden Risikomanagementrahmen aufsetzen. Betroffene Unternehmen müssen dafür die eigenen Risiken kennen, angemessene risikoverringernde Maßnahmen ergreifen und deren Wirksamkeit überprüfen. Dieser Zyklus von Risikoerkennung, Maßnahmenengreifung und Maßnahmenüberprüfung muss dabei regelmäßig wiederholt werden.

Diese Verpflichtung gilt dabei für „Produkte mit digitalen Elementen“, die in der Europäischen Union in Verkehr gebracht werden. Nach dem CRA sind „Produkte mit digitalen Elementen“ solche, die über eingebaute digitale Komponenten Funktionen ausführen oder Daten verarbeiten. Dazu zählen beispielsweise Geräte oder Maschinen mit Softwaresteuerung, Produkte mit Vernetzungsschnittstellen sowie Hardware, in die Software integriert ist und die für den Betrieb des Produkts wesentlich ist. Kurz gesagt umfasst die Verordnung alle physischen Produkte, deren Funktionalität direkt oder indirekt von digitalen Elementen abhängt.

Grundlegende Sicherheitsanforderungen

Im Kern verlangt der CRA in seinem Anhang I die Erfüllung grundlegender Sicherheitsanforderungen, die die Minimierung bekannter Schwachstellen, den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit sowie die Einführung wirksamer Zugriffsbeschränkungen und Authentifizierungssysteme zum Gegenstand haben. Teil hiervon ist auch die Implementierung eines Schwachstellenmanagements. Angesichts immer komplexer werdender Technik und der damit stetig wachsenden Gefahr des Bestehens und Ausnutzens von Sicherheitslücken gewinnt das Schwachstellenmanagement immer mehr an Relevanz.

Systematische Risikobewertung und „Softwarestückliste“

Für jedes CRA-regulierte Produkt muss eine systematische Risikobewertung nach Art. 13 Abs. 2 bis 3 CRA vorgenommen werden, wobei die potentiellen Cyberrisiken

bereits in der Konzeptionierungsphase des Produkts und sodann fortlaufend bewertet werden müssen.

Hinzu tritt die Verantwortlichkeit für in den Produkten eingesetzte Drittkomponenten, insbesondere Open-Source-Bibliotheken. Aus diesem Grund muss für jedes Produkt eine sogenannte Softwarestückliste geführt werden. Diese „Software Bill of Materials“ (SBOM) ermöglicht es, bei Bekanntwerden von Schwachstellen umgehend nachzuvollziehen, inwiefern die eigenen Produkte betroffen sind, so dass angemessene Gegenmaßnahmen eingeleitet werden können. Dies ist auch relevant in Bezug auf die Meldepflichten bei Schwachstellen und Sicherheitsvorfällen (vgl. Art. 13 und Art. 14 CRA).

Neben Informationspflichten gegenüber Nutzern, zum Beispiel Anleitungen für die sichere Installation und Inbetriebnahme, müssen Hersteller sicherstellen, dass das Produkt für die gesamte erwartetet Nutzungsdauer, mindestens jedoch fünf Jahre, Sicherheitsupdates erfährt.

Wie Unternehmen vorgehen können

Ein häufiges Problem bei der Umsetzung vieler Digitalakte liegt – gemessen am Maßstab dieser neuen Gesetze – in der oftmals unvollständigen und inkonsistenten Dokumentation in den Unternehmen.

Der risikobasierte Ansatz verlangt von den Unternehmen, die Risiken sowie die sie mitigierenden Maßnahmen zu dokumentieren und sie regelmäßig einer dokumentierten Wirksamkeitsprüfung zu unterziehen. Es reicht nicht mehr aus, standardisierte Checklisten abzuarbeiten. Vielmehr muss man die unternehmensindividuellen Risiken ermitteln und entsprechend maßgeschneiderte Sicherheitsmaßnahmen implementieren, um eine Abstimmung auf das jeweilige Produkt zu gewährleisten. Da diese Herangehensweise für viele der betroffenen Unternehmen – jedenfalls im Bereich der Produktsicherheit digitaler Produkte – ein Umdenken erfordert, muss auch hier ein Risikomanagementrahmen etabliert werden.

Ein ähnliches Defizit zeigt sich beim Schwachstellenmanagement: Unternehmen haben teils keine oder nur unzureichende Dokumentationen darüber, wie Schwachstellen identifiziert, bewertet und behandelt werden. Zudem ist oft unklar, welche Stelle im Unternehmen für das Schwachstellenmanagement verantwortlich ist.

> „Ein häufiges Problem bei der Umsetzung vieler Digitalakte liegt (...) in der oftmals unvollständigen und inkonsistenten Dokumentation in den Unternehmen.“

Sicherlich können viele Unternehmen ad hoc reagieren und Schwachstellen bei Gefahr in Verzug identifizieren. Allerdings erfolgt dies meist ohne Einbettung in einen formalisierten Prozess, die in Zukunft vom CRA vorausgesetzt wird.

Im ersten Schritt empfiehlt sich eine umfassende Bestandsaufnahme mit anschließender Lückenanalyse (Gap-Analyse), um zu ermitteln, in welchen Fachabteilungen bereits verwertbare Dokumentationen vorliegen, die lediglich angepasst oder erweitert werden müssen, und wo ein vollständiger Neuaufbau erforderlich ist. Sodann sollten die Rollen und Verantwortlichkeiten im CRA-Umsetzungsprojekt geklärt und interdisziplinäre Teams – bestehend aus Entwicklung, IT, Recht und Management – gebildet werden, die über den Fortschritt regelmäßig berichten.

Inhaltliche Umsetzung des CRA

Einer der ersten inhaltlichen Schritte dürfte die Klassifizierung der einzelnen Produkte entsprechend dem Anhang III zum CRA zum Gegenstand haben. Das Ergebnis entscheidet darüber, ob nur die grundlegenden Cybersicherheitsanforderungen für einzelne Produkte gelten oder weitergehende Pflichten. Letzteres ist beispielsweise der Fall, wenn es sich um kritische Produkte wie Firewalls oder Intrusion-Detection-Systeme handelt.

Die Anforderungen des CRA sollten tief in die Produktentwicklung eingreifen und Sicherheit durch Gestaltung und entsprechende Voreinstellungen gewährleisten. Daher müssen aktuelle Einstellungen überprüft, bei Bedarf angepasst und dokumentiert werden. Dabei ist an die Integration einer Bedrohungsmodellierung („Threat Modeling“) und umfassender Risikoanalysen in der Produktentwicklung zu denken. Auch sollten sichere Entwicklungsstandards, zum Beispiel OWASP (Open

Web Application Security Project), und automatisierte Tests zum Pflichtrepertoire gehören. All das wird zwangsläufig zur Stärkung der DevSecOps-Kultur, das heißt der Integration von Sicherheit in alle Phasen der Softwareentwicklung, führen. Dann wird, so das Ziel des EU-Gesetzgebers, die Sicherheit kein nachgelagerter Schritt mehr sein, sondern von Anfang an integriert werden.

Eine weitere gesetzliche Anforderung ist die Einführung eines strukturierten Schwachstellenmanagements. Es müssen dokumentierte Prozesse zur Erkennung, Bewertung und Behebung von Sicherheitslücken vorhanden sein, und die Behebung von Schwachstellen darf nicht dem Zufall überlassen werden.

Daneben lohnt es sich, eine Kommunikationsstrategie zu entwickeln, um transparent über Schwachstellen und Updates zu informieren, ohne hierbei die Reputation des Unternehmens zu beschädigen. Schließlich ist das Auftreten von Schwachstellen normal, es geht daher vielmehr um die Frage, wie man damit rechtskonform und reputationswahrend umgeht.

Angesichts der Tatsache, dass Softwarebestandteile nicht ausschließlich unternehmensintern entwickelt werden, sondern häufig aus Auftragsentwicklungen stammen, ist eine sorgfältige Prüfung der entsprechenden Verträge unerlässlich. Im besten Fall verpflichten die Verträge den Entwickler schon, die Software nicht nur gemäß den beauftragten Spezifikationen, sondern auch unter Einhaltung der regulatorischen Anforderungen des Auftraggebers zu entwickeln. Sollte dies nicht der Fall sein, empfiehlt es sich, frühzeitig Vertragsanpassungen vorzunehmen und neue Vereinbarungen mit entsprechenden Verpflichtungen abzuschließen. Der Auftragnehmer sollte unbedingt eine detaillierte SBOM erstellen, um dem Auftraggeber die Erfüllung seiner Pflichten gemäß dem CRA zu ermöglichen.

Auch eine Schulungsstrategie ist unerlässlich, damit Entwickler sichere Programmierpraktiken anwenden, die IT-Teams das Schwachstellenmanagement beherrschen und im Fall eines Incidents entsprechend den aufgestellten Richtlinien darauf reagieren. Die Umsetzung des CRA ist nicht nur Aufgabe der erweiterten IT-Abteilung, sondern Chefsache. Daher müssen sowohl die Geschäftsführung als auch der Einkauf und Vertrieb zu den rechtlichen und geschäftlichen Implikationen des CRA geschult werden. Eine wertvolle Hilfestellung, insbesondere für KMU, bietet die dreiteilige technische Richtlinie **TR-03183** des BSI.

Fazit

Obwohl die Umsetzung des CRA angesichts der Vielzahl neuer digitalrechtlicher Regelwerke derzeit bei vielen Unternehmen in den Hintergrund tritt, dürfen die Anforderungen und Pflichten des CRA keinesfalls vernachlässigt werden. Damit Produkte mit digitalen Elementen künftig in der EU vertrieben werden können, ist an verschiedenen Stellen ein strategisches Umdenken erforderlich.

Der Grundstein für eine erfolgreiche Umsetzung darf angesichts langer Entwicklungszyklen nicht erst im Jahr 2027 gelegt werden, sondern muss bereits jetzt vorbereitet werden. Unternehmen, die frühzeitig mit der Analyse, Planung und Anpassung ihrer Prozesse beginnen, sichern sich nicht nur regulatorische Compliance, sondern schaffen zugleich Wettbewerbsvorteile und stärken damit ihre Resilienz in einem zunehmend komplexen digitalen Umfeld. ←

Abkehr von Microsoft

Wie Deutschland seine technologische Zukunft nachhaltig sichert

Von Prof. Dr. Dennis-Kenji Kipker

Deutschland muss die Abhängigkeit von Tech-Monopolen wie Microsoft durch den Aufbau eines offenen, multianbieterfähigen digitalen Ökosystems überwinden, um Cybersicherheit, Wettbewerb und digitale Souveränität nachhaltig zu stärken.

Das Problem: Tech-Monopole

Kürzlich äußerte BSI-Präsidentin Claudia Plattner, dass digitale Souveränität für Deutschland vorläufig unerreichbar sei – zu groß sei die technologische Abhängigkeit von Soft- und Hardware aus dem Ausland. Dafür erntete sie in einem offenen Brief der Open Source Business Alliance (OSBA) erheblichen Widerspruch (siehe **hier**). In der aktuellen Debatte jedoch übersehen beide Seiten einen wichtigen gemeinsamen und grundlegenden Nenner: die Beendigung der technologischen Erpressbarkeit durch Tech-Monopolisten, die jahrzehntelang deutsche Kunden an sich gebunden und auf diese Weise gezielt zunächst auf dem Software- und nachfolgend auf dem Cloudmarkt einen freien Wettbewerb behindert haben. Die beim Aufspalten eines solchen Monopols entstehende Wahlfreiheit würde Vorteile mit sich bringen, die weit über die abstrakte Forderung nach digitaler Souveränität hinausgehen: Dazu gehören geringere Kosten, bessere Cybersicherheit, mehr Wettbewerb und damit letzten Endes ein erfolgversprechenderes Umfeld, in dem Unternehmen und Organisationen ihre digitalen Infrastrukturen frei nach ihrem Willen gestalten können, ohne sich von einem einzelnen Anbieter strukturell abhängig zu machen.

Prof. Dr. Dennis-Kenji Kipker
cyberintelligence.institute, Frankfurt am Main
Research Director, Professor für IT-Sicherheitsrecht und Berater der Bundesregierung
dennis.kipker@cyberintelligence.institute
www.cyberintelligence.institute

Aktuelle Entwicklungen: Es ist was los im Staate Dänemark

Umso mehr zu begrüßen ist deshalb auch der jüngste Vorstoß des neuen Bundesministeriums für Digitales und Staatsmodernisierung (BMDS), den bisher umfassenden Einsatz von Microsoft-Produkten in der Bundesverwaltung nicht nur zu überprüfen, sondern auch kritisch zu hinterfragen und entsprechende Ausstiegsoptionen aufzuzeigen (siehe **hier**). Eine ganz ähnliche Richtung schlägt das Land Schleswig-Holstein ein, indem es Büroanwendungen von Microsoft – und damit im Regelfall gleichzeitig auch den Zwang, dessen Cloud zu verwenden – strategisch aus dem Produktivbetrieb in der Verwaltung verbannt (siehe **hier**). Doch auch international zeigen sich mittlerweile ähnliche Entwicklungen: Wo man jahrzehntelang auf die Technik weitestgehend eines einzelnen Anbieters vertraut hat, bahnt sich ein gravierender Wechsel in der digitalen Verwaltungsinfrastruktur an, denn diese ist nicht nur wichtig, sondern gar systemkritisch. So kündigte beispielsweise Dänemark im Sommer dieses Jahres an, in den kommenden Monaten komplett auf Microsoft-Software zu verzichten – und das im Rekordtempo, denn bis zum Herbst dieses Jahres schon solle das komplette dänische Digitalministerium „von Microsoft befreit sein“ (siehe **hier**).

Und in der Tat erfolgt der globale Umstieg auf IT-Alternativen jenseits der großen Monopole mit System. Richtigerweise betont daher die dänische Digitalministerin auch, dass es nicht um Microsoft allein geht, sondern man generell deutlich zu abhängig von einigen wenigen Anbietern sei – der Softwarekonzern aus Redmond ist in dieser Debatte aber nicht selten der primäre Stein des Anstoßes, weil die Abhängigkeiten hier im Vergleich mit anderen Anbietern noch deutlich massiver ausgeprägt sind. Denn nicht umsonst wird festgestellt, dass das Betriebssystem und die Office-Software in Deutschland private und dienstliche Endgeräte gleichermaßen dominieren. Doch nicht nur das: Über die Cloud versucht Microsoft gezielt, neue User an seine Produkte zu binden, indem diese über das Angebot eines kompletten Ökosystems in einem „goldenen Käfig“ gefangen werden, der mit der Integration nicht nur von Produktivitätssoftware in die Cloud, sondern mittlerweile auch der künstlichen Intelligenz immer massiver wird (siehe **hier**) – im Ergebnis eine toxische Mischung.

Ein digitalsouveränes Deutschland …

Aber es geht hier nicht allein um wettbewerbsrechtliche Fragen, sondern auch um Fragen der Cybersicherheit und der unfairen Preisgestaltung: Denn wo einmal ein Monopol besteht, wird dieses in aller Regel auch zum eigenen Vorteil ausgenutzt. Nicht anders ist das auch bei Microsoft, indem der Konzern seinen Kunden kaum Einblicke in seine technische Infrastruktur unterhalb der Benutzeroberfläche gewährt, keine nennenswerten Mitspracherechte bei der Produktplanung und Systemgestaltung möglich sind und letztlich eine viel zu geringe Verhandlungsmacht bei der Preisgestaltung besteht – weil man sich eben jahrelang auch um eine Alternative nicht ernsthaft bemüht hatte. Genau diesen Missstand prangert letztlich auch die OSBA in ihrem offenen Brief an BSI-Präsidentin Claudia Plattner vom 26.08.2025 an, indem festgestellt wird, dass es sehr wohl möglich sei, ein digitalsouveränes Deutschland aufzubauen – man muss es eben nur wollen, indem man gezielt bestehende Monopole aufbricht und Deutschland dadurch erst wieder digital handlungsfähig macht (siehe **hier**).

… gibt es nicht zum Nulltarif

Definitiv behauptet niemand, dass ein solcher Schritt einfach oder gar kostenneutral wäre – im Endeffekt gewinnen wir mit einem Ausschluss von Microsoft aus der öffentlichen Verwaltung in Deutschland aber deutlich mehr, als wir verlieren könnten. Denn in einem Zeitalter, in dem es immer mehr auch um die Vertrauenswürdigkeit von Technologien und Herstellern geht, hat Microsoft in den letzten Monaten und Jahren schon mehrfach sehr deutlich gezeigt, dass ebenjene Vertrauenswürdigkeit nicht vorhanden ist, so zuletzt in diesem Jahr mit der kritischen Sharepoint-Sicherheitslücke mit erheblichen Folgen für die Sicherheit und Vertraulichkeit von sensiblen Daten, von der deutsche Unternehmen, Behörden und Bildungseinrichtungen im europaweiten Vergleich am stärksten betroffen gewesen sind, wie noch Anfang August berichtet wurde (siehe **hier**).

Doch gerade aufgrund der in den vergangenen Jahrzehnten aufgebauten erheblichen Abhängigkeiten von einem einzelnen Softwareanbieter ist es jetzt umso wichtiger, den Umstieg nicht überstürzt anzugehen, sondern mit System zu planen. Denn gerade die öffentliche Hand ist es, die hier mit gutem Beispiel vorangehen müsste, weil die staatliche Beschaffungspolitik nicht nur nationa-

len Vorbildcharakter hat, sondern weil gerade vom Bund eine signifikante Hebelwirkung ausgeht, die sich bei einer Abkehr von Microsoft-Software und -Cloud auch in den einzelnen Bundesländern deutlich bemerkbar machen dürfte. Nicht ohne Grund ist der Deutschland-Stack – auch „D-Stack" genannt – eines der zentralen Flaggschiffvorhaben des BMDS, das bis zum Jahr 2028 abgeschlossen sein soll. Das Ziel: der Aufbau eines „strategischen Plattformkernsystems", das zukünftig als Basis für die gemeinsame digitale Infrastruktur dient und von der öffentlichen Hand und privaten Anbietern gleichermaßen betrieben und weiterentwickelt wird, um ein lebendiges Ökosystem für digitale Lösungen zu schaffen (siehe **hier**). Der D-Stack soll am Ende eine einheitliche IT-Infrastruktur zur Verfügung stellen, die sich aus Basiskomponenten wie Cloud- und IT-Diensten, Fachplattformen und Schnittstellen mit Fokus auf Cybersicherheit und damit Datenvertraulichkeit zusammensetzt, um die IT-Infrastruktur zu konsolidieren, Standards zu setzen, Anwendungen zu verbessern und Ressourcen zu sparen (siehe **hier**). Letztlich kann ein solch ambitioniertes Projekt aber nur dann gelingen, wenn man in Sachen Verwaltungsdigitalisierung nicht von einem einzelnen Anbieter abhängig ist, sondern wenn ein freies Ökosystem mit einer realen Wahl- und Entscheidungsfreiheit auf dem Software- und Cloudmarkt vorhanden ist.

Digitale Innovation durch digitale Wahlfreiheit

Die Vorteile eines solchen Multi-Cloud-Systems liegen auf der Hand. So könnten öffentliche Einrichtungen und Unternehmen die für sie passendsten Dienste und Plattformen darin aussuchen, ohne von einem einzelnen Anbieter abhängig zu sein. Überdies können spezifische Anforderungen besser erfüllt und die Betriebskosten gesenkt werden, indem reale Verhandlungsspielräume nutzbar sind. Doch nicht nur das: Mit der Reduzierung der Abhängigkeit von einem einzelnen Anbieter ist im Regelfall ebenso eine erhöhte Zuverlässigkeit und Ausfallsicherheit verbunden, denn durch die Verteilung des Workloads optimalerweise über verschiedene Cloudumgebungen hinweg wird zugleich eine bessere Redundanz geschaffen (siehe **hier**).

> „Es geht nicht allein um wettbewerbsrechtliche Fragen, sondern auch um Fragen der Cybersicherheit und der unfairen Preisgestaltung."

Zu lange haben wir uns in Deutschland in Sachen Software und Cloud mit Microsoft auf einen einzelnen Anbieter verlassen, der dies über Jahre hinweg auch gründlich ausgenutzt hat. Nun aber ist die Zeit für den Wechsel gekommen – und bei einer Betrachtung der Gesamtumstände ist ein solcher Wechsel nicht nur notwendiger, sondern auch günstiger denn je. Das Aufbrechen von Monopolen und der Aufbau von realer digitaler Wahlfreiheit zwischen den verschiedenen Alternativen im Cloud- und Softwareumfeld sichert Deutschlands digitale Innovation und Souveränität nicht nur jetzt, sondern, als nachhaltige strategische Investition verstanden, auch in Zukunft. ←

Giovanni Brugugnone
Fresenius Medical Care, Bad Homburg
Data Protection Officer

giovanni.brugugnone@fmc-ag.com

Volker Buß
Merck Group, Darmstadt
Chief Security Officer

volker.buss@merckgroup.com

Christoph Dahl
SCHOTT AG, Mainz
Data Protection & Human Rights Officer/Senior Compliance Manager

christoph.dahl@schott.com

Jürgen Grommes
Nestlé Deutschland AG, Frankfurt am Main
Z-EUR IT Security & Compliance Governance Manager

juergen.grommes@de.nestle.com

Jutta Löwe
Continental AG, Hannover
Head of Data Compliance / Chief Data Compliance Officer

jutta.loewe@conti.de

Iskro Mollov
GEA Group Aktiengesellschaft, Düsseldorf
Senior Vice President / Chief Information Security Officer

iskro.mollov@gea.com

Dr. Nicole Monleon de Wallmann
Panasonic Europe B.V., Hamburg
Senior Legal Counsel | Head of Data Protection

nicole.monleondewallmann@eu.panasonic.com

Dr. Andreas Peya
Verizon Deutschland GmbH, Frankfurt am Main
Director Regulatory & Govt. Affairs Central & Eastern Europe

andreas.peya@de.verizon.com

Prof. Dr. Igor Podebrad
Google, Frankfurt am Main
Director, Office of the CISO, Google Cloud

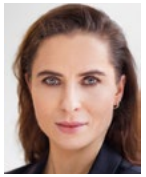
igorpodebrad@google.com

David Sänger
GEA Group AG, Düsseldorf
Vice President Data Protection, IT and Digitalization, Group Data Protection Officer

david.saenger@gea.com

Ulrike-Beate Schroth
Deutsche Telekom Security GmbH, Bonn
Management Sicherheit & Recht

ulrike-beate.schroth@telekom.de



Prof. Dr. Haya Schulmann
Goethe-Universität Frankfurt und ATHENE, Frankfurt am Main
Professorin und Board Mitglied

schulmann@em.uni-frankfurt.de

Hendrik Seidel
OBI Group Holding SE & Co. KGaA , Wermelskirchen
Principal Legal Counsel

hendrik.seidel@obi.de

Jörg Steinhaus
BarmeniaGothaer, Köln
Konzerndatenschutzbeauftragter

joerg.steinhaus@gothaer.de

Dr. Anna-Miriam Tresselt
Deutsche Bahn AG, Frankfurt am Main
Senior Legal Counsel

anna-miriam.tresselt@deutschebahn.com

Bernd Vellguth
Microsoft Deutschland GmbH, München
Specialist for Risk Management and Compliance

berndv@microsoft.com

Tobias Wahl
Heraeus Consulting & IT Solutions GmbH, Hanau
Head of Cybersecurity & Risk Advisory

tobias.wahl@heraeus.com

Matthias Woldter
Commerzbank AG, Frankfurt am Main
Managing Director Group Legal/Divisional Head Technology, Data & Infrastructure

matthias.woldter@commerzbank.com

Strategische Partner und Kooperationspartner

Bastian Finkel
BLD Bach Langheid Dallmayr Rechtsanwälte Partnerschaftsgesellschaft mbB
Geschäftsführender Partner
Theodor-Heuss-Ring 13-15
50668 Köln
Telefon: 0221/944027-400

bastian.finkel@bld.de
www.bld.de

Dr. Alexander Beyer
BLD Bach Langheid Dallmayr Rechtsanwälte Partnerschaftsgesellschaft mbB
Partner
Theodor-Heuss-Ring 13-15
50668 Köln
Telefon: 0221/944027-894

alexander.beyer@bld.de
www.bld.de

Volker Heck
Deekeling Arndt Advisors in Communications GmbH
Senior Partner
Lindleystraße 8c
60314 Frankfurt am Main
Telefon: 069/97098550

volker.heck@h-advisors.global
www.deekeling-arndt.com

Dr. Hauke Hansen
FPS Rechtsanwaltsgesellschaft mbH & Co. KG
Partner, Fachanwalt für IT-Recht, zert. DSB (TÜV)
Eschersheimer Landstr. 25-27
60322 Frankfurt am Main
Telefon: 069/95957-237

hansen@fps-law.de
www.fps-law.de

Dr. Philip Kempermann, LL.M.
Heuking Kühn Lüer Wojtek
Managing Partner
Georg-Glock-Straße 4
40474 Düsseldorf
Telefon: 0211/60055-166

p.kempermann@heuking.de
www.heuking.de

Dr. Lutz Martin Keppeler
Heuking Kühn Lüer Wojtek
Partner, Fachanwalt für Informationstechnologierecht
Magnusstraße 13
50672 Köln
Telefon: 0221/2052-436

l.keppeler@heuking.de
www.heuking.de

Michael Kuska, LL.M., LL.M. (Düsseldorf)
Heuking Kühn Lüer Wojtek
Salaried Partner, Leiter der Expertisegruppe Informationssicherheit
Georg-Glock-Straße 4
40474 Düsseldorf
Telefon: 0211/60055-166

m.kuska@heuking.de
www.heuking.de

Strategische Partner

BLD

FPS
Ihre Kanzlei. Ihr Partner.

HEUKING

Kooperationspartner

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

H/ADVISORS
Deekeling Arndt

„Strategische Partner“ und „Kooperationspartner“

Die Strategischen Partner von CyberSecurityQuarterly sind führende Anwaltssozietäten und Wirtschaftsprüfungsgesellschaften; die Kooperationspartner von CyberSecurityQuarterly sind anerkannte wissenschaftliche Organisationen oder Unternehmen mit inhaltlichen Bezügen zum Rechtsmarkt. Alle Strategischen Partner und Kooperationspartner respektieren ohne Einschränkung die Unabhängigkeit der Redaktion, die sie fachlich und mit ihren Netzwerken unterstützen. Sie tragen damit zum Erfolg des Magazins CyberSecurityQuarterly bei.

Impressum

Herausgeber: Prof. Dr. Thomas Wegerich

Redaktion: Thomas Wegerich (tw, V.i.S.d.P.),
Karin Gangl, Dr. Thomas R. Wolf

Verlag: F.A.Z. BUSINESS MEDIA GmbH –
Ein Unternehmen der F.A.Z.-Gruppe

Geschäftsführung: Dominik Heyer, Hannes Ludwig
Pariser Straße 1, 60486 Frankfurt am Main

Sitz: Frankfurt am Main,
HRB Nr. 53454, Amtsgericht Frankfurt am Main

German Law Publishers GmbH:
Verleger: Prof. Dr. Thomas Wegerich
Stalburgstraße 8, 60318 Frankfurt am Main
Telefon: 069 95 64 95 59
E-Mail: redaktion@deutscheranwaltspiegel.de
Internet: www.cybersecurity-quarterly.de

Verantwortlich für das Internetangebot
www.cybersecurity-quarterly.de
F.A.Z. BUSINESS MEDIA GmbH –
Ein Unternehmen der F.A.Z.-Gruppe

Jahresabonnement:
Bezug kostenlos, Erscheinungsweise: quartalsweise

Projektmanagement: Karin Gangl
Telefon: 069 75 91-22 17

Layout: Jan Hofmann

Strategische Partner: BLD Bach Langheid Dallmayr Rechtsanwälte Partnerschaftsgesellschaft mbB; FPS Rechtsanwaltsgesellschaft mbH & Co. KG; Heuking Kühn Lüer Wojtek Partnerschaft mit beschränkter Berufshaftung von Rechtsanwälten und Steuerberatern

Kooperationspartner: Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE; Deekeling Arndt Advisors in Communications GmbH

Haftungsausschluss: Alle Angaben wurden sorgfältig recherchiert und zusammengestellt. Für die Richtigkeit und Vollständigkeit des Inhalts von SustainableValue übernehmen Verlag und Redaktion keine Gewähr.

Genderhinweis: Wir streben an, gut lesbare Texte zu veröffentlichen und in unseren Texten alle Geschlechter abzubilden. Das kann durch Nennung des generischen Maskulinums, Nennung beider Formen („Unternehmerinnen und Unternehmer“ bzw. „Unternehmer/-innen“) oder die Nutzung von neutralen Formulierungen („Studierende“) geschehen. Bei allen Formen sind selbstverständlich immer alle Geschlechtergruppen gemeint – ohne jede Einschränkung. Von sprachlichen Sonderformen und -zeichen sehen wir ab.

Eine Gemeinschaftspublikation von:

F.A.Z. BUSINESS MEDIA
Ein Unternehmen der F.A.Z.-Gruppe

GLP German Law Publishers