Deutscher AnwaltSpiegel Spezial 2023

Cybersicherheit: Unternehmen im Fokus – Strategien für den Cyberkampf

Eine Publikation von

Deutscher AnwaltSpiegel

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

Linklaters

BRUNSWICK

valantic

Inhalt

Impressum

Herausgeber
Deutscher AnwaltSpiegel,
F.A.Z. BUSINESS MEDIA GmbH –
Ein Unternehmen der F.A.Z.-Gruppe,
German Law Publishers GmbH,
Linklaters, Brunswick, valantic

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
HRB Nr. 53454,
Amtsgericht Frankfurt am Main
www.faz-bm.de

German Law Publishers GmbH
Verleger: Prof. Dr. Thomas Wegerich
Stalburgstraße 8, 60318 Frankfurt am Main
Telefon: +49 (0)69 95 64 95 59
thomas.wegerich@germanlawpublishers.com

Projektmanagement
Karin Gangl
F.A.Z. BUSINESS MEDIA GmbH
Telefon: +49 (0)69 75 91-22 17
redaktion@deutscheranwaltspiegel.de

Redaktion
Thomas Wegerich (V.i.S.d.P.);
Karin Gangl, Michael Dörfler,
Dr. Thomas R. Wolf
F.A.Z. BUSINESS MEDIA GmbH

Layout
Christine Lambert
F.A.Z. BUSINESS MEDIA GmbH

Titelfoto
© ADDICTIVE STOCK – stock.adobe.com

Druck und Verarbeitung:
FLYERALARM GmbH,
Alfred-Nobel-Str. 18, 97080 Würzburg

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

Teamgeist und Transparenz in der Krise

Sehr geehrte Leserinnen und Leser,

wenn es um das Thema Cybersicherheit geht, muss ich Ihnen leider gleich zu Beginn eine Hoffnung nehmen. Vollständige Sicherheit im Netz gibt es nicht – und wird es auch nie geben. Wir von TRILUX waren Anfang 2020 selbst von einer Hackerattacke betroffen und haben von allen IT-Spezialisten unisono gehört: „Sie sind NIE sicher." Das heißt, wir rechnen eigentlich IMMER mit einem weiteren IT-Angriff – und bereiten uns entsprechend vor.

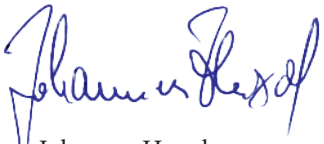
Damals hatte ein Virus große Teile unserer Server-, Infrastruktur- und Endgerätelandschaft infiziert und selektiv lahmgelegt. Die Produktion an unseren Standorten in Europa stand drei Tage lang still. Unser Expertenteam identifizierte innerhalb kurzer Zeit einen gezielten Angriff auf unser Netzwerk. Glücklicherweise waren wir mit einem Notfallmaßnahmenpaket auf ein derartiges Krisenszenario vorbereitet, wenn auch nicht in diesem Ausmaß. Ein zentraler Baustein dabei: Schnelligkeit und maximale Transparenz in Richtung Kunden und Mitarbeiterschaft.

Mit Klarheit und beherztem, mutigem Handeln haben wir den Schaden für unser Unternehmen minimieren können. Statt den Vorfall herunterzuspielen, wurden alle relevanten Partner unverzüglich über den Hackerangriff informiert, um Schäden von deren Systemen abzuwenden. Gleichzeitig mobilisierten wir unsere Mitarbeiter und richteten sofort einen War-Room ein. Mit der Unterstützung kompetenter externer Spezialisten wurde binnen eines Tages entschieden, eine komplett neue Infrastruktur inklusive aller Endgeräte aufzubauen. Dies ist, gesteuert durch das Kernteam, in beeindruckender Geschwindigkeit gelungen. Währenddessen hielt das gesamte #TeamTRILUX das operative Tagesgeschäft dank einer großartigen Teamleistung am Leben, um unsere Kunden auch weiterhin bestmöglich zu betreuen.

Bereits am dritten Tag nach dem Cyberangriff gingen die ersten Systeme wieder ans Netz. Die vollständige Wiederherstellung dauerte jedoch Monate bis Jahre. Ergebnis dieses Prozesses: eine stärkere IT-Infrastruktur, eine intensivere Digitalisierung des Gesamtunternehmens und ein hohes Bewusstsein für IT-Sicherheit. Gleichzeitig konnten wir unsere Kundenbeziehungen durch Transparenz und Offenheit stärken. Vor allem aber sind wir als Team noch enger zusammengerückt.

Unterm Strich haben wir durch die Attacke eine wichtige Lektion gelernt: Zwar gibt es keine totale Cybersicherheit – man kann sich aber bestmöglich auf den Fall der Fälle vorbereiten. Dazu möchte ich Sie alle ermutigen, auch wenn ich hoffe, dass Sie nie in diese Situation kommen mögen.

Ihr



Johannes Huxol
CFO TRILUX

Herausforderung Cybersicherheit

Liebe Leserin, lieber Leser,

die Auseinandersetzung mit dem Thema Cybersicherheit ist für Unternehmen im digitalen Zeitalter zentral. Denn die Frage lautet längst nicht mehr, ob ein Unternehmen Opfer eines Cyberangriffs werden kann, sondern allenfalls, wann es so weit ist.

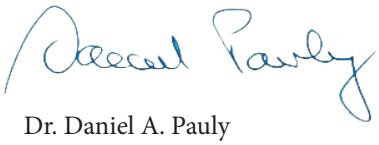
Auch Unternehmen, die bereits in die Sicherheit ihrer Cyberinfrastruktur investiert haben, werden von der Professionalität und Effizienz der Angreifer häufig überrascht: Cyberattacken gehen nicht mehr von dem einzelnen Computernerd aus, dessen Bild der Begriff „Hacker“ noch immer vor dem geistigen Auge heraufbeschwört. Vielmehr handelt es sich um hochprofessionelle kriminelle Gruppen, deren organisiertes, arbeitsteiliges Vorgehen das Schädigungspotential deutlich erhöht.

Die gute Nachricht ist: Bei entsprechender Vorbereitung sind Unternehmen solchen Cyberangriffen nicht schutzlos ausgeliefert. Zuständigkeiten, Kommunikationskanäle und Erste-Hilfe-Maßnahmen können im Vorfeld festgelegt und in Simulationen erprobt werden. Dies trägt entscheidend dazu bei, dass im Ernstfall verschiedene Unternehmensbereiche an einem Strang ziehen und das Ausmaß drohender Schäden erheblich vermindert wird.

Ein derartig umfassender Ansatz spiegelt sich auch in den Beiträgen wider, die wir in diesem Heft versammeln konnten. Von straf- und arbeitsrechtlichen Themen über Krisenkommunikation bis hin zum „Dauerbrenner“ Datenschutz bilden die Artikel ein breites Themenspektrum ab. Wir freuen uns, Ihnen hiermit einen möglichst vielseitigen Überblick darüber zu geben, wie Sie die Vorbereitung, Reaktion und Kommunikation mit Blick auf das Eintreten eines Cybersicherheitsvorfalls in Ihrem Unternehmen gestalten können.

Ich wünsche Ihnen eine spannende Lektüre!

Ihr



Dr. Daniel A. Pauly
Linklaters

Mit Transparenz den Hackern einen Schritt voraus sein

Präventivmaßnahmen können den entscheidenden Unterschied machen

Von Thomas Lang

Cybersicherheit befasst sich mit dem Schutz von Computersystemen, Netzwerken und Daten vor digitalen Bedrohungen. Dabei geht es nicht nur um den Schutz vor unerlaubten Zugriffen, sondern auch darum, die Integrität, Verfügbarkeit und Vertraulichkeit von Daten zu gewährleisten. Die Gefahren, denen sich Unternehmen gegenübersehen, reichen von Malware, Täuschungsversuchen und erpresserischen Ransomwareattacken bis hin zu ausgeklügelten „Man-in-the-Middle"-Angriffen, bei denen unternehmensinterne Kommunikationskanäle belauscht werden. Jeder dieser Angriffe kann erhebliche finanzielle Verluste verursachen, den Ruf eines Unternehmens schädigen und rechtliche Konsequenzen nach sich ziehen.

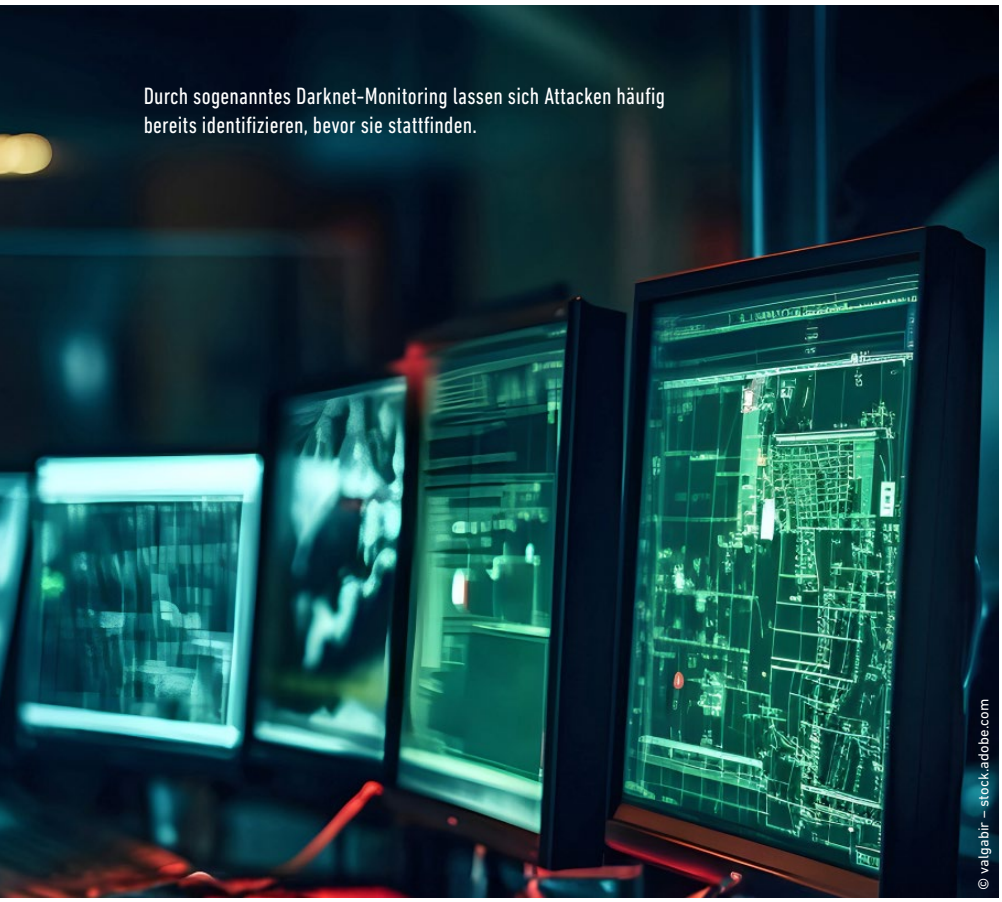
Das Herstellen einer ausreichenden Resilienz ist deshalb für jedes Unternehmen wichtig. Die vordringlichste Aufgabe der Geschäftsführung und des Vorstandes besteht darin, sich einen Überblick über die Gefahrenlage ihres Unternehmens zu verschaffen, das notwendige Schutzniveau zu bestimmen und die Herstellung wie Einhaltung dieses Schutzniveaus zu begleiten. Wie exponiert sind zum Beispiel geschäftskritische Prozesse gegenüber Cyberangriffen, welche monetären Folgen hätte ein Ausfall und wie können stark umsatz- und ergebnisrelevante Geschäftsprozesse wirksamer geschützt werden?

> „Unternehmen müssen sich nicht nur technisch, sondern auch organisatorisch mit Informationssicherheit auseinandersetzen."

Elementar wichtig dabei ist: Unternehmen müssen sich nicht nur technisch, sondern auch organisatorisch mit Informationssicherheit auseinandersetzen. Diese ist kein exklusives Vergnügen der IT; Cybersicherheit muss im ganzen Unternehmen in den Köpfen der Mitarbeiter verankert werden. Jeder Fachbereich – vom Vorstandsbüro bis hin zum Warenausgangslager – sollte mittels Business-Continuity-Management (BCM) evaluieren, wie resilient er für welche Schadensszenarien aufgestellt ist, also wie lange er zum Beispiel seine Geschäftsprozesse ohne IT betreiben kann.

Ransomwareangriff: Nichts geht mehr – die Geschäftstätigkeit wird komplett unterbrochen

Eine unter Cyberangreifern zurzeit sehr beliebte Angriffstechnik sind Ransomwareattacken. Diese Angriffsmethodik verschlüsselt mit Hilfe von Kryptoalgorithmen quasi das gesamte IT-System, macht es dadurch unbrauchbar und schleudert Unternehmen buchstäblich zurück in die digitale Steinzeit. Die Konsequenzen für die attackierten Unternehmen sind gravierend: Von einem Tag auf


Durch sogenanntes Darknet-Monitoring lassen sich Attacken häufig bereits identifizieren, bevor sie stattfinden.

© valgabir – stock.adobe.com

den anderen stehen zum Beispiel alle Systeme – von der Software für das zentrale Enterprise-Resource-Planning (ERP) über Microsoft Office bis hin zu den Kassen- und Verkaufssystemen – still. Die Geschäftstätigkeit kommt zum Erliegen. Der finanzielle Schaden fällt in der Regel hoch aus.

Präventivmaßnahmen: Business-Continuity-Management und Monitoring durch Dashboards

Um negative Auswirkungen von Cyberangriffen zu vermeiden, sollten Geschäftsführung und Vorstand nicht nur das oben erwähnte Business-Continuity-Management etablieren, sondern in diesem Zuge auch eine Business-Impact-Analyse vornehmen lassen. Außerdem ist die Einhaltung von Schutz- und Präventionsmaßnahmen durch ein geeignetes Steuerungswerkzeug wie ein Dashboard zu überwachen. Mehr Transparenz bedeutet in diesem Fall mehr Sicherheit. Dabei geht es nicht zwingend um rein technische KPIs. Es gilt, genau die relevanten Kennzahlen und Merkmale zu ermitteln, die das bereits erwähnte Schutzniveau beziehungsweise den aktuellen Reifegrad darstellen. Und zwar sowohl für die technischen als auch für die organisatorischen Maßnahmen. Gibt es ein Notfallkonzept, wann ist dies zuletzt überarbeitet worden, wann ist die letzte Übung durchgeführt worden, wie ist das Ergebnis der letzten Awareness-Kampagne, gibt es eine Offline-Liste mit Mitarbeiterkontaktdaten und wie alt ist sie? Diese und weitere Fragen sind relevant, um auf den Tag X vorbereitet zu sein. Die Aktualität und Vollständigkeit sowie der Stand der Umsetzung lassen sich über ein Dashboard vom Vorstand oder der Geschäftsführung überwachen.

Um zu unserem Beispiel zurückzukehren: Ransomwareangriffe sind immer mit – oftmals hohen – Lösegeldforderungen verbunden. Nachdem sich die erste Panik unmittelbar nach dem Angriff und dem Komplettausfall der IT-Systeme gelegt hat, stellt sich deshalb dem betroffenen Unternehmen immer die Gretchenfrage: Zahlen wir oder zahlen wir nicht? [→ Laufersweiler/Schmitt/von der Linden, S. 27]

Präventivmaßnahme: Zeitrhythmus von Backups kalkulieren und überwachen

Das No-Pay-Szenario geht davon aus, dass das angegriffene Unternehmen den Restart seiner Systeme bewerkstelligen kann, indem es die infizierten IT-Systeme säubert, sichert und Backups einspielt. Dafür sind aber lückenlose und regelmäßig durchgeführte Backups, die ohne Netzanbindung an die produktiven IT-Systeme aufbewahrt werden, die Voraussetzung. Das Zeitintervall, in dem Backups durchgeführt werden, hängt von den zu schützenden Daten ab. Werden die Backups zum Beispiel täglich durchgeführt, gehen schlimmstenfalls die Firmendaten eines Tages verloren. Welchen Business-Impact hätte der Verlust eines Tages und ist es eventuell sinnvoll, sensible Firmendaten in kürzeren Zeitabständen zu sichern? Diese Fragen sind von höchster Relevanz

für das Business und können nur dort beantwortet werden.

Unterlassen Unternehmen die notwendigen Vorbereitungen und ein enges Monitoring der Schutzmaßnahmen, dann sind Backups möglicherweise unvollständig oder nicht ausreichend und es bleibt nichts anderes übrig, als in den sauren Apfel zu beißen und das Lösegeld zu zahlen. Gefordert wird eine nach Einschätzung der Angreifer am Unternehmenswert orientierte Summe in Bitcoin oder in einer anderen Kryptowährung. Anhand jüngst im Darknet veröffentlichter interner Kommunikation von Angreifergruppen wird übrigens deutlich, dass die Höhe der Lösegeldforderungen drastisch steigen soll und als unverschämt niedrig bewertete Angebote von Verhandlern mit sofortiger Datenlöschung geahndet werden. Hier wird offenbar versucht, durch drastische Präzedenzen eine abschreckende Wirkung zu erzielen. Dass Cyberkriminelle zudem den Druck durch sogenannte Double- oder Triple-Extortion erhöhen, ist ebenfalls nicht neu. Es ist ihnen in diesen Fällen nicht nur gelungen, die IT-Systeme und Daten zu verschlüsseln und dadurch den Geschäftsbetrieb zu unterbrechen. Sie haben außerdem sensible Unternehmensdaten wie Mitarbeiter- und Kundeninformationen, Strategiepläne, Rezepturen oder die Konstruktionspläne für ein neues Produkt erbeutet und drohen mit deren Veröffentlichung.

Was können Geschäftsführer, CIOs, CEOs und Vorstandsmitglieder tun, um Schäden durch Cyberangriffe von ihrem Unternehmen schon im Vorfeld abzuwenden oder zumindest zu reduzieren? Neben den klassischen Sicherheitsvorkehrungen bietet sich Darknet-Monitoring als hochwirksame Präventivmaßnahme an. Denn Cyberkriminelle sind Geschäftsleute, die Geld verdienen wollen. Sie denken wie Unternehmer, die ihre Geschäfte möglichst effizient und gewinnbringend abwickeln wollen. Gehandelt und zu Geld gemacht werden die gestohlenen und oft vertraulichen Daten, Logins, PINs, Passwörter, Identitäten oder Mailzugänge im Darknet, im unsichtbaren, nicht ohne Weiteres zugänglichen Teil des World Wide Web.

Präventivmaßnahme: Darknet-Monitoring

Durch sogenanntes Darknet-Monitoring lassen sich Attacken häufig bereits identifizieren, bevor sie stattfinden. Unternehmen können entsprechende Präventivmaßnahmen einleiten und dadurch den Angreifern zuvorkommen. Sicherheitsexperten sind zum Beispiel im Zuge ihrer Recherchen im Darknet auf die Zugangsdaten einer großen deutschen Versicherung gestoßen, die auf einem der Marktplätze zum Verkauf angeboten worden sind. Natürlich haben die Sicherheitsspezialisten den „Fund“ der Versicherung gemeldet. Zwischen dem Angriff und dem Verkauf der Daten vergeht in der Regel einige Zeit, somit konnte das Unternehmen rechtzeitig Schutzmaßnahmen einleiten. Solche durch Darknet-Monitoring mit Hilfe modernster Technologie recherchierte Informationen sind Gold wert und helfen, Schäden in Millionenhöhe zu verhindern.

Sind bei einem Cyberangriff personenbezogene Daten betroffen, muss ein Unternehmen außerdem die zuständige Aufsichtsbehörde darüber informieren. Die Datenschutz-Grundverordnung (DSGVO) schreibt dafür ein Zeitfenster von 72 Stunden vor. [→ Pauly/Nabulsi, S. 30]

Mit der neuen NIS2-Richtlinie der EU kommen in den nächsten Monaten zudem weitere rechtliche Anforderungen auf Unternehmen zu, die die Umsetzung der hier geschilderten Maßnahmen verpflichtend machen und gleichzeitig die persönliche Verantwortung und Haftung der Geschäftsleiter noch einmal klar regeln.

> „Sind bei einem Cyberangriff personenbezogene Daten betroffen, muss ein Unternehmen außerdem die zuständige Aufsichtsbehörde darüber informieren.“

Es lohnt sich also, Prävention auf einem für jedes einzelne Unternehmen sinnvollen Level zu betreiben. Denn auch wenn ein Sicherheitsgurt einen Unfall zwar nicht verhindern kann, so verringert er doch die Schwere der Verletzungen. Nicht anders verhält es sich auch mit den geschilderten Maßnahmen, die die Schäden eines mit hoher Wahrscheinlichkeit eintretenden Sicherheitsvorfalls beherrschbar und möglichst geringhalten sollen. ←

Thomas Lang
valantic Management Consulting, Dreieich
Partner
thomas.lang@mc.valantic.com
www.valantic.com

Wächter der Bits und Bytes

Cybersicherheit und Datenschutz

Von Prof. Dr. Boris P. Paal, M.Jur. (Oxford)

Da digitale Daten zu einer der wichtigsten und wertvollsten Ressourcen geworden sind, stehen auch und gerade Cybersicherheit und Datenschutz mit guten Gründen zunehmend im Fokus. Sowohl Unternehmen und Behörden als auch Einzelpersonen sind heute immer stärker vernetzt und hierbei datengetriebener als je zuvor. Während diese datenbasierte Vernetzung zum einen erhebliche Chancen und Vorteile bietet, wird zum anderen zugleich eine attraktive Angriffsfläche für Cyberkriminelle eröffnet. Konkretes Ziel des Angriffs ist zumeist der Diebstahl von Daten, um auf diese Weise finanzielle Vorteile zu erlangen, wobei erheblicher Schaden angerichtet und gegebenenfalls auch Chaos gestiftet wird. Zunehmend ist ein durch Hacker ausgeführter Cyberangriff weniger eine Frage des „Ob" als vielmehr des „Wann" und „Wie". So stieg die Zahl der Cyberangriffe auf privatwirtschaftliche Unternehmen, öffentliche Einrichtungen und kritische Infrastrukturen in Deutschland im Jahr 2022 im Vergleich zum Vorjahr um rund 30%, verbunden mit einem Schaden von über 200 Milliarden Euro; die Dunkelziffer dürfte noch deutlich höher sein.

Um die (Cyber-)Sicherheit von (personenbezogenen) Daten und maßgeblichen Datenverarbeitungssystemen zu gewährleisten, sind sowohl technische als auch organisatorische Maßnahmen (TOMs) zu ergreifen.

© nakedking – stock.adobe.com

Vor diesem Hintergrund bieten Unternehmen etwa sogenannte Bug-Bounty-Programme an, bei denen aktiv zum Hacken aufgefordert wird, um Sicherheitslücken und Schutzdefizite

aufzudecken. Apple zahlt erfolgreichen Hackern eine Million US-Dollar, (selbstverständlich nur) sofern die Hacker eine Verschwiegenheitserklärung unterzeichnen. Neben dem Schaden durch die Cyberangriffe können zudem empfindliche Bußgelder drohen: Mit dem Vorwurf, dass der Meta-Konzern sich nicht an die Vorgaben des DSGVO-Regelungsregimes gehalten habe und Hacker durch Data Scraping die Daten von mehr als 533 Millionen Nutzern erlangten, hat die irische Datenschutzaufsichtsbehörde ein – noch nicht rechtskräftiges – Bußgeld in Höhe von 265 Millionen Euro verhängt.

Hervorzuheben ist, dass nicht nur große Konzerne im Fokus der Hackerangriffe stehen: Vielmehr handelt es sich bei nahezu der Hälfte der von Cybersicherheitsvorfällen Betroffenen um kleine und mittlere Unternehmen (KMU) sowie um öffentliche Einrichtungen. Somit sollten sämtliche der potentiell Betroffenen sich der erheblichen Cybersicherheitsgefahren, auch und gerade mit Blick auf den Datenschutz, bewusst sein – und geeignete Compliance- und Vorsorgemaßnahmen treffen.

Zur Bedrohungslage

Cyberangriffe sind allgegenwärtig, was kaum verwundert, da täglich etwa 319.000 Schadsoftwarevarianten produziert werden. Bis eine Datenschutzverletzung entdeckt wird, dauert es allerdings durchschnittlich knapp 300 Tage. Dabei droht ein Cyberangriff umso schädlicher und kostspieliger zu werden, je länger er unentdeckt bleibt und daher eingrenzende Maßnahmen unterbleiben. Von Phishingangriffen bis hin zu Ransomwareattacken, bei denen Lösegeld für die Freigabe verschlüsselter Daten gefordert wird, ist das Bedrohungsspektrum durch Cyberangriffe ebenso breit wie besorgniserregend. Regelmäßig werden in Unternehmen, Behörden und weiteren Einrichtungen riesige Datenmengen gespeichert und verarbeitet, wobei die Bandbreite von Mitarbeiter- und Kundendaten bis hin zu Daten über die wirtschaftliche Situation des Unternehmens und über neue Produkte reicht.

Für die Opfer von Cyberangriffen kann ein Verstoß gegen den Datenschutz, und hierbei insbesondere wegen mangelnder Datensicherheit, nicht nur finanzielle Schäden, sondern darüber hinaus den – mitunter sogar schwerwiegenderen – Verlust von Vertrauen und Reputation bedeuten, ferner den Verlust von Geschäftsgeheimnissen und vor allem der nun nicht mehr verfügbaren Daten. Zugleich drohen bei Datenschutzverstößen rechtliche Verfahren, sei es durch Aufsichtsbehörden oder durch – zumeist auf Schadensersatz gerichtete – Zivilklagen von Betroffenen. Denn Unternehmen, die personenbezogene Daten verarbeiten, sind durch die DSGVO (unter anderem) verpflichtet, angemessene Sicherheitsvorkehrungen zu treffen und Datenschutzvorfälle an die Aufsichtsbehörden zu melden.

Technische und organisatorische Maßnahmen

Um die (Cyber-)Sicherheit von (personenbezogenen) Daten und maßgeblichen Datenverarbeitungssystemen zu gewährleisten, sind sowohl technische als auch organisatorische Maßnahmen (TOMs) zu ergreifen. Das Themenfeld „Cybersicherheit“ erstreckt sich weit über den Bereich der IT-Sicherheit hinaus und erfordert deshalb ein übergreifendes Konzept zum Schutz von Computersystemen, Netzwerken und Daten vor Bedrohungen und Angriffen. Zu beachten und zu implementieren ist eine Vielzahl von gesetzlichen Vorgaben, Maßnahmen und Best Practices, um die digitale Dateninfrastruktur gegen Cyberangriffe sicher(er) zu machen.

Technische Schutzmaßnahmen

In technischer Hinsicht ist der Blick insoweit zunächst auf robuste Firewallsysteme, Zugriffskontrollen, regelmäßige Softwareupdates (auch wenn diese mitunter als lästig und zeitaufwendig empfunden werden) und auf hinreichende Verschlüsselungsvorkehrungen zu richten. Denn nicht zuletzt prüfen Cyberkriminelle nach Softwareupdates regelmäßig, welche Sicherheitslücken geschlossen wurden – und wo noch Schutzlücken und Einfallstore bestehen. Dabei können auch kleine(re) Maßnahmen erheblich zur Erhöhung und Stabilisierung von Cyber- und Datensicherheit beitragen, wenn etwa bereits beim Hardwarekauf auf eine angemessene Verschlüsselung der Geräte und Daten geachtet wird.

Homeofficesicherheit

Ein weiterer nicht zu unterschätzender Faktor ist das immer häufiger vorkommende Arbeiten im Homeoffice. Auch in diesem Zusammenhang ist auf eine angemessene Datensicherheit zu achten, wofür die Mitarbeitenden zu sensibilisieren und entsprechend technisch auszustatten sind. Konkret

müssen zum Beispiel die zur Verfügung gestellten Geräte sicher an das Unternehmensnetz angeschlossen und dort eingebunden werden.

Organisatorische Schutzmaßnahmen

Doch auch die beste Sicherheitssoftware hilft allenfalls begrenzt, wenn sie nicht richtig angewendet wird. In diesem Sinne müssen auf organisatorischer Ebene eindeutige und belastbare Sicherheitsrichtlinien und Routinen etabliert sowie eingeübt werden, möglichst einschließlich der Erstellung eines Ablaufs- und Zuständigkeitskonzepts für das Krisenmanagement im Ernstfall. Von zentraler Bedeutung ist hierbei die Zusammenarbeit zwischen IT-Experten und Entscheidungsträgern, damit Risiken ebenso frühzeitig wie vorausschauend identifiziert und effektive Schutzmaßnahmen implementiert sowie ergriffen werden können.

Mitarbeiter als erste Verteidigungslinie

Die Aufgabe der Gewährleistung von Cybersicherheit ist zudem keinesfalls (nur) auf die IT-Abteilung beschränkt: Mitarbeiter spielen eine entscheidende Rolle, da Phishing eine besonders häufige Angriffsart zur rechtswidrigen Erlangung von Daten(sätzen) darstellt. Hier mag es beispielsweise an der erforderlichen Aufmerksamkeit und Vorsicht fehlen, so dass ein schadhafter E-Mail-Anhang heruntergeladen wird, oder es werden (zu) schwache Passwörter („1234“) verwendet. Diesen Szenarien kann und sollte mit regelmäßigen Schulungen entgegengewirkt werden. In vielen Unternehmen sind entsprechende „Security Awareness“-Trainings bereits Standard, wobei regelmäßig unter anderem auch ein Phishing-Test implementiert ist.

Die Rolle von KI für Cybersicherheit und Datenschutz

Schließlich kommt für das Themenfeld „Cybersicherheit und Datenschutz“ der Anwendung von Technologien der künstlichen Intelligenz (KI) eine immer größere Bedeutung zu; dies gilt sowohl für die Cyberkriminellen als auch aus Sicht der Betroffenen. So durchsucht KI zum Beispiel das E-Mail-Postfach nach verdächtigen Dateien und sortiert diese aus, oder das Leseverhalten wird in sicherheitsrelevanten Bereichen auf verdächtige Muster hin überwacht. Von den Angreifern kann KI nicht zuletzt etwa zur Erzeugung von Fakebildern, -anrufen und -videos sowie für Imitationen und Chatbots im Kontext von Cyberattacken eingesetzt werden.

Zwischenbefund

Insgesamt bedarf es einer kontinuierlichen gemeinsamen Anstrengung aller Beteiligten, um die Integrität und Sicherheit von Daten und Systemen im Zeitalter der digitalen Transformation maßgeblich zu verbessern.

Handlungsempfehlungen

1. Es sind umfassende Richtlinien zur Cybersicherheit zu implementieren.
2. Mitarbeiter sollten regelmäßig sensibilisiert und geschult werden.
3. Software, Betriebssysteme und Sicherheitsanwendungen sind kontinuierlich zu aktualisieren.
4. Durch Netzwerksicherheit und Zugriffskontrollen ist zu gewährleisten, dass nur autorisierte Personen auf sensible Daten und Systeminfrastrukturen zugreifen können.
5. Regelmäßige Backups dienen der Datensicherung und ermöglichen eine Wiederherstellung im Ernstfall.
6. Zur Identifizierung von Schwachstellen sollten externe Sicherheitsprüfungen durchgeführt werden.
7. Ein Aktions- und Reaktionsplan für den Ernstfall dient der Eindämmung und Prävention von Schäden.

Investitionen in Cybersicherheit

Die Kosten für die Bewältigung von Cybersicherheitsvorfällen sind zumeist deutlich höher als die erforderlichen Investitionen für Präventionsmaßnahmen. Unternehmen und Organisationen sollten daher (auch) in die Cybersicherheit ihrer digitalen Infrastruktur investieren. Insgesamt stellen Cybersicherheit und Datenschutz gerade nicht lediglich optionale Aufgaben dar, sondern sind vielmehr Kernelemente einer zukunftsfähigen Compliancestruktur. ←

Prof. Dr. Boris P. Paal, M.Jur. (Oxford)
Technische Universität München
Chair for Law and Regulation of the Digital Transformation
TUM School of Social Sciences and Technology
boris.paal@tum.de
www.gov.sot.tum.de/lrd

Finanzaufsichtsrechtliche Anforderungen an die IT-Sicherheit

Aktuelle Regulierungsvorhaben und Ausblick

Von Dr. Florian Reul und Pascal Mildahn

Die zunehmende Bedeutung der generellen Anforderungen mit Blick auf die IT-Systeme von Finanzunternehmen wird auch dadurch deutlich, dass die BaFin in den vergangenen Jahren die aufsichtsrechtlichen Anforderungen durch mehrere Rundschreiben weiter spezifiziert und kontinuierlich entwickelt hat.

Schon seit mehreren Jahren ist die IT-Sicherheit eines der Fokusthemen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Das ungebrochene Bedeutungswachstum von IT in fast allen Bereichen des Finanzsektors führt unweigerlich zu einem zunehmenden Gewicht des angemessenen Umgangs mit Cyberrisiken. Relevante Sicherheitsvorfälle können dabei sowohl externe als auch interne Gründe haben und schwerwiegende Folgen für Unternehmen, Kunden und letztlich für die Finanzstabilität mit sich bringen. Die Widerstandsfähigkeit und Verlässlichkeit der verwendeten Informationssysteme sind daher von entscheidender Bedeutung.

Daneben gewinnt die Fähigkeit, mit IT-Infrastrukturen beziehungsweise aus den gewonnenen Daten Mehrwert zu schaffen und neue Geschäftschancen zu generieren, stetig an Signifikanz. Neue Wettbewerber, veränderte Erwartungshaltungen der Kunden und potentere technische Möglichkeiten führen zu hohem Anpassungsdruck. Zudem ist es das erklärte Ziel der EU-Kommission, über Open Finance die Unternehmen der Finanzindustrie stärker in Richtung einer datengetriebenen Wirtschaft zu führen.

Damit bekommt der Umgang mit den sich aus IT-Systemen und Daten ergebenden Chancen und Risiken eine zunehmende strategische Bedeutung. Aus diesem Grund ist eine frühe und intensive Auseinandersetzung mit den sich verändernden regulatorischen Anforderungen erforderlich.

Zunehmende Cyberrisiken

Cyberrisiken haben viele Ursachen. Neben menschlichen Schwachstellen (beispielsweise Phishing, Social Engineering und Insiderbedrohungen) existieren technologische Schwach-

stellen (veraltete Systeme, fehlende Verschlüsselung und unsichere APIs). Des Weiteren müssen die Technologien in vorhandene Prozesse von komplexen Organisationen integriert werden, ohne systematisch organisatorische Schwachstellen herbeizuführen. Die oftmals kurzen Innovationszyklen digitaler Technologien erschweren dies zusätzlich. Dazu kommen eine vermehrte Nutzung von Drittanbietern, eine erhöhte Angriffsfläche durch Homeofficearbeitsplätze und geopolitische Risiken, etwa durch staatliche oder halbstaatliche Akteure.

Bestehende regulatorische Anforderungen

Für regulierte Finanzunternehmen bestehen bereits heute detaillierte Pflichten, wie sie Cyberrisiken zu adressieren haben.

Die Geschäftsleiter eines Kredit- oder Finanzdienstleistungsinstituts sind für eine „ordnungsgemäße Geschäftsorganisation" verantwortlich, was explizit auch eine „angemessene […] technisch[-]organisatorische Ausstattung des Instituts" sowie die Einrichtung eines „angemessenen Notfallmanagements, insbesondere für IT-Systeme" umfasst (vgl. § 25a Kreditwesengesetz – KWG). Ähnliche Verpflichtungen bestehen auch für Zahlungsdienstleister, Versicherungen und Kapitalverwaltungsgesellschaften, sprich Fondsmanager.

Die zunehmende Bedeutung dieser generellen Anforderungen mit Blick auf die IT-Systeme von Finanzunternehmen beziehungsweise auf bestehende Cyberrisiken wird nicht zuletzt dadurch deutlich, dass die BaFin in den vergangenen Jahren die aufsichtsrechtlichen Anforderungen an die IT durch mehrere Rundschreiben weiter spezifiziert und kontinuierlich entwickelt hat (die sogenannten BAIT für Banken, VAIT für Versicherungen, ZAIT für Zahlungsdienstleister und KAIT für Kapitalverwaltungsgesellschaften). Diese Rundschreiben sind grundsätzlich prinzipienorientiert strukturiert und stellen Anforderungen hinsichtlich Governance, Steuerung sowie der operativen Aspekte der IT auf. Zudem haben die Finanzaufsichtsbehörden in letzter Zeit verstärkt die aufsichtsrechtliche IT-Compliance der Finanzunternehmen geprüft und in nicht wenigen Fällen Kapitalaufschläge wegen festgestellter Mängel verhängt.

Künftige regulatorische Anforderungen durch DORA

Der Trend zu einer intensiveren Regulierung IT-bezogener Sachverhalte zeigt sich auch anhand des „Digital Operational Resilience Act" (DORA). Der europäische Gesetzgeber hat mit DORA ein einheitliches Rahmenwerk geschaffen, um die digitale Resilienz von Finanzunternehmen zu stärken. DORA soll Finanzunternehmen in die Lage versetzen, ihre operative Integrität auch während Zwischenfällen – wie einem Cyberangriff oder rein internen Störungen – aufrechtzuerhalten. Hierfür ist ein Komplex von Regelungen geschaffen worden, die insbesondere das Risikomanagement von Informations- und Kommunikationstechnologien (IKT) betreffen, einschließlich Anforderungen an die Behandlung, Klassifizierung und Meldung von IKT-bezogenen Vorfällen sowie das regelmäßige Testen der digitalen operationalen Resilienz. Dies umfasst etwa auch die Verpflichtung, für den Krisenfall Maßnahmen festzulegen, die eine Übermittlung aktueller Informationen über relevante (schwerwiegende) Vorfälle an interne Mitarbeiter sowie an sogenannte externe Interessenträger (also Kunden, andere Finanzunternehmen und die Öffentlichkeit) gewährleisten.

> „IT-Regulierung wird damit auch in den kommenden Jahren eines der Fokusthemen der Finanzmarktaufsicht bleiben."

Die Regelungen von DORA werden zudem durch diverse technische Regulierungsstandards („Regulatory Technical Standards", RTS), die von den europäischen Aufsichtsbehörden EBA, EIOPA und ESMA derzeit entworfen und konsultiert werden, noch detaillierter ausgearbeitet. Die Umsetzung bis Anfang 2025 ist eine herausfordernde Aufgabe angesichts der Detailtiefe und des Umfangs von DORA sowie der zahlreichen noch zu veröffentlichenden RTS, ferner aufgrund der regelmäßig gegebenen Komplexität und Langwierigkeit von IT-Projekten.

Da DORA – trotz des eher deskriptiven Regelungsansatzes – grundsätzlich eine holistische Betrachtung der betroffenen Unternehmen verfolgt, sind in DORA dementsprechend vielfältige Überlappungen und Fortentwicklungen bestehender Regelungen vorzufinden. Insoweit hat die BaFin bereits

angekündigt, dass die bestehenden Regelungen in BAIT, VAIT, ZAIT und KAIT nach Abschluss der Umsetzungsarbeiten für DORA überprüft und etwaige Doppelregulierungen möglichst abgebaut werden sollen.

Weiterhin erscheint es erwähnenswert, dass DORA erstmals bislang unregulierte, große IKT-Dienstleister einer Aufsicht unterstellt.

FIDA und die datengetriebene Wirtschaft

Neben der Befassung mit Cyberrisiken zeigt sich auf europäischer Ebene das Bestreben der EU-Kommission, eine stärker datengetriebene Wirtschaft zu ermöglichen und einzufordern. Insofern dürfen die bisher skizzierten cyberspezifischen Gesetze nicht isoliert betrachtet werden, denn nach Ansicht der EU-Kommission ist der Datenaustausch zwischen Inhabern von Daten zur Erbringung von Dienstleistungen durch unterschiedliche Anbieter unzureichend. Als Grund hierfür werden fehlende Standards, zu teure Prozesse und daraus resultierendes mangelndes Vertrauen ausgemacht. Daher wird der in der „Payment Services Directive II" (PSD II) angestoßene Weg, Drittanbietern über Schnittstellen den Zugriff auf Konten und Kontendaten von Kunden zu erlauben, weiter forciert und ausgebaut. Dies geschieht etwa anhand der PSD III/PSR (sogenanntes Open Banking; PSR: „Payment Services Regulation" der EU), insbesondere aber durch Open Finance in Form der „Financial Data Access Regulation" (FIDA). Dieser wird fast sämtliche regulierte Einheiten der Finanzindustrie umfassen.

Danach werden diese als Dateninhaber bezeichneten Unternehmen für zahlreiche definierte Kategorien von Kundendaten gezwungen, zunächst sogenannte Schemes zu bilden, in denen die Industriestandards für den Austausch dieser Kundendaten entwickelt werden sollen. Basierend auf diesen Standards, sollen die Dateninhaber zukünftig ihren Kunden Dashboards anbieten. Über diese sollen die Kunden nicht nur die über sie gesammelten Daten einsehen können. Sie sollen auch festlegen können, ob andere Datennutzer, das heißt Finanzinstitute oder die durch FIDA eingeführten sogenannten Finanzinformationsdienstleister, Zugriff auf Daten erhalten. So erhofft sich die Kommission, den Nutzern höhere Datenautonomie zu geben und einen wichtigen Schritt in Richtung datengetriebener Wirtschaft zu gehen.

Neben offenen praktischen Fragen – wie zum Beispiel, ob die Bildung von Industriestandards im avisierten Zeitrahmen überhaupt realistisch ist – erscheint es allerdings wahrscheinlich, dass eine so vorangetriebene Vernetzung weitere Risiken für die Cybersicherheit der regulierten Unternehmen mit sich bringt. Zugleich wird deutlich, dass eine ganzheitliche Strategie zur Wertschöpfung durch Kundendaten und zum Umgang mit diesen auch aus finanzregulatorischer Perspektive eine stetig wachsende Bedeutung einnehmen wird.

Ausblick

Die regulatorische, datenschutzrechtliche und strategische Relevanz von IT-Compliance nimmt somit weiter zu. In Verbindung mit der Fähigkeit, Cyberrisiken wirksam zu begegnen, wird die IT-Compliance im weitesten Sinne zu einem der wesentlichen Erfolgsfaktoren der Finanzindustrie. Damit hat die IT-Compliance längst nicht mehr nur defensiven Charakter, sondern muss die Unternehmen in die Lage versetzen, Mehrwert aus den generierten Daten erzeugen zu können (genannt sei hier nur das Stichwort Artificial Intelligence/AI). IT-Regulierung wird damit auch in den kommenden Jahren eines der Fokusthemen der Finanzmarktaufsicht bleiben.

Wie anhand von DORA zu erkennen ist, schreckt die EU dabei nicht davor zurück, Unternehmen außerhalb des Finanzsektors von der Cyberregulierung zu erfassen. Ob dies zugleich für die betroffenen Tech-Anbieter die Markteintrittshürde in den Finanzsektor absenkt, bleibt abzuwarten. Niederschwellige Möglichkeiten für einen solchen Markteintritt, zum Beispiel als Kontoinformationsdienstleister oder – wie mit FIDA vorgeschlagen – als Finanzinformationsdienstleister, sind jedenfalls bereits vorhanden. ←

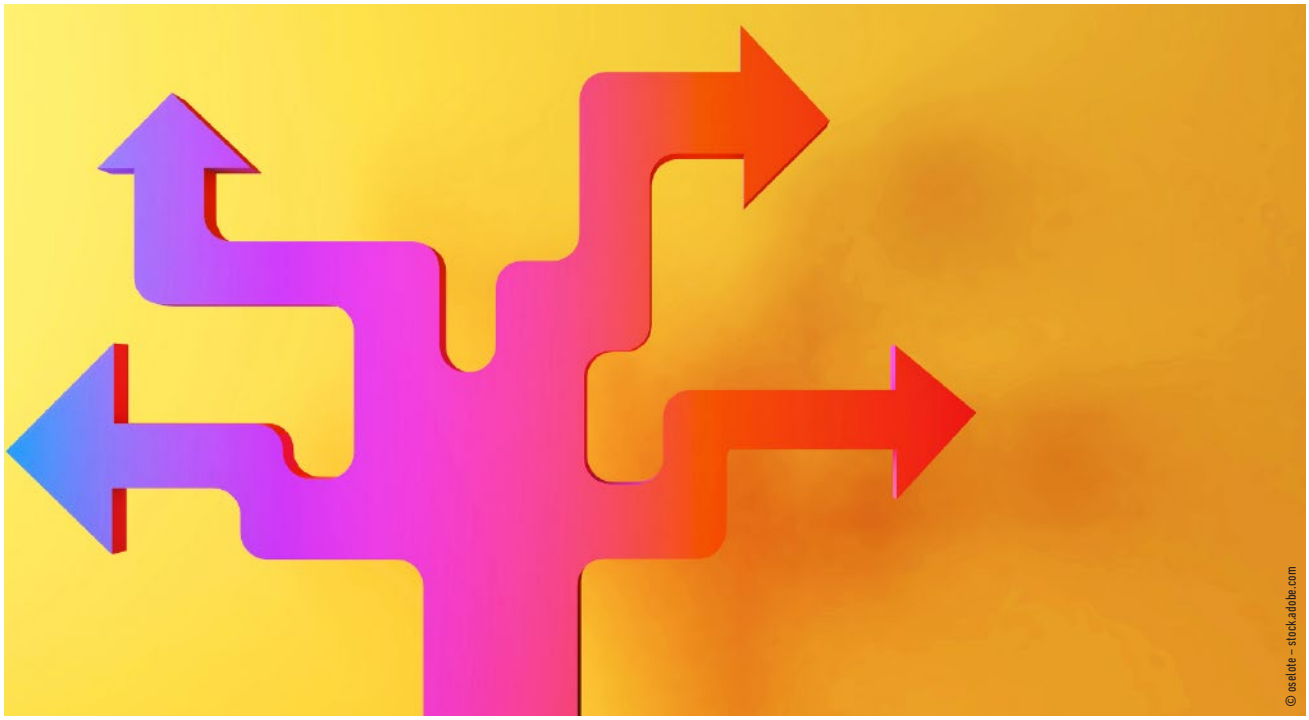
Dr. Florian Reul
Linklaters LLP,
Frankfurt am Main
Counsel, Head of Fintech Germany
florian.reul@linklaters.com
www.linklaters.de

Pascal Mildahn
Linklaters LLP,
Frankfurt am Main
Managing Associate, Aufsichtsrecht
pascal.mildahn@linklaters.com
www.linklaters.de

Best Practice Krisenkommunikation

Vorbereitung und Umsetzung

Von Suntka von Halen



Als Teil des Krisenmanagements und der ganzheitlichen Krisenvorbereitung des Unternehmens muss auch die Unternehmenskommunikation mit dem wachsenden Risiko von Cyberangriffen Schritt halten.

Die Bedrohungslage im Cybersicherheitsbereich wächst exponentiell

Die im aktuellen Allianz Risk Barometer 2023 veröffentlichten Zahlen sind (leider) beeindruckend: Cyberangriffe gehören mittlerweile zum Alltag der globalen Wirtschaft. 2022 hat die Menge von Angriffen im Vergleich zum Vorjahr weltweit um 34% zugenommen und einen geschätzten Schaden von über einer Billion US-Dollar verursacht – das entspricht etwa einem Prozent des globalen Bruttoinlandsprodukts.

34% der im Allianz Risk Barometer befragten Unternehmen sehen Cyberattacken mittlerweile als die größte Bedrohung – noch vor makroökonomischen und geopolitischen Problemen. Innerhalb des Risikobereichs Cybersicherheit bereitet Datenschutz dabei besonders große Sorge, wie 53% der Befragten angaben: Die durchschnittlichen Kosten für Datenschutzverletzungen erreichten 2022 mit 4,35 Millionen US-Dollar pro Fall einen historischen Höchststand. Ransomwareangriffe werden ebenso als hohes Risiko empfunden – zu Recht, denn Angreifer nehmen weiterhin große Unternehmen und zunehmend Lieferketten und kritische Infrastrukturen ins Visier.

Im Bereich geopolitischer Risiken sieht der CrowdStrike Global Threat Report 2023 ein steigendes Risiko für Angriffe durch Nationalstaaten, wobei insbesondere Russland, China und der Iran ihre Cyberaktivitäten intensivieren. Die Art dieser Angriffe geht üblicherweise von rein destruktiven Attacken wie Datenzerstörung und Betriebsunterbrechung bis hin zu Datendiebstahl und Spionage.

Interessant ist dabei, dass und wie sich die Zugriffsvektoren verändern. Gingen im Jahr 2019 noch 60% der Angriffe auf Malware zurück, sank dieser Anteil im Jahr 2022 auf 29%, während Techniken zum Abgreifen von Zugangsdaten zu Benutzerkonten in Organisationen stark gestiegen sind. Dass in der professionell arbeitsteilig organisierten Cyberkriminalität Angreifer solche Zugänge zu Organisationskonten an andere Akteure wie Ransomwarebetreiber verkaufen, ist bekannt. Im Jahr 2022 verzeichneten diese Dienste laut CrowdStrike einen bemerkenswerten Anstieg von 112% gegenüber dem Vorjahr.

Die Wahrscheinlichkeit, getroffen zu werden, ist hoch – und steigt weiter

In unserem Beratungsalltag hören wir von Kunden häufig das Argument, dass international agierende Hackergruppen zuvorderst auf die globalen Konzerne zielten und die kleinen und mittleren Unternehmen (KMU) oder die Hidden Champions in Deutschland und Europa im Zweifel nicht auf dem Radar hätten. Doch dagegen steht ein Satz, den FBI-Chef Robert Muller geprägt hat: Es gibt zwei Arten von Unternehmen – die, die bereits gehackt worden sind, und die, denen es noch bevorsteht.

Natürlich bestimmen die breitangelegten Hacks auf international bekannte Unternehmen die Schlagzeilen – MGM Grand, Estée Lauder, Microsoft, T-Mobile, Rheinmetall, Uber und Continental. Aber diese Konzerne bilden eine im Verhältnis eher kleine Gruppe, die gezielt ins Visier genommen wird mit sehr detailliert vorbereiteten Angriffen. Dieser Gruppe gegenüber steht die große Mehrheit der Unternehmen, die durch in die Breite zielende Attacken wie Phishingwellen oder Zero-Day-Exploits angegriffen werden.

> „Es gibt zwei Arten von Unternehmen – die, die bereits gehackt worden sind, und die, denen es noch bevorsteht."

Zero-Day-Vulnerabilities, also unentdeckte Schwachstellen, die dementsprechend nicht überwacht werden und ungepatcht sind, entstehen nicht selten durch Sicherheitslücken in vergleichsweise kleinen Softwarebestandteilen oder Programmen, die als Teil größerer Programmumgebungen eingesetzt und weltweit genutzt werden. Weisen diese eine Schwachstelle auf, ist der Hebel für Angreifer aufgrund der breiten Anwendung extrem groß – und damit die Anzahl der betroffenen Unternehmen weltweit hoch. Bekannte aktuelle Fälle sind beispielsweise die Javabibliothek Log4J sowie Schwachstellen in Googles Browser Chrome oder die Dateiaustauschplattform MOVEit.

Mit den Möglichkeiten der KI werden Cyberangriffe weiter exponentiell wachsen – Stichwort Deepfakes, CEO-Fraud, Social Engineering. Kurz gesagt: Cyberangriffe werden immer „besser". Dementsprechend werden die Anzahl erfolgreicher Angriffe, die Komplexität und voraussichtlich auch ihr Schadensumfang weiter steigen. Im Zuge dieser technischen Weiterentwicklung ist die Wahrscheinlichkeit, als Unternehmen früher oder später von einem Hack betroffen zu sein, derzeit so hoch wie nie – und wird weiter steigen.

Krisenmanagement und Krisenkommunikation müssen mit der Entwicklung Schritt halten

Krisenvorbereitung ist im unternehmerischen Alltag üblicherweise fest etabliert. Mit Cyberangriffen ist allerdings ein Risiko ins Portfolio eingezogen, das in seiner Veränderlichkeit auch eine dynamische Krisenvorbereitung erfordert. Dazu gehören eine regelmäßig aktualisierte Risikobewertung der IT-Systemlandschaft und der zugehörigen Lieferkette, der „Crown Jewels" des Unternehmens und deren Sicherheit sowie der für die unternehmerische Business-Continuity notwendigen Prozesse. Als Teil des Krisenmanagements und der ganzheitlichen Krisenvorbereitung des Unternehmens muss auch die Unternehmenskommunikation mit dem wachsenden Risiko von Cyberangriffen Schritt halten.

Haltung, Prozesse, Tools für die Krisenkommunikation – es geht um jedes Detail

Grundlage der Krisenvorbereitung ist ein gemeinsames unternehmerisches Verständnis zur Herangehensweise an die Krisenkommunikation. Die Bedürfnisse der Zielgruppen in den Mittelpunkt zu stellen, zügig zu informieren und operative Hilfestellung anzubieten wird oftmals als selbstverständlich angesehen, ist in der Praxis aber häufig mit personellen und

finanziellen Investitionen verbunden. Die Empathie, mit der ein Unternehmen seinen Kundinnen und Kunden, Mitarbeitern und Mitarbeiterinnen, den Finanzmärkten oder der Öffentlichkeit begegnen will, führt immer zu der auch juristisch diskutierten Frage, ob und in welcher Form man sich entschuldigt – oder auch nicht. Die Haltung eines Unternehmens übersetzt sich also in entsprechende strategische Entscheidungen, die im Vorfeld zu treffen sind.

Darauf baut eine klassische Toolbox auf mit Reputations-, Risiko- und Stakeholderanalyse, einem gut definierten Krisenkommunikationsprozess mit Rollen und Verantwortlichkeiten sowie definierten Schnittstellen innerhalb des Krisenstabs und in der Organisation. An diesem Punkt der Krisenvorbereitung geht es um jedes Detail. Die Krisenkommunikationsmaterialien – beispielsweise Holdingstatements, erste FAQ, Roll-out-Plan für individuelle Zielgruppen – müssen an zentraler Stelle aktualisiert werden und jederzeit online wie offline verfügbar sein. Für den Fall, dass Laufwerke verschlüsselt sind, braucht es redundante Speicherorte oder im Zweifel einen Ausdruck, auch im Homeoffice. Und wer hat noch mal den Zugang zum Content-Management-System von Website oder Darksite, wenn eine Erstinformation veröffentlicht werden soll?

Auch die Kanäle für Krisenkommunikation, intern wie extern, müssen priorisiert und zugänglich sein. Und nicht zuletzt sind ein ausreichend umfassendes Medien- und Social-Media-Monitoring sowie die Ressourcen für eine inhaltliche Krisenanalyse entscheidend, um den Überblick über Debattenumfang und -sentiment der Märkte und Zielgruppen zu behalten.

> „Grundlage der Krisenvorbereitung ist ein gemeinsames unternehmerisches Verständnis zur Herangehensweise an die Krisenkommunikation."

Ergänzt wird diese prozessorientierte Vorbereitung durch eine angemessene, kontinuierliche Trainingsroutine, die alle beteiligten Teams aktiviert und „auf der Stuhlkante" hält. Empfehlenswert ist, die Trainings nicht isoliert innerhalb der Unternehmenskommunikation umzusetzen, sondern gemeinsam mit dem Krisenmanagement-Team, das heißt mit allen denjenigen Funktionen und Personen umzusetzen, die auch im Krisenfall zusammenarbeiten werden. Speziell im Trainingsbereich lassen sich die dynamischen Veränderungen der Cybersicherheitslandschaft gut abbilden und adressieren, zum Beispiel in umfassenden Simulationen. Sorgfältig vorbereitete Szenarien auf Basis aktueller Trends und technischer Entwicklungen stellen sicher, dass die Krisenvorbereitung aktuell ist und Fälle trainiert werden, die für das Unternehmen tatsächlich relevant sind.

Priorität – 360-Grad-Blick auf alle Zielgruppen

Die Erwartungen sämtlicher Zielgruppen an die Kommunikation eines Unternehmens verändern sich stetig und erheblich. Investoren, Kunden, Mitarbeiter, politische Entscheidungsträger, Medien, die Öffentlichkeit und sonstige Interessengruppen interessieren sich stärker denn je für Managemententscheidungen und ethisches Verhalten von Unternehmen, aber auch für dessen Dialogkultur.

Es gilt: „Walk the talk!" Unternehmerische Werte werden gerade in der Krisenkommunikation unter Beweis gestellt. Die Art und Weise, wie ein Unternehmen in der Krise, aber auch im persönlichen Dialog, beispielsweise mit Kunden und Partnern, agiert, ist ein erheblicher Reputationsfaktor. Immer wieder tun sich Unternehmen aus unterschiedlichen, im Einzelnen häufig nachvollziehbaren Gründen schwer damit, eine Kommunikation zu liefern, die den Zielgruppen weiterhilft. Dabei entscheiden gerade die ersten Tage über den Erfolg von Krisenkommunikation.

Die gute Nachricht ist: Aktuelle Fälle zeigen, dass Kunden, Mitarbeiter, Investoren, Medien und weitere Zielgruppen durchaus Verständnis für Unternehmen aufbringen, wenn sie sich sorgfältig und angemessen informiert fühlen. ←

Suntka von Halen
Brunswick Group, München
Director, Co-Lead Cybersecurity Germany
svonhalen@brunswickgroup.com
www.brunswickgroup.com

Wer trägt die Verantwortung in Bezug auf Cybersicherheit?

Sorgfaltspflichten und Haftung von Führungskräften

Von Dr. Christian Schmitt und Dr. Benedict Heil

Typische Bausteine eines Cyber-Risikomanagementsystems sind die Ernennung eines fachlich qualifizierten IT-Sicherheitsbeauftragen, die Entwicklung und Umsetzung einer unternehmensinternen IT-Richtlinie, die regelmäßige Durchführung von Mitarbeiterschulungen sowie die Erstellung eines IT-Notfallplans.

Die Fließbänder laufen wieder, alle Systeme wurden erfolgreich zurückgesetzt. Knapp drei Wochen nach der Cyberattacke und dem ungeplanten Ausfall der Steuerungssoftware nimmt die Produktion wieder ihren gewohnten Gang. Geblieben sind finanzielle Schäden in beträchtlicher Höhe. Durch den Betriebsausfall konnten Lieferzusagen nicht eingehalten werden, Aufträge wurden storniert, Vertragsstrafen fällig. Schnell wird in einem solchen Szenario die Frage laut, wer die Verantwortung für den Vorfall trägt. Der Mitarbeiter, der den verdächtigen E-Mail-Anhang geöffnet hat? Der IT-Abteilungsleiter, der die sicherheitsrelevanten Updates für die Steuerungssoftware nicht im Blick hatte? Der Geschäftsführer, der dem Thema Cybersicherheit bislang keine Bedeutung beigemessen hat?

Der vorliegende Beitrag gibt Antwort auf die Fragen, wer im Falle eines Cyberangriffs finanziell zur Verantwortung gezogen werden kann, welche Sorgfaltspflichten Führungskräfte in Bezug auf die Cybersicherheit im Unternehmen zu erfüllen haben und welche Veränderungen in diesem Bereich zukünftig zu erwarten sind.

Wer haftet für Schäden bei Cyberangriffen?

Bei der Suche nach Haftungsadressaten für Schäden durch Cyberattacken wird man in erster Linie an den Angreifer oder an die Inanspruchnahme des Versicherers denken. Meistens kann der Angreifer jedoch nicht identifiziert werden, und viele Unternehmen haben keine Cyberversicherung abgeschlossen. Vor diesem Hintergrund rücken schnell die verantwortlichen Arbeitnehmer und Arbeitnehmerinnen im Unternehmen und dessen Leitungsorgane in den Blick.

Bei dieser sogenannten Innenhaftung ist strukturell zwischen Schadensersatzansprüchen der Gesellschaft gegen die organschaftliche Leitungsebene (Vorstände/Geschäftsführer) einerseits sowie gegen Führungskräfte und Mitarbeiter auf nachgelagerter Ebene andererseits zu unterscheiden:

- **Führungskräfte und Mitarbeiter unterhalb der Organebene**
  Eine persönliche Haftung von Mitarbeitern und Führungskräften unterhalb der Organebene kommt in

Betracht, wenn diese ihre Pflichten aus dem Arbeitsverhältnis schuldhaft verletzt haben. Dies kann der Fall sein, wenn die Durchführung sicherheitsrelevanter Softwareupdates unterblieben ist oder der Arbeitnehmer entgegen den Anweisungen einer unternehmensinternen IT-Richtlinie gehandelt hat. Die Arbeitnehmerhaftung ist jedoch der Höhe nach – auch bei leitenden Angestellten – entsprechend der von der Rechtsprechung entwickelten Kriterien begrenzt. Maßgeblich ist der Grad des persönlichen Verschuldens. Hat der Arbeitnehmer lediglich leicht fahrlässig gehandelt, ist ein Schadensersatzanspruch ausgeschlossen. Nur bei (grob) fahrlässigem oder vorsätzlichem Handeln haftet der Verantwortliche. Doch auch hier entscheiden die Gerichte über die Anspruchshöhe im Einzelfall unter Berücksichtigung der Höhe des eingetretenen Schadens und der persönlichen Leistungsfähigkeit des Arbeitnehmers. In aller Regel wird das Unternehmen den entstandenen Schaden auf diesem Weg allenfalls teilweise kompensieren können.

- **Vorstände und Geschäftsführer**
  Vorstandsmitglieder und Geschäftsführer, die ihre Pflichten verletzen, sind der Gesellschaft nach § 93 Absatz 2 AktG beziehungsweise § 43 Absatz 2 GmbHG zum Ersatz des daraus entstehenden Schadens verpflichtet; arbeitsrechtliche Einschränkungen greifen hier nicht. Dabei gilt eine Beweislastumkehr zu Lasten der Führungskraft. Mit anderen Worten: Bestehen Anhaltspunkte dafür, dass der Gesellschaft durch eine Pflichtverletzung ihres Leitungsorgans ein Schaden entstanden sein könnte, liegt es am jeweiligen Vorstandsmitglied bzw. Geschäftsführer zu beweisen, dass er seine Pflichten nicht verletzt hat. Gelingt dies nicht, haften sie gegenüber der Gesellschaft für den entstandenen Schaden grundsätzlich in voller Höhe. Ob der Schaden von einer zugunsten der Führungsorgane abgeschlossenen D&O-Versicherung umfasst ist, muss im Einzelfall geprüft werden. Jedenfalls ist für Vorstandsmitglieder einer Aktiengesellschaft ein zwingender Selbstbehalt in Höhe von 10% des Schadens bis mindestens zur Höhe des Eineinhalbfachen der festen jährlichen Vergütung gesetzlich vorgeschrieben.

Welche Sorgfaltspflichten treffen Führungskräfte in Bezug auf Cybersicherheit?

Vorstand und Geschäftsführung sind ganz allgemein zur Abwendung von der Gesellschaft drohenden Schäden verpflichtet. Hierfür haben sie ein angemessenes und wirksames internes Kontroll- sowie Risikomanagementsystem einzurichten, welches auch die Vorsorge gegen Cyberrisiken berücksichtigt. Erste Anhaltspunkte für dessen Inhalte können sich aus Normen wie dem IDW-Prüfungsstandard PS 340 oder – speziell für den Bereich Informationssicherheit – dem internationalen Standard ISO/IEC 27001 ergeben.

Bei der konkreten Umsetzung und Ausgestaltung des Cyberrisiko-Managementsystems steht Führungskräften jedoch ein Ermessensspielraum nach Maßgabe der sogenannten Business-Judgement-Rule (BJR) zu. Diese schließt eine Haftung aus, wenn der Geschäftsführer oder das Vorstandsmitglied bei einer unternehmerischen Entscheidung vernünftigerweise annehmen durfte, auf der Grundlage angemessener Informationen zum Wohle der Gesellschaft zu handeln. Zwingender Ausgangspunkt jeder Entscheidung ist daher die Beschaffung einer angemessenen Informationsbasis. Zu diesem Zweck sollten Führungskräfte eine Risikoanalyse durchführen.

Typische Bausteine eines Cyberrisiko-Managementsystems sind sodann die Ernennung eines fachlich qualifizierten IT-Sicherheitsbeauftragten, die Entwicklung und Umsetzung einer unternehmensinternen IT-Richtlinie, die regelmäßige Durchführung von Mitarbeiterschulungen sowie die Erstellung eines IT-Notfallplans. Darüber hinaus müssen Führungskräfte dafür Sorge tragen, dass alle auf ihr Unternehmen anwendbaren Gesetze im Bereich IT und Cybersicherheit eingehalten werden (IT-Compliance).

Je nach Branche und Tätigkeit können sich spezielle Anforderungen und Vorgaben für die Ausgestaltung des Cyberrisiko-Managementsystems ergeben:

- **Datenschutz**
  Bei jeglicher Verarbeitung personenbezogener Daten sind die Vorschriften der DSGVO zu beachten. Diese schreibt insbesondere die Einhaltung eines dem Risiko angemessenen Schutzniveaus bei der Datenverarbeitung vor, welche u.a. durch Pseudonymisierung, die Sicherstellung der Vertraulichkeit, Integrität und Belastbarkeit der verwendeten Systeme sowie regelmäßige Backups erfolgen kann. Darüber hinaus ist ein

Meldeprozess für Datenschutzverletzungen einzurichten, unter Umständen ist auch die Benennung eines Datenschutzbeauftragten und die Durchführung einer Datenschutzfolgenabschätzung erforderlich.

- **Banken und Versicherungen**
  Branchenspezifische Anforderungen gibt es insbesondere für Banken und Versicherungen. Führungskräfte sollten dringend die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) veröffentlichten Anforderungen an die IT von Banken (BAIT) und von Versicherungen (VAIT) beachten. Hervorzuheben sind etwa die Analyse- und Prüfpflichten vor Neueinführung von bzw. bei wesentlichen Änderungen an IT-Systemen, darüber hinaus im Zusammenhang mit der Ausgliederung von Dienstleistungen (IT-Outsourcing). Neue Pflichten für den Umgang mit Cyberrisiken im Finanzsektor enthält zudem der europäische „Digital Operational Resilience Act“ (DORA). [→ Reul/Mildahn, S. 12]

- **Kritische Infrastrukturen**
  Spezielle Vorgaben gelten ferner für Betreiber kritischer Infrastrukturen in den Bereichen Energie, Wasser, Gesundheit, Ernährung, Telekommunikation, Finanz- und Versicherungswesen sowie Verkehr. Seit Mai 2023 sind diese insbesondere zur Nutzung von Systemen zur Angriffserkennung verpflichtet.

Welche Änderungen sind zukünftig zu erwarten?

Anfang des Jahres ist die NIS2-Richtline (NIS: „Network and Information Security Directive“) in Kraft getreten, welche von den EU-Mitgliedstaaten bis Oktober 2024 in nationales Recht umgesetzt werden muss.

Die Richtlinie sieht eine erhebliche Ausweitung der Vorgaben zur Cybersicherheit in Unternehmen vor – mit unterschiedlichen Auswirkungen.

- **Mehr Unternehmen betroffen**
  Durch die NIS2-Richtlinie werden deutlich mehr Unternehmen spezielle IT-Sicherheitsvorgaben erfüllen müssen. Die Richtline gibt eine nach Sektor und Unternehmensgröße gestaffelte Regulierung vor. In den Anwendungsbereich der Richtlinie können Unternehmen schon ab einer Größe von 50 Mitarbeitern und/oder bei Tätigkeit in einem der insgesamt 18 genannten Sektoren fallen.

- **Umfassendere Pflichten**
  Die Richtlinie legt eine Reihe verpflichtender Maßnahmen zum Schutz vor IT-Sicherheitsvorfällen fest. Hierzu zählen u.a. Vorgaben zum Krisenmanagement, verpflichtende Sicherheitsschulungen, der Einsatz kryptografischer Verfahren sowie die Verwendung zertifizierter IT-Produkte. Darüber hinaus müssen betroffene Unternehmen künftig auch Maßnahmen zur Sicherstellung der Informationssicherheit in der Lieferkette ergreifen.

- **Höhere Bußgelder**
  Für Bußgelder sieht die Richtlinie eine Höhe von bis zu 10 Millionen Euro oder 2% des weltweiten Jahresumsatzes vor. Zuständig für die Verhängung von Bußgeldern ist das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Checkliste für Führungskräfte

Zur Vermeidung der persönlichen Haftung im Falle eines Cyberangriffs auf ihr Unternehmen sollten sich Führungskräfte die folgenden Fragen stellen:

- Welche rechtlichen Vorgaben sind von meinem Unternehmen im Bereich Cybersicherheit zu beachten? Fällt mein Unternehmen zukünftig in den Anwendungsbereich der NIS2-Richtlinie?

- Wurde bereits eine IT-Risikoanalyse als Entscheidungsgrundlage für die Ausgestaltung des IT-Risikomanagementsystems durchgeführt?

- Haben wir bereits einen fachlich qualifizierten IT-Sicherheitsbeauftragten benannt und mit der Erstellung einer unternehmensinternen IT-Richtlinie, einem IT-Notfallplan und der Durchführung regelmäßiger Mitarbeiterschulungen im Bereich Cybersicherheit beauftragt? Werden diese einer regelmäßigen Prüfung und Aktualisierung unterzogen? ←

Dr. Christian Schmitt
Linklaters LLP,
Frankfurt am Main
Partner, Litigation,
Arbitration & Investigations
christian.schmitt@linklaters.com
www.linklaters.de

Dr. Benedict Heil
Linklaters LLP,
Frankfurt am Main
Associate, Litigation,
Arbitration & Investigations
benedict.heil@linklaters.com
www.linklaters.de

Arbeitsrechtliche Herausforderungen im Fall einer Cyberattacke

Handlungsoptionen in der Praxis

Von Dr. Timon A. Grau

Der Rahmen der IT-Nutzung in einem Unternehmen lässt sich durch sogenannte IT-Policies abstecken. In diesen können etwa ein IT-Sicherheitsbeauftragter bestimmt oder Richtlinien zur Verwendung der Dienstgeräte aufgestellt werden.

Cyberangriffe sind infolge immer weiter voranschreitender Digitalisierungsprozesse kein singuläres Phänomen mehr. Sie betreffen Staat und Gesellschaft im Ganzen, besonders auch die deutsche Wirtschaft. Moderne Formen der Cyberkriminalität richten sich dabei nicht allein gegen große, umsatzstarke, sondern vielmehr auch gegen kleine und mittelständische Unternehmen (KMU). Im Folgenden soll ein Überblick über typische arbeitsrechtliche Fragestellungen gegeben werden, die im Zusammenhang mit Cyberattacken stehen.

Unmittelbare arbeitsrechtliche Folgen

Folge der Kompromittierung des IT-Netzwerks des Arbeitgebers kann sein, dass Arbeitnehmer Arbeitsaufträge nicht mehr wie üblich abwickeln können. Etwa lassen sich Laptops

nicht mehr bedienen oder Maschinen nicht mehr steuern, es kommt zu Betriebsunterbrechungen bis hin zum Stillstand ganzer Anlagen oder Betriebe. Bietet der Arbeitnehmer seine Arbeitsleistung an, aber kann der Arbeitgeber ihn nicht beschäftigen, bleibt der Vergütungsanspruch des Arbeitnehmers ohne Nachleistungspflicht bestehen (sogenanntes Betriebsrisiko). Nicht möglich ist es in solchen Fällen, dem Mitarbeiter spontan vorzugeben, gegen seinen Willen Urlaub zu nehmen. Das Weisungsrecht des Arbeitgebers erlaubt es jedoch, dem Arbeitnehmer – soweit möglich – eine gleichwertige alternative Aufgabe zuzuweisen, die trotz Ausfalls der IT-Infrastruktur erfüllbar ist. Existiert ein Betriebsrat, könnte durch eine „Cyberbetriebsvereinbarung“ die Frage der Beschäftigung vorbeugend konkretisiert werden. Auch Kurzarbeit wäre eine Option, scheitert in der Regel jedoch an der fehlenden Planbarkeit. Denkbar, aber teuer sind auch maßgeschneiderte Versicherungen gegen wirtschaftliche Risiken einschließlich der Verluste durch weiterlaufende Personalkosten bei einem cyberbedingten Produktivitätsausfall.

Fortbildungen

Ein wichtiges Instrument zur Prävention von Cyberangriffen stellen Mitarbeiterfortbildungen dar. Aufklärung darüber, wie verdächtige Anhänge von E-Mails oder zugespielte Direktlinks erkannt und schadfrei isoliert werden können, gehört in der Praxis zu den wichtigsten Mitteln, um Gefahren aus dem Cyberbereich vorzubeugen.

Arbeitgeber und Betriebsrat kommt gemeinsam die Aufgabe zu, die Berufsbildung der Arbeitnehmer zu fördern. Darunter fallen auch Lehrgänge, die Kenntnisse und Fähigkeiten im Zusammenhang mit der Gefahrenerkennung und -abwehr im Cyberbereich verschaffen. Bei deren Ausgestaltung sind die Rechte des Betriebsrats allerdings eingeschränkt: Ein echtes Mitbestimmungsrecht greift nur dann, wenn sich das Tätigkeitsprofil der Arbeitnehmer durch eine Maßnahme ändert und die beruflichen Kenntnisse und Fähigkeiten zur Aufgabenerfüllung nicht mehr ausreichen. Strebt der Arbeitgeber also die Etablierung von Tutorien oder Lernprogrammen zu Zwecken der bloßen Aufklärung über die Risiken und zu beachtenden Sicherheitsmaßnahmen an, löst dies nicht zwangsläufig ein Mitbestimmungsrecht aus. Anders ist es, wenn zum Beispiel bei E-Learning im Nachhinein automatisch kontrolliert werden kann, wer wann welche Schulung absolviert hat.

> „Folge der Kompromittierung des IT-Netzwerks des Arbeitgebers kann sein, dass Arbeitnehmer Arbeitsaufträge nicht mehr wie üblich abwickeln können.“

Das Arbeitszeitrecht gebietet eine Unterscheidung zwischen obligatorischen und rein freiwilligen Fortbildungen. Veranlasst der Arbeitgeber ein freiwilliges Fortbildungsangebot, zählt dieses allgemein nicht zur Arbeitszeit, es sei denn, vertraglich oder kollektivrechtlich sind abweichende Regelungen vereinbart worden. Insofern steht dem Arbeitnehmer auch kein Vergütungsanspruch für eine wahrgenommene Schulung zu. Demgegenüber ist die Teilnahme an einem vom Arbeitgeber angewiesenen Pflichtangebot jeweils der Arbeitszeit des Arbeitnehmers zuzurechnen und mithin auch vergütungspflichtig. Das dürfte bei IT-Sicherheitsschulungen der Normalfall sein.

IT-Policy

Der Rahmen der IT-Nutzung in einem Unternehmen lässt sich durch sogenannte IT-Policies abstecken. In diesen können etwa ein IT-Sicherheitsbeauftragter bestimmt oder Richtlinien zur Verwendung der Dienstgeräte aufgestellt werden. Möglich ist es etwa, durch solche Regelwerke die private Nutzung oder Einbringung von Geräten zu untersagen, Passwortvorgaben zu etablieren oder regelwidrige Verhaltensweisen, wie etwa das unbefugte Weitergeben von Accountdaten oder die Manipulation der IT-Systeme, festzulegen. Entscheidet sich der Arbeitgeber für die Etablierung solcher IT-Richtlinien, sind Mitbestimmungsrechte zu beachten.

Beschäftigtendatenschutz bei Prävention und Sachverhaltsaufklärung

Möglich ist der Einsatz von Überwachungssoftware zur Prävention von Gefahren aus dem Cyberbereich. Diese ist imstande, durch die Auswertung von Daten Bedrohungsszenarien zu erkennen und Warnungen zu erstellen. Bei der Einführung solcher Systeme besteht nicht stets ein Mit-

bestimmungsrecht des Betriebsrats. Dieses greift aber dann, wenn durch die Datenerhebung oder -verarbeitung eine Verhaltens- oder Leistungskontrolle von Arbeitnehmern durch die erhobenen Daten möglich ist, selbst wenn diese nicht Ziel des Einsatzes ist. Ist ein Personenbezug der Daten nicht gegeben, scheidet ein Mitbestimmungsrecht aus. Dennoch ist überall dort, wo es um den Einsatz digitaler Überwachungstechnologien geht, ein umfassender Regelungsrahmen durch Kollektivvereinbarung (zum Beispiel einer Betriebsvereinbarung) zu empfehlen. Im Fall der Erhebung personenbezogener Beschäftigtendaten kann diese zugleich auch datenschutzrechtlich als Rechtsgrundlage für das Erheben, Verarbeiten und Nutzen von Beschäftigtendaten dienen.

> „Entscheidet sich der Arbeitgeber für die Etablierung von IT-Richtlinien, sind Mitbestimmungsrechte zu beachten."

Kam es zu einem Cyberangriff, sind verschiedene Aufklärungsarten möglich. Zu denken ist etwa an Mitarbeiterbefragungen oder an den Einsatz von Filtersoftware, um verdächtige Datensätze (etwa E-Mail- oder Cloudinhalte) zu überprüfen. Betrifft die automatisierte Auswertung Daten, die einen Leistungs- oder Verhaltensbezug aufweisen, steht dem Betriebsrat ein Mitbestimmungsrecht zu. Demgegenüber unterliegen aufklärende Mitarbeitergespräche regelmäßig nicht der Mitbestimmung. Diese kann der Arbeitgeber vielmehr einseitig anordnen – der Arbeitnehmer ist zur Teilnahme am Interview und zu einer wahrheitsgemäßen Aussage verpflichtet, wenn es um den eigenen Arbeitsbereich geht. Datenschutzrechtlich besonders problematisch gestaltet sich die Aufklärung, wenn Dienstgeräte in der Freizeit oder private Endgeräte dienstlich genutzt werden dürfen („Bring your own device"). Hier sind persönliche Daten meist eng mit dienstlichen Inhalten verknüpft, was den Zugriff des Arbeitgebers auf die dienstlichen Daten rechtlich erschwert. In diesen Fällen ist eine sorgfältige Prüfung anzuraten, um (straf)rechtliche Risiken zu vermeiden, bevor auf die Daten zugegriffen wird.

Haftung und arbeitsrechtliche Konsequenzen

Eine Gefahr geht für Unternehmen im Cyberbereich oftmals auch unwillkürlich von den eigenen Mitarbeitern aus, da diese Zugriff auf die internen IT-Strukturen haben. Erzeugt ein Arbeitnehmer durch ein Verhalten, wie das unbedachte Öffnen eines verdächtigen E-Mail-Anhangs, die Ursache für das Verbreiten der Schadsoftware, kommt es allgemein nur dann zu einer weitgehenden oder vollständigen Haftung, wenn vorsätzlich oder grob fahrlässig gehandelt wurde (Haftungsprivilegierung). [→ Schmitt/Heil, S. 18]

Neben einer Haftung für die verursachten Schäden ist an disziplinarische Konsequenzen zu denken, wenn zum Beispiel gegen die internen Anweisungen zur IT-Sicherheit verstoßen worden ist. Dies kann je nach Schwere des Verstoßes und seiner Folgen, je nach Grad des Verschuldens und weiteren abwägungsrelevanten Umständen bis zu einer außerordentlichen Kündigung führen. Möglich ist zudem eine Kündigung „auf Verdacht", wenn etwa die Ergebnisse interner Untersuchungen aufzeigen, dass ein Arbeitnehmer mit großer Wahrscheinlichkeit Täter einer Cyberattacke war. Auch eine Abmahnung kommt bei Verstößen gegen IT-Policies in Betracht. ←

Dr. Timon A. Grau
Linklaters LLP, Düsseldorf
Partner, Employment
timon.grau@linklaters.com
www.linklaters.de

Strafverfolgung im Cyberraum

Warum Unternehmen handeln sollten

Von Dr. Kerstin Wilhelm

Mitteilungen über Unternehmen, die Opfer von Cyberkriminalität geworden sind, gehören mittlerweile schon fast zum Alltag. Die Bedrohung im Cyberraum ist, ausweislich des aktuellen Berichts des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Lage der IT-Sicherheit in Deutschland, so hoch wie nie zuvor. Dies spiegelt sich auch in der jüngsten Statistik des Bundeskriminalamts (BKA) wider, wonach im Jahr 2022 insgesamt 136.865 Fälle von Cyberkriminalität erfasst worden sind. Doch die Statistik zeigt noch nicht einmal die ganze Wahrheit, denn tatsächlich handelt es sich hierbei nur um die Spitze des Eisbergs: So nimmt das BKA eine hohe Dunkelziffer von bis zu 90% an, was bedeutet, dass im Schnitt nur einer von zehn kriminellen Cyberangriffen überhaupt zur Anzeige gebracht wird. Eine effektive Strafverfolgung wird so erschwert. Hinzu kommt, dass es den Behörden kaum möglich ist, sich ein zutreffendes Bild der aktuellen Gefährdungslage zu machen, wenn sie nur einen Bruchteil der Vorfälle kennen.

Warum erstatten betroffene Unternehmen keine Strafanzeige?

Jedes Unternehmen wird individuelle Gründe dafür haben, warum es Ermittlungsbehörden nicht mit ins Boot holen möchte. Oftmals dürfte die Befürchtung ausschlaggebend sein, dass durch die Involvierung Dritter das Risiko eines öffentlichen Bekanntwerdens des Vorfalls und damit einhergehend die Gefahr eines möglichen Reputationsschadens oder gar möglicher Wettbewerbsnachteile steigt.

Denkbar ist auch, dass sich Unternehmen gerade bei erfolgreich abgewendeten oder glimpflich verlaufenden Cyberangriffen schlicht keinen Vorteil von einer Anzeige versprechen, sondern vielmehr langwierige und ergebnislos laufende Ermittlungen erwarten.

Auch können vom konkreten Angriff losgelöste Motive eine Rolle spielen: So soll es laut BKA Fälle geben, in denen Unternehmen Sorge haben, ihrerseits zum Gegenstand eines separaten Strafverfahrens zu werden, etwa wenn Unternehmen keine ausreichend lizenzierte Software nutzen oder wissen, dass sich illegale Dateien auf den Firmenrechnern befinden.

Ein weiterer Grund wird die tatsächliche Unkenntnis darüber sein, wie ein strafrechtliches Ermittlungsverfahren abläuft, da manche Unternehmen vermutlich Bedenken haben, dass die Einbindung der Behörden ihren weiteren Betriebsablauf (zusätzlich) stören könnte, beispielsweise weil sie eine Sicherstellung der geschäftlichen Computer befürchten.

Vorteile der Zusammenarbeit mit den Strafverfolgungsbehörden

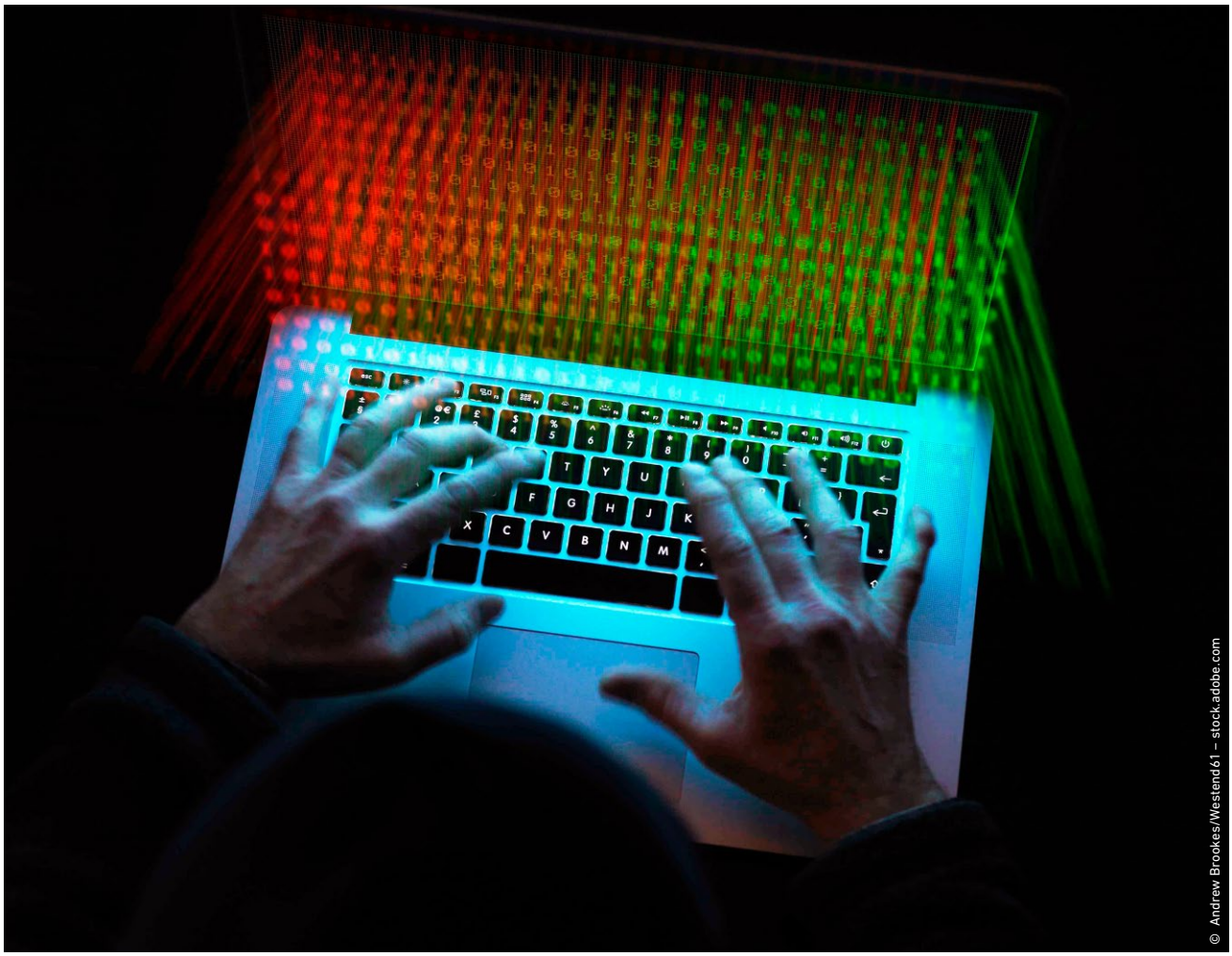
Typischerweise ist es für betroffene Unternehmen kaum möglich, selbst zu identifizieren, wer der konkrete Urheber des gegen sie gerichteten Angriffs ist, da die meisten Cyberangriffe unter dem Deckmantel der Anonymität begangen werden und die den Unternehmen zur Verfügung stehenden investigativen Optionen naturgemäß limitiert sind. Zu wissen, wer hinter dem Angriff steckt, ist mit Blick auf eine spätere Verfolgung zivilrechtlicher Schadensersatzansprüche von Bedeutung und wird umso wichtiger, je größer die dem Unternehmen durch den Cyberangriff entstandenen Schäden sind. Insoweit ist hier nicht nur an die Kosten zu denken, die im Zusammenhang mit der Abwehr und der Behebung der durch den Angriff verursachten Schäden am internen IT-System entstehen. Eine Rolle spielt auch das finanzielle Risiko durch Ansprüche, die von durch den Cybervorfall betroffenen Dritten gegenüber dem Unternehmen geltend gemacht werden könnten, insbesondere wenn solche Drittschäden nicht von einer Cyberpolice abgedeckt werden oder das Unternehmen keine solche Versicherung vor dem Vorfall abgeschlossen hatte.

Die Strafverfolgungsbehörden hingegen verfügen über eine breite Palette

von möglichen Ermittlungsmaßnahmen zur Identifikation der Täter, die Privatpersonen und Unternehmen nicht zustehen, etwa weil es sich um öffentlich nicht zugängliche Informationsquellen handelt, auf die nur mit hoheitlichen Befugnissen zugegriffen werden kann.

So können Strafverfolgungsbehörden beispielsweise Durchsuchungsmaßnahmen anordnen mit dem Ziel der Sicherung von relevantem Beweismaterial, unter anderem durch die Beschlagnahme von physischen Datenträgern oder sonstigen Unterlagen. Möglich sind unter bestimmten Voraussetzungen darüber hinaus auch eine Onlinedurchsuchung, bei der die Behörden remote auf den Computer des mutmaßlich Tatverdächtigen zugreifen, ohne dass dieser von dem Zugriff etwas mitbekommt, oder eine Überwachung des E-Mail-Verkehrs, die sich auch auf Maßnahmen im Endgerät des Angreifers erstrecken kann. Gleichsam verfügen die Ermittlungsbehörden über die Befugnis, mittels der IP-Adresse eine Bestandsdatenabfrage beim Provider durchzuführen, um in Erfahrung zu bringen, welchem Anschluss die IP-Adresse zum Zeitpunkt des Cyberangriffs zugeordnet war, und so die eine Identifizierung ermöglichenden Vertragsdaten des Anschlussinhabers beziehungsweise Tatverdächtigen zu erhalten.

Dabei machen die Ermittlungen nicht an der Landesgrenze halt: Soweit Cyberangriffe aus dem Ausland erfolgen – was häufig und mit steigender Tendenz der Fall ist –, können die Strafverfolgungsbehörden im Wege der internationalen Rechtshilfe Beweise sichern und unter Umständen auch Täter aus dem Ausland verfolgen.



© Andrew Brookes/Westend61 – stock.adobe.com

Für betroffene Unternehmen ist es kaum möglich, selbst zu identifizieren, wer der Urheber des gegen sie gerichteten Angriffs ist, da die meisten Cyberangriffe anonym begangen werden und die den Unternehmen zur Verfügung stehenden investigativen Optionen naturgemäß limitiert sind.

„Time is of the essence“

Wird ein Unternehmen Opfer einer Cyberattacke, befindet es sich im akuten Krisenmodus und steht vor der Herausforderung, unter Zeitdruck angemessene Entscheidungen für die Bewältigung einer Situation zu treffen, deren Ausmaß in den meisten Fällen noch nicht eingeschätzt werden kann. Priorisierung von Aufgaben ist in einer solchen Konstellation unerlässlich, und die Entscheidung, ob das Unternehmen die Strafverfolgungsbehörden involviert, sollte nicht auf die lange Bank geschoben werden. Je mehr Zeit verstreicht, desto größer ist das Risiko, dass digitale Spuren „verwischt“ und entsprechende Beweismittel vernichtet werden, was eine Ermittlung des Täters erschwert.

Strafanzeige – was passiert nun?

Hat ein Unternehmen sich für eine Anzeige entschieden, kann es sich dazu entweder an die Polizei, die Staatsanwaltschaft oder an die sogenannten Zentralen Ansprechstellen Cybercrime (ZAC) wenden, die bei den Landeskriminalämtern speziell dafür eingerichtet worden sind, Unternehmen bei IT-Sicherheitsvorfällen zu unterstützen. Unmittelbare Kosten fallen hierdurch nicht an, und besondere Formerfordernisse sind ebenfalls nicht zu beachten. Allerdings bietet es sich an, den Ermittlern so viele Details über den Vorfall wie möglich (und bekannt) mitzuteilen, damit diese zielgerichtet tätig werden können. Konkrete Straftatbestände, die aus Sicht des Unternehmens in Betracht kommen, müssen aber nicht bezeichnet werden.

Welche Maßnahmen die Ermittlungsbehörden dann ergreifen und welche Informationen vom Unternehmen benötigt werden, hängt vom Einzelfall beziehungsweise der Art des konkreten Angriffs ab. Regelmäßig wird es zu einer forensischen Datensicherung der als beweisrelevant erachteten Daten des Unternehmens und zu einer diesbezüglich sorgfältigen Dokumentation kommen. Dies ist vor allem mit Blick auf den Beweiswert der Daten von Bedeutung. Nur wenn belegt werden kann, dass die Daten ordnungsgemäß gesichert und nach ihrer Sicherstellung nicht verändert worden sind, kann an ihrer Integrität im Rahmen des strafrechtlichen Verfahrens nicht gerüttelt werden.

> „Jedes Unternehmen wird individuelle Gründe dafür haben, warum es Ermittlungsbehörden nicht mit ins Boot holen möchte.“

Dem Unternehmen steht als Geschädigtem im Verfahren unter anderem auch das Recht zu, Akteneinsicht in die strafrechtliche Ermittlungsakte zu verlangen, was insbesondere für die etwaige Geltendmachung von Ersatzansprüchen erforderlich sein kann. Hat der Täter Vermögenswerte des angegriffenen Unternehmens erbeutet, so kann es sinnvoll sein, die Anordnung eines sogenannten Vermögensarrests anzuregen, um Vermögenswerte, etwa auf dem Konto des Täters, vorläufig sicherzustellen. Sofern ein Täter identifiziert wird und dieser in einem Strafverfahren für seine Taten zur Rechenschaft gezogen wird, besteht für das Unternehmen auch die Option eines sogenannten Adhäsionsverfahrens. Ein solches Verfahren erlaubt es dem Unternehmen als dem Verletzten der Straftat, seine zivilrechtlichen Schadensersatzansprüche gegen den Angreifer in dem gegen ihn gerichteten Strafverfahren geltend zu machen.

Fazit

Trotz der in der Praxis – ausweislich der Polizeilichen Kriminalstatistik (PKS) – noch relativ niedrigen Aufklärungsquote von knapp 30% der erfassten Cyberkriminalitätsfälle im Jahr 2022 ist es für Unternehmen häufig empfehlenswert, sich im Fall eines Cyberangriffs an die Strafverfolgungsbehörden zu wenden. Wie so oft gilt auch hier: Je schneller ein Vorfall gemeldet wird, desto höher sind die Chancen auf eine Täterermittlung und damit – je nach Konstellation – auch auf die etwaige Sicherung von Vermögenswerten. ←

Dr. Kerstin Wilhelm
Linklaters LLP, München
Partner, German Co-Head of Crisis Management & Compliance
kerstin.wilhelm@linklaters.com
www.linklaters.de

Zahlen oder Zittern?

Lösegeldforderungen bei Cyberangriffen

Von Dr. Jochen Laufersweiler, Dr. Christian Schmitt und Dr. Klaus von der Linden

Es versteht sich von selbst, dass Erpressung verboten und strafbar ist. Doch kann für die Zahlung von Lösegeld Ähnliches gelten.

Die Ausgangs- und Bedrohungslage

Cyberangriffe sind heute für Unternehmen eine allgegenwärtige Bedrohung mit potentiell verheerenden Auswirkungen: Sensible Daten können verlorengehen oder an die Öffentlichkeit dringen, Produktionsabläufe und Lieferketten können unterbrochen werden, im schlechtesten Fall steht das Unternehmen auf unabsehbare Zeit still. All das geht einher mit horrenden finanziellen und reputativen Schäden. Die Unternehmen sind deshalb gut beraten, in hohem Maße in ihre Datensicherheit und in die Prävention von Cyberangriffen zu investieren. Mehr noch: Beides gehört heute für Geschäftsführer, Vorstände und Aufsichtsräte sogar zum unabdingbaren Pflichtenprogramm [→ Schmitt/Heil, S. 18]. Doch selbst die beste Prävention bietet bekanntlich keinen lückenlosen Schutz. Dem entspricht es, dass Unternehmen sich nicht nur auf die Abwehr eines etwaigen Cyberangriffs vorbereiten müssen – sondern auch auf den unliebsamen Fall, dass der Angreifer Erfolg hat. Eine Kernfrage in diesem Kontext ist: Darf ein Unternehmen, das zum Opfer eines Cyberangriffs geworden ist, dem Angreifer ein Lösegeld zahlen, um die Rück- oder Freigabe seiner Daten zu erreichen und so seinen Schaden zu begrenzen?

Darauf gibt es keine einfache Antwort. Sicherheits- und Strafverfolgungsbehörden raten zwar nachdrücklich von solchen Zahlungen ab. Die Reali-

tät ist aber eine andere: Studien deuten darauf hin, dass über 40% der erpressten Unternehmen in Deutschland das geforderte Lösegeld zahlen. Der Druck auf die Unternehmen ist also offenbar immens. Umso wichtiger ist es, dass die Unternehmen sich auch insoweit nach Kräften auf den Ernstfall vorbereiten. Denn anderenfalls lassen sich unter dem Eindruck eines laufenden Cyberangriffs sowie einer zumeist knapp bemessenen Zahlungsfrist schwerlich besonnene Entscheidungen treffen.

> „Cyberangriffe sind heute für Unternehmen eine allgegenwärtige Bedrohung mit potentiell verheerenden Auswirkungen."

Ein Playbook – ähnlich einem übernahmerechtlichen Defence-Manual – kann hierbei ein wichtiges Hilfsmittel sein. Darin sollte sich neben inhaltlichen Entscheidungskriterien insbesondere die unternehmensinterne Meldekette finden:

- Wo kann die erpresserische Forderung realistischerweise eingehen?
- Wer leitet sie an wen weiter?
- Welche externen Berater sind einzubeziehen, um technisch, rechtlich und kommunikativ zu unterstützen?
- Wer informiert wann welche Behörden?
- Welche Personen und Abteilungen sollten umgekehrt zunächst außen vor bleiben, damit die Information über die eigene Verwundbarkeit sich nicht verselbstständigt und so in die weitere Belegschaft oder gar nach außen dringt?

Zudem gehört hierher die Frage, ob und wann die Geschäftsleitung sich vor einer Entscheidung an die Gesellschafter wenden sollte – denn ein Lösegeld geht in letzter Konsequenz zu deren finanziellen Lasten. Eine realistische Option ist dies aber allenfalls in Unternehmen mit sehr überschaubarem Gesellschafterkreis. Der Vorstand einer börsennotierten Gesellschaft hingegen hat keine andere Wahl, als die Entscheidung ohne die Aktionäre zu treffen – denn die Hauptversammlung kann weder kurzfristig zusammentreten noch die nötige Vertraulichkeit wahren. Zu bedenken ist auch, ob und wie Zustimmungsvorbehalte trotz Eilbedürftigkeit und Vertraulichkeitsbedürfnis erfüllt werden können. In Abwesenheit klarer Vorgaben ist regelmäßig zumindest der Aufsichtsratsvorsitzende einzubeziehen, der je nach Lage des Falls seinerseits das Präsidium oder den Gesamtaufsichtsrat informieren und um ein Votum ersuchen wird.

Darf man sich erpressen lassen?

Es versteht sich von selbst, dass Erpressung verboten und strafbar ist. Doch kann für die Zahlung von Lösegeld Ähnliches gelten – zum einen, weil sie auf die finanzielle Unterstützung einer kriminellen oder gar einer terroristischen Vereinigung hinauslaufen kann. Und zum anderen, weil im Einzelfall auch Sanktionsregime der Europäischen Union, der Vereinten Nationen oder – besonders brisant – der USA verletzt sein könnten, wenn und weil die Zahlung in sanktionierte Staaten, an sanktionierte Personen oder in sanktionierte Aktivitäten fließt. Der Geschäftsleiter mag sich demgegenüber im Einzelfall allerdings auf einen rechtfertigenden Notstand berufen. Das gelingt umso eher, je schwerer die Konsequenzen des Angriffs wiegen und je geringer im Verhältnis dazu das Lösegeld ausfällt. Dabei kommen nicht nur die finanziellen und reputativen Auswirkungen auf das Unternehmen selbst in Betracht.

Namentlich bei Angriffen auf Unternehmen, die kritische Infrastrukturen unterhalten, fließen auch die Rechtsgüter Dritter in die Betrachtung ein – so etwa Gesundheit und Leben der Patienten eines angegriffenen Krankenhauses oder die öffentliche Verkehrs- und Versorgungssicherheit beim Angriff auf einen Energieversorger. Zwar haben Strafgerichte sich bislang mit diesen Fragen noch nicht

Red Flags für Sanktionsrisiken

Hinweise auf sanktionierte Staaten
Hinweise auf sanktionierte Personen (zum Beispiel SDN-Liste der USA)
Hinweise auf sanktionierte Sektoren oder auf sanktionierte Aktivitäten (zum Beispiel Terrorismus oder Geschäfte mit Dual-Use-Gütern)
US-Bezug – etwa durch eigene Mitarbeiter oder Konzerngesellschaften in den USA, Abwicklung der Lösegeldzahlung über US-Personen (zum Beispiel Banken bei US-Dollar-Zahlungen)
Schwer nachvollziehbare Zahlungsmethode des Lösegelds (zum Beispiel Kryptowährungen wie Bitcoin)

befasst. Das aber liegt daran, dass keine Fälle bekannt sind, in denen Strafverfolgungsbehörden ein Lösegeld überhaupt zum Anlass für eine Anklage gegen den zahlungsbereiten Geschäftsleiter genommen hätten.

Es ist somit immerhin denkbar, bei Cyberangriffen ein Lösegeld zu zahlen, ohne dabei gegen geltendes Recht zu verstoßen. Diese Feststellung ist wichtig, führt sie doch aus gesellschaftsrechtlicher Perspektive fort von der strikten Legalitätspflicht des Geschäftsleiters und hin zur flexiblen Business-Judgement-Rule. Kurzum: Der Geschäftsleiter darf und muss nach pflichtgemäßem Ermessen selbst abwägen und einschätzen, was dem Wohl seines Unternehmens eher dient – das Aussitzen der Drucksituation oder aber ein Nachgeben durch Zahlung von Lösegeld.

Entscheidend ist dabei auch, ob er annehmen darf, auf Basis angemessener Information zu handeln. Das führt zurück zum eingangs erwähnten Playbook für erpresserische Cyberangriffe. Ein wesentlicher Baustein dieses Playbooks muss es nämlich sein, vertrauenswürdige IT-Experten an der Hand zu haben, um die Lage zu beurteilen. Erst die Feststellung eines solchen Experten, dass die betroffenen Daten anders nicht wiedergewonnen werden können, eröffnet den Ausweg der Lösegeldzahlung.

Darüber hinaus muss der Geschäftsleiter etwaige Hinweise auf die Identität der Angreifer sammeln und auswerten lassen – einschließlich etwaiger Red Flags für Sanktionsrisiken. Auch muss er die Folgen abschätzen, die dem Unternehmen drohen, falls es sich gegen ein Lösegeld entscheidet. Umgekehrt ist aber auch zu bedenken, dass ein Lösegeld keine Garantie ist, die Daten tatsächlich zurückzuerhalten. Ferner ist das Risiko einzupreisen, als nachweislich „leichtes Opfer“ später noch weitere Erpressungsversuche zu erleben.

Wer haftet?

Wie auch immer der Geschäftsleiter sich entscheidet: Ein erfolgreicher Cyberangriff wirft die Frage nach seiner Organhaftung auf. Das Lösegeld kann hierbei einen weiteren Schadensposten bilden, ist aber für die Haftungsfrage zumeist nicht konstitutiv. Je nach Rechtsform des Unternehmens werden daher entweder der Aufsichtsrat oder die Gesellschafter auf Fehlersuche gehen.

Dabei rückt dann die Frage nach angemessener Risikoprävention in den Fokus. Bestanden ausreichende technische Abwehrmechanismen? Gab es Backups, die einen Datenverlust verkraftbar gemacht hätten? Waren Mitarbeiter in ausreichendem Maße für die Gefahren eines Cyberangriffs sensibilisiert und geschult? Und gab es für den Notfall einen angemessenen Ablaufplan? Der Geschäftsleiter tut daher gut daran, all diese Punkte im ureigenen Interesse sorgsam zu dokumentieren – denn im Streitfall muss er nachweisen, dass er seine Sorgfaltspflichten eingehalten hat.

Auch ist zur Begrenzung des Haftungsrisikos an ausreichenden Versicherungsschutz zu denken, und zwar in zweifacher Hinsicht: erstens in Gestalt der herkömmlichen D&O-Versicherung, die den Geschäftsleiter als solchen gegen Eigenhaftung absichert und zugleich dem Unternehmen einen leistungsstarken zweiten Schuldner verschafft; und zweitens, indem geprüft wird, ob das Unternehmen sein eigenes Risiko ergänzend durch eine sogenannte Cyberversicherung abmildern sollte, um etwaige Lösegelder zu kompensieren. Dabei lässt sich aber feststellen, dass die Bedingungen einer Cyberversicherung eine Einstandspflicht regelmäßig nur dann vorsehen, wenn das Unternehmen umfassende Sicherheitsvorkehrungen getroffen hat. Es geht hier also um solche Fälle, in denen eine Verletzung der Sorgfaltspflicht und somit eine Organhaftung gerade nicht in Rede stehen – oder zumindest im Ergebnis ausscheiden. ←

Dr. Jochen Laufersweiler
Linklaters LLP,
Frankfurt am Main
Partner, Gesellschaftsrecht/M&A
jochen.laufersweiler@linklaters.com
www.linklaters.de

Dr. Christian Schmitt
Linklaters LLP,
Frankfurt am Main
Partner, Litigation,
Arbitration & Investigations
christian.schmitt@linklaters.com
www.linklaters.de

Dr. Klaus von der Linden
Linklaters LLP,
Düsseldorf
Partner, Gesellschaftsrecht/M&A
klaus.von_der_linden@linklaters.com
www.linklaters.de

Insgesamt können Unternehmen im Zusammenhang mit Cybersicherheitsvorfällen eine Vielzahl von Meldepflichten treffen.

Schweigen ist Gold?

Meldepflichten bei Cybersicherheitsvorfällen

Von Dr. Daniel A. Pauly und Selma Nabulsi

Mit fortschreitender Digitalisierung von Unternehmensprozessen steigt die Wahrscheinlichkeit von Cybersicherheitsvorfällen. Was in der Vergangenheit noch als Schreckensszenario eingeordnet wurde, ist mittlerweile nur eine Frage der Zeit. Eine gründliche Vorbereitung auf Cyberbedrohungslagen beinhaltet daher stets auch die Vorbereitung einer angemessenen Reaktion auf einen Cybersicherheitsvorfall. Dazu sollten Unternehmen wissen, welche Verpflichtungen sie unmittelbar nach einem solchen Vorfall treffen: In welchen Fällen muss der Cybersicherheitsvorfall gemeldet werden und an wen? Um diese Fragen zu beantworten, gibt der folgende Beitrag einen Überblick über mögliche Meldepflichten und ihre Folgen für betroffene Unternehmen.

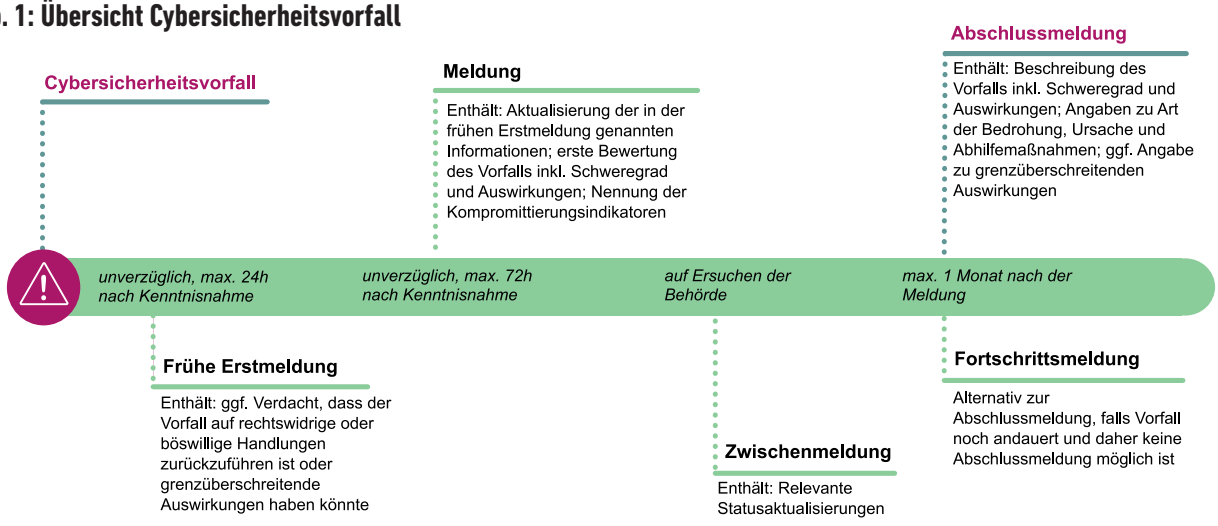
Meldepflichten nach BSI-Gesetz

Nach aktueller Rechtslage sind Cybersicherheitsanforderungen für Unternehmen insbesondere in dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) geregelt. Dieses enthält die Pflicht zur Meldung bestimmter, besonders risikobehafteter Cybersicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Meldepflicht trifft Unternehmen, die in bestimmten Bereichen tätig sind: So sind gerade Betreiber sogenannter kritischer Infrastrukturen erfasst, d.h. Betreiber besonders versorgungskritischer Einrichtungen in den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie künftig Abfallentsorgung. Zudem sind Unternehmen im besonderen öffentlichen Interesse betroffen, die sich durch eine herausragende Bedeutung für die staatliche Sicherheit oder Volkswirtschaft auszeichnen. Hinzu tritt eine Meldepflicht für Anbieter digitaler Dienste – etwa Suchmaschinen oder Onlinemarktplätze – bei Vorfällen, die erhebliche Auswirkungen auf die Bereitstellung des digitalen Dienstes haben.

Ausweitung nach NIS2

Diese bislang nur punktuellen Meldepflichten erfahren eine erhebliche Ausweitung durch die NIS2-Richtlinie (NIS: „Network and Information Security Directive“), die im Januar 2023 in Kraft getreten ist und bis Oktober 2024 in deutsches Recht umgesetzt werden muss. Anders als die bisherige Regelung betrifft die NIS2-Richtlinie alle mindestens mittelgroßen Unternehmen sowohl in den bereits vom BSI-Gesetz erfassten als auch in neu hinzutretenden Sektoren, darunter z.B. die Verwaltung von IKT-Diensten (Informations- und Kommunikationstechnologien), die Produktion von chemischen Stoffen oder Lebensmitteln, die Herstellung bestimmter Waren und Forschung. Meldepflichten werden unter der NIS2-Richtlinie deshalb künftig deutlich mehr Unternehmen betreffen – darunter auch solche,

Abb. 1: Übersicht Cybersicherheitsvorfall



© Quelle: Linklaters

deren Kerngeschäft nicht im digitalen Bereich liegt.

Infolge der hohen Relevanz der NIS2-Richtlinie lohnt sich ein Blick auf die Eckpunkte der Meldepflicht:

- **Was muss gemeldet werden?** Zu melden ist jeder „erhebliche Sicherheitsvorfall". Ein Vorfall gilt als erheblich, wenn er zum einen schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht oder – zum anderen – andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt.

- **Wie muss die Meldung aussehen?** Die NIS2-Richtlinie sieht – anders als bisher – ein mehrstufiges Meldeverfahren vor (vgl. Abb. 1). Dieses umfasst eine frühe Erstmeldung innerhalb von 24 Stunden nach Kenntnisnahme von dem Sicherheitsvorfall, eine reguläre Meldung innerhalb von 72 Stunden, regelmäßige Zwischenmeldungen auf Ersuchen der zuständigen Behörde sowie eine Abschlussmeldung. Zu den vorgegebenen Mindestinhalten der Meldung gehören etwa Beschreibungen des Vorfalls und seiner Ursachen sowie ein Bericht über getroffene Abhilfemaßnahmen.

- **An wen ist die Meldung zu richten?** Die Meldung ist zu richten an die zuständige Behörde oder an das Computer-Notfallteam (CSIRT). In Deutschland wird dies voraussichtlich weiterhin das BSI sein.

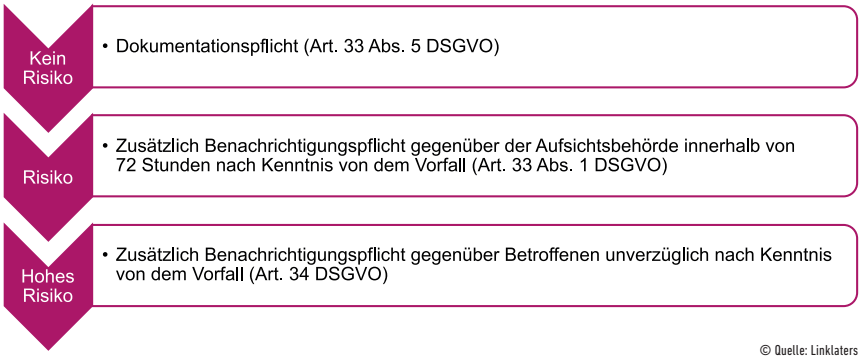
- **Müssen auch Kunden informiert werden?** Sind die Empfänger der Dienste des Unternehmens ebenfalls von einer Cyberbedrohung betroffen, so sieht die NIS2-Richtlinie vor, dass das Unternehmen sie hiervon in Kenntnis setzen muss. Laut ersten Gesetzentwürfen soll das BSI Unternehmen zudem anweisen können, ihre Kunden über einen Cybersicherheitsvorfall zu informieren, wenn der Vorfall die Erbringung von Diensten an die Kunden beeinträchtigt.

- **Ab wann gilt die Meldepflicht?** Es liegt bereits ein Referentenentwurf vor, der die mit der NIS2-Richtlinie einhergehenden Änderungen in das BSI-Gesetz überführen soll. Der Entwurf sieht ein Inkrafttreten am 01.10.2024 vor. Verstöße können dann teuer werden: Die NIS2-Richtlinie sieht Bußgelder von bis zu 7.000.000 Euro oder 1,4% des weltweiten Jahresumsatzes vor; sektorspezifisch sogar bis zu 10.000.000 Euro oder 2% des weltweiten Jahresumsatzes.

Der Klassiker: Meldepflichten nach DSGVO

Neben neu eingeführten Regelungen sollten Unternehmen auch altbekannte Meldepflichten im Blick behalten. Dies betrifft die Meldung von Datenpannen nach der DSGVO, sofern im Rahmen des Cybersicherheitsvorfalls (auch) personenbezogene Daten vernichtet, verändert oder gegenüber Unbefugten offengelegt wurden. Dies kann z.B. der Fall sein, wenn das Unternehmen einer Cyberattacke oder einem Ransomwareangriff zum Opfer gefallen ist. Auch der Einsatz bestimmter Schadsoftware wie etwa Emotet kann im Einzelfall zu einem meldepflichti-

Abb. 2: Meldepflichten nach Risikoabstufung



© Quelle: Linklaters

gen Vorfall führen, wenn diese Malware auf personenbezogene Daten – im Falle von Emotet aus dem Postfach des Betroffenen – zugreift.

Die Meldepflichten nach der DSGVO sind entsprechend dem für Betroffene entstehenden Risiko abgestuft (vgl. Abb. 2): Stellt der Verantwortliche kein aus dem Vorfall resultierendes Risiko für die Rechte und Freiheiten des Betroffenen fest, so treffen ihn lediglich Dokumentationspflichten hinsichtlich des Vorfalls. Besteht ein Risiko, so trifft ihn zusätzlich eine Meldepflicht gegenüber der zuständigen Datenschutzaufsichtsbehörde innerhalb von 72 Stunden nach Kenntnisnahme von dem Vorfall. Wird schließlich ein hohes Risiko für die betroffenen Personen festgestellt, so müssen neben der Aufsichtsbehörde auch die Betroffenen unverzüglich informiert werden.

Bei Nichtbeachtung der Meldepflichten können Bußgelder bis zu einer Höhe von 10.000.000 Euro oder 2% des weltweiten Jahresumsatzes des Unternehmens verhängt werden. Beruht der Cybersicherheitsvorfall zudem auf unzureichenden Maßnahmen zur Gewährleistung der Datensicherheit, so kann auch dieser DSGVO-Verstoß ein Bußgeld nach sich ziehen. Die Bußgeldpraxis zeigt: Eine verspätete oder unvollständige Meldung des Vorfalls kann dann zu einem erhöhten Bußgeld führen.

Bereichsspezifische Meldepflichten

Abhängig von der Art des Cybersicherheitsvorfalls und dem Unternehmenssektor kommen weitere, bereichsspezifische Vorgaben in Betracht. Ein besonderes Augenmerk ist zu richten auf neue oder künftig in Aussicht stehende Meldepflichten. So sollten sich Unternehmen im Finanzsektor auf mehrstufige Meldepflichten nach dem „Digital Operational Resilience Act“ (DORA) einstellen [→ Reul/Mildahn, S. 12], der die bisherigen Pflichten zur Meldung an die Finanzaufsichtsbehörden nach dem Zahlungsdiensteaufsichtsgesetz (ZAG) ablösen wird. Hersteller von vernetzten Produkten sollten den im Gesetzgebungsverfahren befindlichen „Cyber Resilience Act“ im Blick behalten, der in der Entwurfsfassung eine Meldung von ausgenutzten Sicherheitsschwachstellen sowie von Sicherheitsvorfällen, die sich auf die Produktsicherheit auswirken, an die europäische Cybersicherheitsbehörde ENISA sowie an die Produktnutzer vorsieht.

Handlungsempfehlungen

Um ein vollständiges Bild von ihren Meldepflichten im Zusammenhang mit Cybersicherheitsvorfällen zu erhalten, sollten Unternehmen sorgfältig prüfen, welche – bestehenden und künftigen – Rechtsakte auf ihre Tätigkeit Anwendung finden und welche Verpflichtungen diese Rechtsakte vorsehen. Dabei ist stets zu beachten, dass ein Vorfall Meldungen an mehrere bzw. unterschiedliche Behörden erforderlich machen kann. Sind die anwendbaren Meldepflichten identifiziert, so sollte das Unternehmen seine Meldeprozesse hierauf abstimmen. Dazu gehört die Beantwortung der Frage, wer unternehmensintern über den Cybersicherheitsvorfall informiert werden muss und wer für die Meldung an die Behörde zuständig ist: Eine klare Kompetenzverteilung hilft, im Ernstfall zügig handlungsfähig zu sein. Schließlich sollten Meldeprozesse einer regelmäßigen Evaluation unterworfen werden. Im Lichte der stetig zunehmenden Regulierungsdichte im Cybersicherheitsbereich ist dies unentbehrlich, um rechtzeitig auf neue Entwicklungen reagieren zu können. ←

Dr. Daniel A. Pauly
Linklaters LLP,
Frankfurt am Main
Partner, German Head of Technology, Media & Telecommunications
daniel.pauly@linklaters.com
www.linklaters.de

Selma Nabulsi
Linklaters LLP,
Frankfurt am Main
Doktorandin, wissenschaftliche Mitarbeiterin, Technology, Media & Telecommunications
selma.nabulsi@linklaters.com
www.linklaters.de

Rechtlichen Anwendungsbereichen steht eine Vielzahl von Legal-Tech-Lösungen zur Verfügung – die Palette verfügbarer Tools wird weiterwachsen.

Umgang mit Virtual Data im Rahmen rechtlicher Prüfungsprozesse

Legal-Tech-Lösungen als Schlüssel zum Erfolg

Von Dr. Timo Engelhardt, Dr. Ruprecht Freiherr von Maltzahn und Jennifer Klement

Geschwindigkeit und Ausmaß von technologischem Fortschritt und Innovation sind unvermindert hoch. Neu- sowie Fortentwicklungen vor allem in den Bereichen Netzwerktechnologie, Logistik und Mobilität führen zu immer stärkerer wirtschaftlicher, operativer und technologischer Vernetzung und Integration. Umfassende Verfügbarkeit von Informationen, Arbeitskraft und spezialisiertem Know-how wird vorausgesetzt, eingesetzt und geteilt. Durch die fortschreitende Digitalisierung dieser Informationen entstehen große Datenmengen, die es zu beherrschen und sinnvoll einzusetzen gilt.

Auch im rechtlichen Kontext sind Unternehmen darauf angewiesen, große Mengen an Daten schnell und effizient zu verarbeiten und für den jeweiligen Nutzen zugänglich zu machen. Die (externe) Rechtsberatung hat sich darauf eingestellt. Durch die Entwicklung und den Einsatz von Legal-Tech-Lösungen kann der Notwendigkeit des schnellen Datenzugangs und -verarbeitung begegnet werden und so die „Erwartungshaltung“ auf Mandantenseite mittels entsprechender Anwendungen und Tools befriedigt werden. Nachfolgend wird anhand konkreter

Praxisbeispiele aufgezeigt, wie durch den Einsatz von Legal-Tech-Tools rechtliche Prüfprozesse erleichtert und beschleunigt werden können.

Aufarbeitung und Weiterverarbeitung von Daten im Zuge von Transaktionen

Im Transaktionskontext sind oftmals umfangreiche Informationen über die wirtschaftlichen, rechtlichen, steuerlichen und technischen Umstände eines Unternehmens bzw. einer Unternehmensgruppe zu verarbeiten – sei es, um einen Verkaufs- oder Finanzierungsprozess vorzubereiten und die Informationen später möglichen Interessenten/Investoren nach entsprechender Aufbereitung zur Verfügung zu stellen. Auf Investorenseite besteht das Erfordernis, sich ein Bild über das Risikoprofil sowie über die Werthaltigkeit des Investitionsgegenstands zu machen und den gewonnenen Erkenntnissen im weiteren Prozess hinreichend Rechnung zu tragen.

Die relevanten Informationen stehen nicht mehr in Papier-, sondern in digitaler Form in elektronischen („virtuellen") Datenräumen zur Verfügung. So ist der Zugang zu den Informationen heute deutlich erleichtert. Gleichsam ist die umfangreiche Menge der Daten in kurzer Zeit zu bewältigen. Es gilt, diese zügig zu prüfen und die Prüfungsergebnisse entsprechend aufbereitet dem Mandanten bzw. Nutzer zur weiteren Verwendung zu übermitteln. Dieser Prozess erfordert neben einer aufwendigen inhaltlichen und rechtlichen Prüfung der Informationen regelmäßig auch einen großen Koordinations- und Organisationsaufwand, der nur mit erheblichem Ressourcen- und Kosteneinsatz zu bewältigen ist.

Hier setzen Legal-Tech-Lösungen an: So haben sich Anwendungen, wie beispielsweise **Kira**, etabliert, die unter Einsatz von künstlicher Intelligenz (KI) automatisiert Textpassagen, Vertragsklauseln oder andere Schlüsselinformationen in Dokumenten lokalisieren und extrahieren sowie – bei Bedarf – die gewonnen Informationen kategorisieren und gruppieren. So aufbereitet, stehen die Informationen für die (rechtliche) Durchsicht und Analyse innerhalb kurzer Zeit zur Verfügung, ohne dass der/die Einzelne die wesentlichen Informationen mit umfangreichem Zeitaufwand erst herausfiltern muss, bevor mit der rechtlichen Prüfung begonnen wird.

> „Umfassende Verfügbarkeit von Informationen, Arbeitskraft und spezialisiertem Know-how wird vorausgesetzt, eingesetzt und geteilt."

Gerade bei komplexen und/oder internationalen Transaktionen besteht regelmäßig Bedarf an effektivem und effizientem Prozessmanagement, um die vorhandenen Ressourcen im Rahmen der rechtlichen Analyse zielgerichtet einzusetzen. Gleichzeitig gilt es, die Prüfungsergebnisse schnell und für den Empfänger individuell aufbereitet zu übermitteln. HTML-basierte Prozessmanagementplattformen, wie zum Beispiel Linklaters **ReportiQ,** verfolgen einen holistischen Ansatz. Jede Phase des Prüfprozesses, wie Zuteilung von Dokumenten, Q&A-Prozess, Erstellung, Konsolidierung und Nachbereitung von Berichtsinhalten sowie die Erstellung eines finalen Prüfungsberichts/Reports, ist in die Plattform integriert. Dabei ist eine individuelle Anpassung an die Transaktion jederzeit möglich. Dem Mandanten steht ein „Realtime"-Zugriff auf den aktuellen Projektstatus zur Verfügung. Prüfungsergebnisse werden in Echtzeit übermittelt und fließen direkt in den weiteren (Entscheidungs-)Prozess ein. Die Bündelung auf einer Plattform führt zu einer Verringerung und Erleichterung des Koordinations- und Organisationsaufwands, bei gleichzeitig höherer Transparenz.

Schwärzung von sensiblen Daten und Informationen

Aufgrund (datenschutz-)rechtlicher Anforderungen und den damit verbundenen Haftungsrisiken sind regelmäßig Vorkehrungen zu treffen, um die Übermittlung von rechtlich geschützten oder sensiblen Daten und Informationen an Nichtberechtigte zu vermeiden. Oftmals sind die betreffenden Informationen nicht separat verfügbar, sondern Teil eines Datensatzes oder Dokuments, dessen sonstiger Inhalt für den Empfänger von Interesse ist. Probates Mittel ist hier die Vornahme von Schwärzungen, anhand derer nur die Informationen für den Empfänger sichtbar bleiben sollen, die übermittelt werden dürfen oder sollen.

Vor dem Hintergrund der oben geschilderten Datenmengen erfordert dies einen oftmals langwierigen und ressourcenintensiven Prozess. Auch hier haben sich Legal-Tech-Lösun-

gen entwickelt: Mittels KI-basierter Schwärzungsprogramme wie etwa **NAIX** oder integrierter Schwärzungstools von Anbietern elektronischer Datenräume können die zu schwärzenden Daten und (sensiblen) Informationen automatisch erkannt und, nach entsprechender Freigabe, geschwärzt werden. Aufgrund flexibler Nutzungsmöglichkeiten können die zu schwärzenden Informationen individuell bestimmt und angepasst werden. Die Zeitersparnis dieser automatisierten Dokumentenbearbeitung liegt auf der Hand.

Sichtung von Informationen im Rahmen von (internen) Untersuchungen

Gerichts- und Schiedsverfahren sowie interne Untersuchungen erfordern regelmäßig eine detaillierte Offenlegung und Auswertung von Informationen zum Zwecke der Aufklärung und/oder (späteren) Beweiserhebung. Die Nutzung elektronischer Kommunikations- und Dokumentationsformen im Unternehmen hat dabei zu einer signifikanten Steigerung des Umfangs der zu sichtenden Informationen und Dokumente geführt. Gleichzeitig stehen anhand dieser Dokumentationsformen zusätzliche Informationen über den unternehmensinternen Informationsfluss und Bearbeitungsablauf zur Verfügung, also zusätzliche Aussagen über den Kreis und den Grad der involvierten Personen. Die Sichtung dieser umfangreichen Datenmengen und Informationsquellen kann, bei einer manuellen Überprüfung, zeit- und ressourcenaufwendig sein. Auch hier helfen Legal-Tech-Anwendungen:

Durch Einsatz sogenannter eDiscovery-Plattformen, wie beispielsweise **Servient** oder **Relativity**, kann der Sichtungs- und Auswertungsprozess erleichtert und beschleunigt werden. Die Plattformen helfen bei der Dokumentensammlung und -sortierung sowie bei der eigentlichen Untersuchung/Sichtung und Prüfung. Hier unterstützen verfügbare Funktionen wie E-Mail-Threading und Deduplizierung (zur Vermeidung von Dopplungen und Ineffizienzen) sowie Dokumentenkategorisierung. Dabei ist die KI-gestützte Plattform in der Lage, im laufenden Prüfprozess zu „lernen" und somit permanent eine dem Prüfungsauftrag entsprechende Priorisierung und Kategorisierung der verfügbaren Dokumente vorzunehmen. Dies ermöglicht eine zielgerichtete Durchsicht.

> „Die Sichtung dieser umfangreichen Datenmengen und Informationsquellen kann, bei einer manuellen Überprüfung, zeit- und ressourcenaufwendig sein."

Gleichzeitig bieten diese Anwendungen Hilfestellung für eine effiziente(re) Zusammenarbeit zwischen den Beteiligten. So dient die Plattform als zentraler Speicherort für Auswertungsergebnisse, Interviewmitschriften und sonstige Erkenntnisgewinne, die so für alle Beteiligten gleichermaßen und unmittelbar zugängig sind. Die Interaktion zwischen einzelnen Arbeitssträngen wird gefördert. Alle können schnell und unkompliziert an neuen Erkenntnisgewinnen partizipieren und somit bereits frühzeitig die Implementierung von Folgemaßnahmen planen und gegebenenfalls schon umsetzen.

Auch für andere (rechtliche) Anwendungsbereiche steht eine Vielzahl von Legal-Tech-Lösungen zur Verfügung. Die Palette verfügbarer Tools wird weiterwachsen. Ein zielgerichteter Einsatz im Unternehmen und/oder durch externe Berater kann – auf ressourcen- und kostenschonende Weise – in großem Maße zu Effizienzsteigerung und unternehmerischem Erfolg beitragen. ←

Dr. Timo Engelhardt
Linklaters LLP, München
Partner Gesellschaftsrecht/M&A
timo.engelhardt@linklaters.com
www.linklaters.de

Dr. Ruprecht Freiherr von Maltzahn
Linklaters LLP, München
Counsel Gesellschaftsrecht/M&A
ruprecht.von_maltzahn@linklaters.com
www.linklaters.de

Jennifer Klement, LL.M.
Linklaters LLP, München
Product Manager ReportiQ
jennifer.klement@linklaters.com
www.linklaters.de

Linklaters

Alle reden über Transformation treiben wir aktiv voran.

Unser Legal Operations Team gestaltet seit Jahren den Wandel der Rechtsbranche: von schlanken Prozessen über effektiven Ressourceneinsatz bis hin zur Nutzung intelligenter Technologien.

Weitere Informationen finden Sie auf unserer Website.

Value added and delivered.

Linklaters Legal Operations