CHRISTIAN SCHRÖDER / TOBIAS LANTWIN

Cyber-Sicherheitsvorfälle in multinationalen Unternehmen in der EU und den USA

Effektives Krisenmanagement bei transatlantischen IT-Zwischenfällen

Incident Response Management
Meldepflichten
Compliance
Verschwiegenheitsverpflichtung

■ Schnell ist es passiert. Ein Angriff auf die IT-Infrastruktur trifft Unternehmen fast immer zur Unzeit. Hacking und andere Infiltrationen der Unternehmenssysteme können binnen kürzester Zeit erhebliche Schadensketten in Gang setzen und demnach ein sofortiges Eingreifen erforderlich machen. Eine gesteigerte Aufmerksamkeit verlangen IT-Sicherheitsvorfälle besonders in multinationalen EU/US-Konzernstrukturen. In solchen Fällen greifen nicht nur die Regelungen des europäischen und nationalen Datenschutzrechts, auch das häufig mit starken Sanktionsandrohungen versehene US-Recht verlangt Beachtung. Welche Besonderheiten im Ernstfall auf beiden Seiten des Atlantiks zu beachten sind und wie diese in der Praxis sinnvoll und zügig umgesetzt werden können, erläutert der folgende Beitrag.

■ It can happen quickly. An attack on the IT infrastructure almost always hits companies at the wrong time. Hacking and other attacks on company systems can set off considerable chains of damage within a very short time and therefore require immediate intervention. IT security incidents require increased attention, especially in multinational EU/US corporate structures. In such cases, not only do the regulations of European and national data protection law apply, but also US law, which often provides for strong sanction threats, requires attention. The following article explains what special aspects need to be taken into account on both sides of the Atlantic in the event of an emergency and how these can be sensibly and quickly implemented in practice.
Lesedauer: 24 Minuten

I. Typische Cyber-Bedrohungsszenarien für Unternehmen

Die Cyber-Bedrohungslage präsentiert sich angesichts des fortschreitenden Stands der Technik und der beeindruckenden Kreativität gewiefter Angreifer als außerordentlich dynamisch. Stetig werden neue Angriffstaktiken entwickelt und in der Praxis zur Anwendung gebracht – mit teils erheblichen, mitunter existenzbedrohenden Schäden für die betroffenen Unternehmen.[1] Cyber-Angriffe werden inzwischen sogar als Dienstleistung (Ransom-as-a-Service) vermarktet. Neben Betriebsstörungen und -ausfällen sowie Reputationsschäden verursachen Cyber-Angriffe in der Regel vor allem enorme Kosten, sei es durch die erforderlichen Maßnahmen zur Aufklärung und Wiederherstellung der Betriebsbereitschaft oder durch den irreversiblen Verlust finanzieller Mittel durch Kontoplünderungen.[2]

Daneben besteht ungeachtet des US-Rechts selbst nach EU-Recht ein erhebliches Risiko von Bußgeldern nach Art. 83 DS-GVO und möglichen Schadensersatzklagen nach Art. 82 DS-GVO zahlreicher Betroffener wegen festgestellten Mängeln in der Datenschutz-Compliance oder der Verletzung von Meldepflichten. Der gesamtwirtschaftliche Schaden durch Angriffe auf Unternehmen beträgt daher allein in Deutschland jährlich mehr als 220 Mrd. EUR, was einer Verdoppelung seit 2018/19 entspricht.[3] Phishing, Ransomware, DDoS – die Angriffsmethoden tragen viele Namen. Zum besseren Verständnis sollen daher die in den letzten Jahren am häufigsten auftretenden Angriffsvarianten in einem kurzen Überblick erläutert werden.

1. Phishing

Das sog. Phishing ist als eine Form des Social Engineering eine seit Jahrzehnten bekannte und gängige Angriffsart, in der durch gefälschte E-Mails, Kurznachrichten oder Websites versucht wird, vertrauliche Daten wie Passwörter oder PIN-Codes abzugreifen.[4] Opfer von Phishing-Attacken werden häufig dazu verleitet, auf Links in E-Mails zu klicken und ihre persönlichen Daten auf präparierten Websites einzugeben, die mit ihrem Erscheinungsbild für das Opfer bekannte Websites nachahmen.

Die hierdurch erlangten Daten werden dann u.a. für einen Identitätsdiebstahl verwendet, um z.B. Zugang zu vertraulichen Dokumenten zu erlangen oder auf Bankkonten zuzugreifen. Das Phishing ist eine Konstante in der Cyber-Bedrohungslandschaft und bildet seit vielen Jahren regelmäßig den Stein des Anstoßes für koordinierte Angriffsserien.[5] Allein für das Jahr 2020 zählte das *FBI* für Phishing-Attacken 241.342 Betroffene,[6] womit sich diese Zahl seit dem Jahr 2019 (114.702 Betroffene) mehr als verdoppelt hat.[7]

2. Malware

Nicht weniger häufig sind Cyber-Angriffe durch gezielte Infiltration von IT-Systemen durch Malware, welche vor allem Angriffe durch Trojaner, Viren, Würmer, Spyware und andere Schadsoftware umfassen. Allein 53% der Angriffsfälle auf Unternehmen in Deutschland im Jahr 2018 waren Malware-Infektionen.[8] Diese Schadprogramme, die zum Ausspähen der Systeme oder zur Kontrollübernahme oder Behinderung betriebsrelevanter Systemabläufe eingesetzt werden, finden ihre Verbreitung in der

1 Einen Überblick über die aktuelle Bedrohungslage geben die Cyber-Sicherheitsberichte des Unternehmens *FireEye, Inc.,* M-Trends 2021, abrufbar unter: bit.ly/2TcS8AV, sowie des *Internet Crime Complaint Center* des *FBI*, 2020 Internet Crime Report, abrufbar unter: bit.ly/3w1FtOC, und der *Allianz für Sicherheit des BSI,* Cyber-Sicherheits-Umfrage – Cyber-Risiken & Schutzmaßnahmen im Unternehmen Betrachtungszeitraum 2018, v. 18.4.2019, abrufbar unter: bit.ly/3nPGeKg.
2 Vgl. zur *Allianz für Cyber-Sicherheit* (o. Fußn. 1), S. 13; im Jahr 2018 beklagten 87% der betroffenen Unternehmen Betriebsstörungen, 65% hatten zusätzliche Kosten zu tragen und 22% erlitten Reputationsschäden.
3 *Bitkom,* PM v. 5.8.2021: Angriffsziel deutsche Wirtschaft: mehr als 220 Milliarden Euro Schaden pro Jahr, abrufbar unter: bit.ly/3lR0gD1.
4 Näher zu den verschiedenen Formen des Phishing *Schmidt/Fischer,* CB 2020, 200 f.; getarnt werden die Mails häufig auch als vermeintlich verschlüsselte Mitteilungen der Bankinstitute oder IT-Dienstleister des Opfers oder als firmeninterne Nachrichten etwa der HR-Abteilung, zu deren Ansicht die Eingabe der Kennwortdaten erbeten wird.
5 *FireEye, Inc.* (o. Fußn. 1), S. 5.
6 *Internet Crime Complaint Center* (o. Fußn. 1), S. 19.
7 S. dazu den Report für das Jahr 2019: *Internet Crime Complaint Center,* 2019 Internet Crime Report, abrufbar unter: bit.ly/3nPKNny, p. 19.
8 *Allianz für Cyber-Sicherheit* (o. Fußn. 1), S. 12.

weit überwiegenden Zahl der Fälle als Anhang oder Link einer E-Mail und werden oft auch mit Phishing-Attacken und -Folgeattacken kombiniert.[9] Im Frühjahr 2021 machte z.B. der Banking-Trojaner „FluBot" Schlagzeilen, der, als Nachricht eines Paketdienstleisters getarnt, im Wege des SMS-Phishing größere Verbreitung fand.[10]

Eine in der Unternehmenspraxis häufig anzutreffende Angriffstaktik betrifft Fälle, in denen eine nicht aktivierte Zweifaktorauthentifizierung bei Office- und Mail-Programmen ausgenutzt wird. Zu diesem Zweck wird eine Mail an die Mitarbeiter*innen des Unternehmens verfasst, die sich als Bitte etwa der IT-Abteilung um erneute Bestätigung der Zugangsdaten durch Eingabe der Daten in eine Phishing-Eingabemaske tarnt. Werden die Zugangsdaten durch einen der Mitarbeiter übermittelt, können die Cyber-Kriminellen wegen des Fehlens zusätzlicher Authentifizierungsfaktoren unmittelbar Zugriff auf weitere, unternehmensinterne Daten nehmen.

Mit den Hintergrundinformationen aus diesen Dateien sind die Täter*innen dann in der Lage, noch authentischere Phishing-Folgemails zu verfassen und so häufig erst den eigentlichen Angriff auf Know-how oder andere Vermögenswerte zu starten. Auch abseits des Phishing erweist sich die Malware-Angriffslage als hochdynamisch, waren schließlich allein 2020 nach einer Studie des Cybersecurity-Unternehmens *FireEye* mehr als 500 der entdeckten Malware-Familien völlig neu und bis dato unbekannt.[11]

3. Ransomware

Ein insbesondere seit den letzten Jahren auftretendes Phänomen betrifft sog. Ransomware-Attacken, denen spätestens durch den großangelegten, weltweiten Cyber-Angriff mit dem Erpressungstrojaner „WannaCry" im Mai 2017 größere mediale Beachtung zuteilwurde.[12] Auch die Angriffe auf die *Colonial Pipeline* im Mai 2021[13] und die *Funke-Mediengruppe* im Dezember 2020[14] sind jüngere Beispiele für „erfolgreiche" Ransomware-Angriffe.

Wird ein System durch einen Ransomware-Angriff infiltriert, beschränkt oder verhindert die Schadsoftware den Zugriff auf Daten und Systeme durch Verschlüsselung bestimmter Nutzerdateien, woraufhin dann in der Regel auf einem Sperrbildschirm für die Freigabe der Dateien die Zahlung eines Lösegelds – meist in Form von Kryptowährungen wie Bitcoin – verlangt wird.[15]

Derartige Schadsoftware findet ihren Weg auf Unternehmensserver oft über Phishing-Mails oder Sicherheitslücken in veralteter oder unzureichend gepatchter Software.[16] Nicht zuletzt die wachsende Bedeutung von Ransomware als Nebeneinnahmequelle von Cyber-Kriminellen oder ganzen Staaten führt zu einer rasant wachsenden Zahl an Ransomware-Angriffen.[17] So haben sich die durch Ransomware jährlich verursachten Schäden in Deutschland seit 2018/19 mehr als vervierfacht.[18]

4. DDoS-Angriffe

Bei einer sog. Distributed-Denial-of-Service(DDoS)-Attacke wird mit einer Vielzahl von gezielten Zugriffen von verschiedenen Rechnern auf einen Internetdienst versucht, diesen durch Überlastung des Datennetzes zum Zusammenbruch zu bringen oder zumindest dessen Verfügbarkeit und Reaktionsgeschwindigkeit erheblich zu behindern.[19] Ein gezielter Angriff etwa auf ein cloudbasiertes Dateisystem des Unternehmens kann so die Betriebsfähigkeit ganz erheblich beeinträchtigen oder gar zum Erliegen bringen. Mit mehr als 10 Mio. registrierten DDoS-Attacken im Jahr 2020 und einer stetig steigenden Tendenz werden DDoS-Angriffe zudem immer häufiger und aggressiver.[20]

5. APT-Angriffe

Mit Advanced-Persistent-Threat(APT)-Angriffen versuchen Angreifer durch komplexe, meist sehr zeitintensive und aufwändige Angriffe auf ein oder wenige Opfer, tief und zielgerichtet in die Infrastruktur eines angegriffenen Unternehmens einzudringen.[21] Das Ziel dieser Attacken ist in der Regel das langfristige Ausspähen vertraulicher Informationen und Passwörter, was regelmäßig durch eine Reihe unentdeckter Angriffe erreicht wird, die eine stabile Verbindung zwischen den infiltrierten Systemen und den Täter*innen aufrechthalten.

Auch diese Attacken beginnen häufig mit einer Kombination aus Phishing- und Malware-Angriffen und werden nicht selten als Mittel der Industriespionage durch Staaten betrieben. Ein jüngeres Beispiel für diese Spielart von Cyber-Angriffen bildet der *SolarWinds*-Spionageangriff, bei dem russische Angreifer über mehr als ein halbes Jahr Zugriff auf sensible Daten von 200 staatlichen Institutionen und Unternehmen hatten.[22]

II. Schritte zur Koordinierung eines Incident Response Management

Ein gut durchdachtes Incident Response Management[23] kann maßgeblich dazu beitragen, dass Unternehmen bei einem Cyber-Sicherheitsvorfall nicht auf dem falschen Fuß erwischt werden. So kann das Schadensausmaß begrenzt und die Handlungsbereitschaft des betroffenen Unternehmens rasch wiederhergestellt werden. Sinnvoll ist es, derartige Überlegungen bereits frühzeitig und noch vor dem ersten Vorfall in Angriff zu nehmen.

Wie Erwägungsgrund 87 DS-GVO zudem klarstellt, soll der Verantwortliche stets in der Lage sein, sofort feststellen zu können, ob eine Datenschutzverletzung vorliegt, um einer umgehenden Meldung an die Aufsichtsbehörden und die betroffenen Personen nachkommen zu können, soweit diese erforderlich ist.[24] Dies setzt voraus, dass der Verantwortliche eine genaue und konkrete Kenntnis von seinen Datenbeständen hat (Prinzip: „Know your data").

Die Erfahrung zeigt, dass viele Unternehmen sich nicht hinreichend darüber im Klaren sind, welche Daten sie im Einzelnen überhaupt Vorhalten. Ein vollständiges Data Mapping ist jedoch

---

9 Vgl. *Allianz für Cybersicherheit* (o. Fußn. 1), S. 12; allein 90% der Schadprogramme wurden als Anhang oder Link in einer E-Mail versendet.
10 S. SPIEGEL Online, v. 23.4.2021, abrufbar unter: bit.ly/3jm44uX; häufig wurden die Betroffenen sogar mit ihrem Namen adressiert.
11 *FireEye, Inc.* (o. Fußn. 1), S. 21.
12 S. etwa SPIEGEL Online, v. 13.5.2017, abrufbar unter: bit.ly/36CrMKV.
13 BBC v. 10.5.2021, abrufbar unter: bbc.in/3w3uV1x.
14 FAZ v. 21.1.2021, abrufbar unter: bit.ly/3A6PKfO.
15 *BSI*, Cyber-Glossar, Stichwort „Ransomware", abrufbar unter: bit.ly/3Ex4Ddt.
16 Vgl. zuletzt etwa den Ransomware-Angriff auf das *Uniklinikum Düsseldorf*, dessen Server über eine Sicherheitslücke einer Remote-Working-VPN-Software mit einem Ransomware-Schadprogramm infiltriert wurden, wobei der Systemausfall zum Tod einer Patientin geführt hatte; *Schmidt,* Cyber-Angriff auf Uniklinik Düsseldorf: #Shitrix schlug zu, heise.de, abrufbar unter: bit.ly/3ndRWdq.
17 *FireEye, Inc.,* M-Trends 2020, S. 35, abrufbar unter: bit.ly/3x1fZSI.
18 *Bitkom* (o. Fußn. 3).
19 *World Wide Web Consortium,* The World Wide Web Security FAQ: Securing against Denial of Service attacks, abrufbar unter: bit.ly/3b5rnoq.
20 *Netscout Systems, Inc.,* Netscout Threat Intelligence Report, Issue 6: Findings from 2H 2020, abrufbar unter: bit.ly/3jkuHAn.
21 *Maloney,* What is an Advanced Persistent Threat (APT)?, Cybereason, v. 9.1.2018, abrufbar unter: bit.ly/3hIPQ4w.
22 Bloomberg v. 19.12.2020, abrufbar unter: bloom.bg/3x1SVDj.
23 Die Entwicklung solcher IT-Incident-Response-Pläne sind z.B. auch als Teil des internationalen Informationssicherheitsstandards ISO 27001 und des Business Continuity Standards ISO 22301 vorgesehen.
24 Dazu auch *Art. 29-Datenschutzgruppe,* Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung 2016/679, WP250rev.01, 3.10.2017 i.d.F. v. 6.2.2018, S. 10 f.; *Reif,* in: Gola, DS-GVO, 2. Aufl. 2018, Art. 33 Rn. 42.

nicht nur Bestandteil des datenschutzrechtlichen Compliance-Pflichtenkatalogs, sondern auch aus Cyber-Sicherheitsperspektive von entscheidender Bedeutung. Zudem muss der Verantwortliche nach Art. 32 Abs. 1 DS-GVO geeignete technische und organisatorische Maßnahmen treffen, um ein angemessenes Datenschutzniveau bei der Verarbeitung personenbezogener Daten zu gewährleisten.

Ein guter Incident-Response-Management-Plan hat daher für jeden Schritt eines Sicherheitsvorfalls die geeigneten Maßnahmen bereits definiert:

1. Anfangsphase: Ordnung in der Unordnung

Zu Beginn eines Incident Response Management steht die Identifizierung des IT-Sicherheitsvorfalls und der diesen ggf. verursachenden infrastrukturellen Schwachstelle. Besonders in der Anfangsphase ist die Lage oft undurchsichtig und sehr dynamisch, gleichwohl ist schon in den ersten Stunden die schnelle Ergreifung von Gegenmaßnahmen erforderlich, um Sicherheitslücken zu schließen und die weitere Schadensentwicklung unter Kontrolle zu bringen.

a) Feststellungen zu Art und Ausmaß der Angriffslage

Um die Reichweite des Zwischenfalls festzustellen, sollte umgehend der Kontakt mit einem in IT-Sicherheitsvorfällen versierten Team aus IT-Forensiker*innen und auf IT-Zwischenfälle spezialisierten Rechtsanwält*innen aufgenommen werden. Aufgabe des IT-Forensikers ist festzustellen, welche Form eines Angriffs vorliegt, ob dieser noch stattfindet, welche Dateien und Systeme betroffen sind und welche Motive der Angreifer haben könnte, um so das weitere Vorgehen planbar zu machen. Die IT-Forensiker*innen werden nach einer ersten Analyse gezielte Maßnahmen empfehlen, die weiteren Schaden minimieren.

Steht z.B. fest, dass ein unbefugter Zugriff auf die Unternehmenssysteme stattgefunden hat, sind in der Regel unverzüglich neue Passwörter zu vergeben. Eine weitere mögliche Maßnahme stellt etwa das Einrichten einer Zwei- oder Multifaktorauthentifizierung mit Zugriffsüberwachung dar. Wurden E-Mail-Accounts kompromittiert, sollten zudem neue E-Mail-Adressen generiert werden, um die Mitarbeiter*innen möglichst rasch wieder arbeitsfähig zu machen und so die Fortsetzung der normalen Arbeitsabläufe im Unternehmen so weit wie möglich zu gewährleisten.

Vor abschließender Klärung der Reichweite des Zugriffs dürfen Systeme jedoch häufig nicht mehr operativ genutzt werden. Mit Hilfe von Monitoring-Systemen können zudem etwaige Schwachstellen in den Systemen aufgedeckt und zügig neutralisiert werden, um weiteren Schäden vorzubeugen. Da bereits bei diesen ersten Schritten sehr viel falsch gemacht werden kann, sollten Unternehmen, die nicht über spezielle Cyber-Teams verfügen, keinesfalls selbst Maßnahmen treffen. Verfügen Unternehmen nicht bereits über entsprechende Kontakte zu den Spezialist*innen, vergeht in der Regel (zu) viel Zeit. Unternehmen sollten daher frühzeitig mit entsprechenden Fachleuten Kontakt aufnehmen, um so sicherzustellen, dass im Fall eines Falles ausgewiesene Expert*innen zu vertretbaren Kosten zur Verfügung stehen.

b) Geordnete Kommunikation und Dokumentation

Eine koordinierte, effiziente Kommunikation zwischen allen Entscheidungsebenen ist Grundvoraussetzung für ein Gelingen jeglicher Bemühungen der Schadensbegrenzung. Daher sind die Geschäftsleitung sowie alle weiteren Entscheidungsträger*innen des Unternehmens so früh wie möglich über den Zwischenfall in Kenntnis zu setzen. Schließlich sollten sämtliche Entwicklungen während der Aufklärung des Sachverhalts sowie alle ergriffenen Gegenmaßnahmen stets minuziös mit datierten Einträgen i.S.e. chronologischen Logbuchs dokumentiert werden. Nicht nur kann dadurch ein besserer Überblick über die Situation gewahrt werden, auch lassen sich eigene Haftungsrisiken der Unternehmen so in vielen Fällen erheblich verringern.

c) Kooperation mit Behörden und anderen zentralen Stellen

Frühzeitig sollte auch über die Einbindung staatlicher Stellen wie Datenschutzaufsichtsbehörden, soweit erforderlich auch Strafverfolgungsbehörden, nachgedacht werden. Dabei ist jedoch zu bedenken, dass sich die Interessen des betroffenen Unternehmens und der zu kontaktierenden Behörden nicht zwingend im Gleichlauf bewegen. Steht etwa statt einer unverzüglichen Strafverfolgung eher die weitere Minimierung von Cyber-Risiken oder die zügige Wiedererreichung einer Handlungsbereitschaft für das Unternehmen stärker im Mittelpunkt seines Interesses, mag es zunächst sinnvoller sein, die wenige wertvolle Zeit auf die zügige Einbindung entsprechender IT-Forensik-Dienstleister zu verwenden und die meist recht zeitintensive Strafverfolgung durch spezialisierte Cybercrime-Units erst zu einem späteren Zeitpunkt in den Blick zu nehmen.

Der IT-Forensiker kann und sollte jedoch zur Erstellung von Kopien der relevanten betroffenen Dokumente angehalten werden, um spätere Ermittlungsarbeiten zu unterstützen. Wenn Strafverfolgungsbehörden eingeschaltet werden, sollte zudem gerade in frühen Stadien der Ermittlungen davon abgesehen werden, bereits voreilig eine Fülle an Strafanzeigen zu stellen, um Zuständigkeitskonflikte zu vermeiden und eine zielgerichtete Ermittlungsarbeit hierdurch nicht zu gefährden. Vielmehr sollte zunächst der Vorfall in Gänze aufgearbeitet werden, damit Strafanzeigen im Anschluss daran gezielt und in angemessenem Umfang gestellt werden können (zu den Meldepflichten nach der DS-GVO, s. unter III.).

d) Im Einzelfall: Unverzügliche Kontaktierung von Schlüsselinstitutionen

Um unautorisierte Zahlungen und Geldabflüsse in das außereuropäische Ausland, wie sie bei Phishing-Attacken keine Seltenheit sind, schnell und effektiv zu unterbinden und ggf. weitere Überweisungsketten noch zu unterbrechen, sind ggf. auch die Bank- und Kreditinstitute des Unternehmens unverzüglich zu kontaktieren.[25] In Absprache mit den Bankinstituten sollten zusätzliche Autorisierungsverfahren eingeführt oder ggf. auch Konten eingefroren werden. Zudem sollte, sofern eine solche Versicherung abgeschlossen wurde, ein etwaiger Cyber-Versicherer kontaktiert werden.

2. Vertiefte Ermittlungsphase: Beginn der Schadensbegrenzung und -behebung

Sind diese ersten Schritte zur Aufklärung des Vorfalls und zur Ausschaltung laufender Risikofaktoren vollzogen, kann der Fokus der Bemühungen auf die weitere Schadensbegrenzung und eine detailliertere Sachverhaltsermittlung gerichtet werden. Sobald der Bericht des IT-Forensikers vorliegt, sollten die von dem Sicherheitsvorfall erfassten Dokumente gesichtet werden, um festzustellen, welche personenbezogenen Daten von der Datenschutzverletzung betroffen sind. Vor jeder Durchsuchung sollten jedoch entweder innerbetriebliche oder externe Datenschutzexpert*innen hinzugezogen werden.

In dieser Phase der Ermittlungen ist häufig auch der geeignete Zeitpunkt erreicht, die Mitarbeiter*innen über den Vorfall in

25 *Schmidt/Fischer,* CB 2020, 200 (203).

Kenntnis zu setzen und durch Kommunikationsrichtlinien darüber einzuweisen, wie der Zwischenfall innerhalb und außerhalb des Unternehmens kommuniziert werden soll. Dadurch lassen sich weitere Risiken, etwa durch unkontrolliert nach außen geratende Informationen, eindämmen. Bei größeren Vorfällen dürfte einer solchen innerbetrieblichen Information eine Abstimmung mit Kommunikationsexpert*innen und ggf. auch mit zuständigen Aufsichtsbehörden vorangehen.

III. Rechtliche Anforderungen auf beiden Seiten des Atlantiks

Tritt ein Cyber-Sicherheitsvorfall in einem multinationalen Konzern ein, der nicht nur in Europa, sondern auch in den USA operiert, sind neben den o.g. praktischen Handlungsschritten auch einige rechtliche Besonderheiten auf beiden Seiten des Atlantiks zu beachten. Im Vordergrund stehen dabei verschiedene datenschutzrechtliche Meldepflichten, die für den Fall greifen, dass der Sicherheitsvorfall zu einer Verletzung des Schutzes personenbezogener Daten führt. Daneben können sich im Einzelfall aber auch spezialgesetzliche oder vertragliche Notifizierungspflichten, etwa aus einer Geheimhaltungsvereinbarung, ergeben.

1. Rechtliche Vorgaben in der EU

a) Meldeverpflichtung nach Art. 33, 34 DS-GVO

Auf europäischer Seite ist eine hohe Priorität vor allem der unverzüglichen Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und die Betroffenen nach den Art. 33 und 34 DS-GVO beizumessen, wenn das betroffene Unternehmen seine Niederlassung in der EU hat oder personenbezogene Daten von in der EU befindlichen Personen verarbeitet.[26] Ein Verstoß gegen diese Meldepflichten kann ein Bußgeld von bis zu 10 Mio. EUR oder bis zu 2% des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs nach sich ziehen. Diese Verpflichtung greift, wenn der IT-Sicherheitsvorfall zugleich auch zu einer Verletzung des Schutzes personenbezogener Daten führt.

Eine solche Datenschutzverletzung definiert Art. 4 Nr. 12 DS-GVO als eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Werden personenbezogene Daten bei einem Hackerangriff unbefugt kopiert, eingesehen oder in sonstiger Weise dem Zugriff Fremder ausgesetzt, liegt darin regelmäßig ein typischer Fall einer Datenschutzverletzung i.S.v. Art. 4 Nr. 12 DS-GVO.[27]

Auch der Verlust der Kontrolle und Verfügbarkeit über personenbezogene Daten, etwa auf Grund einer Verschlüsselung durch Ransomware, stellt eine entsprechende Verletzung dar, wenn kein Backup vorliegt.[28] Dabei besteht oft das Problem, dass das Aufspielen von Backups erhebliche Zeit in Anspruch nehmen kann oder auch das Risiko besteht, dass bereits die Backups selbst von einer möglichen Infizierung betroffen sind. Doch auch eine bloß vorübergehende Beeinträchtigung der Verfügbarkeit kann meldepflichtig sein, wenn sie von längerer Dauer ist.[29]

Die Meldung an die Aufsichtsbehörde hat unverzüglich, möglichst innerhalb von 72 Stunden zu erfolgen, nachdem dem Verantwortlichen die Verletzung bekannt wurde. Die Fristberechnung richtet sich nach Art. 3 Fristen-VO und beginnt mit der nächsten vollen Stunde nach dem Zeitpunkt, an dem eine erste Aufklärung der Sachlage meldepflichtige Umstände erkennen lässt.[30] Eine Verzögerung ist nach Art. 33 Abs. 1 S. 2 DS-GVO begründungsbedürftig. Ebenso zeitnah, wenngleich ohne 72-Stunden-Begrenzung, hat die Meldung an die Betroffenen in klarer und einfacher Sprache zu erfolgen, sofern die Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge hat.

b) Sorgfältige Prüfung der Erforderlichkeit einer Meldung

Dennoch sollte vor einer Meldung stets sorgfältig geprüft werden, ob eine Meldung nach der DS-GVO überhaupt erforderlich ist. So ist eine Meldung nach Art. 33 Abs. 1 S. 1 Hs. 2 DS-GVO nicht erforderlich, wenn der Sicherheitsvorfall voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.[31] So ist etwa der unbefugte Zugriff auf Dokumente, die nur einigermaßen unbedeutende Details enthalten, z.B. Anwesenheitslisten von Meetings, Organigramme und Aufgabenverteilungspläne etc., wohl regelmäßig nicht mit einem Risiko für die Rechte und Freiheiten natürlicher Personen verbunden.

Eine Meldung ist mithin nicht bei jedem IT-Zwischenfall zwingend erforderlich, sondern hängt ganz maßgeblich davon ab, welche Daten von dem Zwischenfall überhaupt betroffen sind. Auch die Meldung an die betroffenen Personen ist in gewissen Konstellationen nach Art. 34 Abs. 3 DS-GVO entbehrlich.

Ist eine Meldung nach dem Gesetz nicht erforderlich, sollte das Absetzen einer überobligatorischen Meldung nur wohlüberlegt erfolgen. I.Ü. aber bringt eine nicht erforderliche Meldung nicht nur keinerlei Mehrwert. Sie birgt vielmehr auch das Risiko unerwünschter, nachteiliger Konsequenzen für den Verantwortlichen und kann im schlechtesten Fall eine ungewollte Aufmerksamkeit der Aufsichtsbehörden erzeugen, die mögliche Folgeuntersuchungen in die allgemeine Datenschutz-Compliance des Unternehmens nach sich ziehen kann.

In Strafverfahren dürfen auf Grund einer Meldung erhaltene Informationen gem. § 42 Abs. 4 BDSG allerdings nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden gegen diese verwertet werden.

c) Inhalt der Erstmeldung

Ist eine Meldung erforderlich, stellt sich regelmäßig die Frage, welchen inhaltlichen Umfang die Erstmeldung einnehmen soll. Da die Sachlage innerhalb der ersten 72 Stunden selten vollständig aufgeklärt ist, empfiehlt es sich, in einer Erstmeldung zunächst nur den Umstand einer Datenschutzverletzung und den aktuell verfügbaren Kenntnisstand mitzuteilen.[32]

Die durch Art. 33 Abs. 4 DS-GVO eingeräumte Möglichkeit einer schrittweisen Bereitstellung verschafft hierbei zusätzliche Zeit zu einer umfassenden Aufklärung der Faktenlage.[33] Diese

26 Vertiefender zu den Anforderungen an eine Meldung nach Art. 33, 34 DS-GVO: *EDSA,* Guidelines 01/2021 on Examples regarding Data Breach Notification, 14.1.2021, Version 1.0; *Art. 29-Datenschutzgruppe* (o. Fußn. 24); *BayLfD,* Orientierungshilfe Meldepflichten und Benachrichtigungspflichten des Verantwortlichen, Version 1.1, 2019, abrufbar unter: bit.ly/2MyUoPl; *Paal,* ZD 2020, 119; *Becker,* ZD 2020, 175.

27 *Art. 29-Datenschutzgruppe* (o. Fußn. 24), S. 9 f., 37; *Mantz,* in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 4 Nr. 180; *Jandt,* in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 12 Rn. 8 f.

28 *EDSA* (o. Fußn. 26), Rn. 26 ff.; *Dix,* in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 12 Rn. 7.

29 *BayLfD* (o. Fußn. 26), S. 17 Rn. 12; *HmbBfDI,* Data-Breach-Meldungen nach Art. 33 DSGVO, S. 2, abrufbar unter: bit.ly/3b8NJFQ.

30 *BayLfD* (o. Fußn. 26), S. 38 f. Rn. 76 ff. mit Berechnungsbeispielen.

31 Zahlreiche Beispiele für derartige Fälle finden sich in: *EDSA* (o. Fußn. 26), Rn. 18 ff., 56 ff., 78 ff., 88 ff., 107 ff., 114 ff.

32 *Art. 29-Datenschutzgruppe* (o. Fußn. 24), S. 17.

33 Die *Art. 29-Datenschutzgruppe* hält dies insb. in komplexen Cyber-Sicherheitsvorfällen für praktikabel, *Art. 29-Datenschutzgruppe* (o. Fußn. 24), S. 17 f.

schrittweise Meldung verlangt dabei auch nicht zwangsläufig eine tagesaktuelle Folgemeldung an die Aufsichtsbehörde über die jeweils neuesten Erkenntnisse.

Vielmehr sollte der Aufsichtsbehörde zu einem späteren Zeitpunkt ein abgerundetes, vollständiges Bild zu einer umfassenden Beurteilung geliefert werden. Dabei kann sich eine minuziöse Dokumentation sämtlicher Entwicklungen als entscheidender Vorteil erweisen, zumal der Verantwortliche nach Art. 33 Abs. 5 DS-GVO ohnehin sämtliche Verletzungen sowie die damit in Zusammenhang stehenden Fakten für die Aufsichtsbehörde zu dokumentieren hat. Auch in den Fällen, in denen das Absetzen einer Meldung i.E. für nicht erforderlich gehalten wird, sollten die zu dieser Entscheidung führenden Gründe unbedingt hinreichend dokumentiert werden.

Bei der Formulierung der Meldungen sowohl an die Aufsichtsbehörde als auch an die Betroffenen ist die Unterstützung durch in Datenschutzverletzungsverfahren erfahrene Rechtsanwält*innen anzuraten, um zusätzliche Haftungsrisiken durch undeutlich formulierte oder inhaltlich überschießende Meldungen auszuschalten.[34]

d) Risiko – Auskunftsansprüche von Betroffenen

Im Fall einer Datenschutzverletzung kann es nicht selten dazu kommen, dass Betroffene versuchen, von ihrem Recht auf Auskunft aus Art. 15 Abs. 1 DS-GVO Gebrauch zu machen. Dabei stellt sich die Frage, ob auf diesem Wege auch Informationen zu den Einzelheiten des IT-Zwischenfalls an Betroffene herausgegeben werden müssen und ob und ggf. wie diese Ansprüche abgewehrt werden können. Hilfreich kann hier der frühzeitige und umfassende Einsatz von Rechtsanwält*innen sein. Möglicherweise kann ein Ausschluss des Auskunftsrechts nach § 29 Abs. 1 S. 2 BDSG mit Verweis auf eine sonst drohende Offenbarung von Informationen begründet werden, die dem anwaltlichen Berufsgeheimnis unterfallen.

Werden die Informationen zu dem Sicherheitsvorfall durch den IT-Forensiker im Auftrag des mandatierten Rechtsanwalts gesammelt und aufbereitet, unterfallen diese dem anwaltlichen Berufsgeheimnis. Mit ähnlichen Erwägungen kann ggf. auch eine Information der Betroffenen gem. Art. 13, 14 DS-GVO nach § 29 Abs. 1 S. 1, Abs. 2 BDSG sowie eine Benachrichtigung gem. Art. 34 DS-GVO nach § 29 Abs. 1 S. 3 BDSG ausgeschlossen sein oder zumindest temporär zurückweisbar sein.

2. Rechtliche Vorgaben in den USA

Auch auf der anderen Seite des Atlantiks existiert eine Fülle an Vorgaben, welche im Falle eines IT-Sicherheitsvorfalls Beachtung verlangen. Zwar verfügen die USA bislang noch nicht über ein einheitliches bundesweit geltendes Regelungsregime im Datenschutzrecht, doch haben einige US-Staaten eigene Gesetze erlassen, die neben vielfältigen Verpflichtungen häufig auch durch Verbraucher*innen einklagbare Rechte auf Schadensersatz enthalten.

a) Data Breach Notification Statutes

So haben sämtliche Staaten der USA[35] sog. State Data Breach Laws[36] erlassen, die unter im Einzelnen unterschiedlichen Voraussetzungen eigene Meldepflichten auslösen. Im Gegensatz zur EU liegt der Fokus in den US-amerikanischen Staaten auf der Meldung gegenüber den Betroffenen, während Meldeverpflichtungen gegenüber öffentlichen Stellen in einigen Staaten teilweise erst ab einer gewissen Anzahl von Betroffenen ausgelöst werden.[37]

Im Staat Kalifornien besteht z.B. eine Meldeverpflichtung, wenn ein unbefugter Zugriff auf „computerisierte", d.h. in einem elektronischen Format gespeicherte persönliche Daten[38] kalifornischer Einwohner*innen erfolgt ist, der die Sicherheit, Integrität oder Vertraulichkeit dieser Daten beeinträchtigt, oder es einen begründeten Verdacht für einen solchen Zugriff gibt.[39] Verschlüsselte Daten sind regelmäßig von der Regelung ausgenommen, soweit nicht der zugehörige Schlüssel ebenfalls kompromittiert ist. Die Meldeverpflichtung gilt für Personen und Unternehmen, die in Kalifornien geschäftlich tätig sind und computerisierte Daten vorhalten oder lizenzieren. Die Meldung hat in einem angemessenen Zeitraum zu erfolgen und darf nicht unangemessen verzögert werden.

Werden Meldeverpflichtungen nicht erfüllt, kann dies in einigen Staaten Schadensersatzpflichten gegenüber Betroffenen oder Klage- und Anordnungsbefugnisse des jeweiligen „State Attorney General" auslösen. Da in einigen Bundesstaaten zudem noch weitere Sondergesetze für bestimmte Kategorien personenbezogener Daten einschlägig sein können, ist die frühzeitige Einbindung eines im US-amerikanischen Recht kundigen Rechtsanwalts sinnvoll.

b) Attorney-Client-Privilege und Work-Product-Doctrine

Die Mandatierung eines amerikanischen Rechtsanwalts empfiehlt sich in Fällen transatlantischer IT-Sicherheitsvorfälle jedoch ohnehin allein schon wegen der Besonderheiten des amerikanischen Prozessrechts. Nach dem Attorney-Client-Privilege[40] ist die gesamte, mit der anwaltlichen Tätigkeit verbundene Korrespondenz zwischen dem Mandanten und seinem Anwalt dem Zugriff Dritter sowie der Strafverfolgungsbehörden und einer Pre-Trial-Discovery[41] entzogen.

Nach der sog. Work-Product-Doctrine[42] gilt dies ferner für solche Dokumente, die auf Auftrag des Anwalts durch Dritte erstellt worden sind. Durch die frühzeitige Mandatierung eines Rechtsanwalts kann bei IT-Sicherheitsvorfällen folglich sichergestellt werden, dass Arbeitsdokumente, die während der Ermittlungsphase angefertigt werden, nicht in etwaigen späteren Discovery-Verfahren i.R.v. Schadensersatzprozessen als Beweismittel verwertet werden können. Damit auch die Dokumente des IT-Forensikers unter die Work-Product-Doctrine fallen, sollte daher bereits dessen Beauftragung durch den mandatierten An-

34 *Schröder,* in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil VI Kap. 3 Rn. 72; *Hanloser,* CCZ 2010, 25 (29).

35 Einschließlich des District of Columbia, Puerto Rico, Guam und der Virgin Islands.

36 Ein detaillierter Überblick über die verschiedenen bundesstaatlichen Regelungen findet sich auf der Website des Unternehmens *Digital Guardian*, The Definitive Guide to U.S. State Data Breach Laws, abrufbar unter: bit.ly/2ZBGOz0.

37 In Kalifornien besteht eine Verpflichtung ggü. dem *California Attorney General* erst ab 500 Betroffenen (Cal. Civ. Code Sec. 1798.82(f)); ähnl. in Washington (Wash. Rev. Code Sec. 19.255.010(7)); demgegenüber gilt in New York eine Meldepflicht stets auch ggü. dem *N.Y. Attorney General*, der N.Y. Division der *State Police* und der *Consumer Protection*.

38 Der Begriff der persönlichen Daten ist regelmäßig deutlich enger als nach dem Verständnis der DS-GVO oder auch des CCPA und betrifft in Kalifornien etwa den Namen einer Person in Kombination mit Kennzeichen wie z.B. der Sozialversicherungsnummer oder Gesundheitsdaten etc., vgl. Cal. Civ. Code Sec. 1798.82(h)); ähnl. auch in New York (N.Y. Gen. Bus. Law Sec. 899-AA(1)(b)).

39 Cal. Civ. Code Sec. 1798.29, 1798.82; vgl. ähnliche Regelungen z.B. in New York: N.Y. Gen. Bus. Law Sec. 899-AA; Washington: Wash. Rev. Code Sec. 19.255.010; Texas: Tex. Bus. & Com. Code Sec. 521.053.

40 Seit Jahrhunderten gefestigter Grundsatz des „common law", vgl. etwa Upjohn Co. v. United States, 449 U.S. 383 (1981), Hunt v. Blackburn, 128 U.S. 464, 470 (1888); teilweise auch im Recht einzelner Bundestaaten kodifiziert, z.B. in Kalifornien in Cal. Evid. Code Sec. 950 et seq. oder New York in N.Y. Civ. Prac. Laws & Rules Sec. 4503; eingehend hierzu *Yoshida,* 66 Fordham L. Rev. 209 (1997).

41 Ausf. zur eDiscovery: *Spies,* in: Forgó/Helfrich/Schneider (o. Fußn. 34), Teil XIII Kap. 2.

42 Grundlegend Hickman v. Taylor, 329 U.S. 495 (1947); auf Bundesebene für das Zivilverfahren kodifiziert in den Federal Rules of Civil Procedure, Rule 26(b)(3), ferner im Recht zahlreicher Bundestaaten, z.B. in Kalifornien in Cal. Civ. Proc. Code Sec. 2018.010 et seq.

walt und nicht durch das betroffene Unternehmen selbst erfolgen.

Da ein konkludenter Verzicht („Waiver") auf die Privilegien des Attorney-Client-Privilege und der Work-Product-Doctrine möglich ist und u.U. bereits dann angenommen werden kann, wenn die Korrespondenz in die Hände beliebiger Dritter gelangt,[43] sollten sämtliche E-Mails und sonstige Korrespondenzen mit dem Hinweis „Privileged and Confidential" im Betreff und/oder der Kopfzeile versehen werden. Des Weiteren sollten alle Dokumente, die im Auftrag der mandatierten Anwält*innen erstellt wurden, in der Kopfzeile den Hinweis „Privileged and Confidential, Attorney Work Product prepared at Legal Counsel's Request" enthalten. Diese Hinweise dienen der Klarstellung, dass ein Verzicht auf die Privilegien nicht beabsichtigt ist. Über die teilweise sehr komplexen Vorgaben für die Gewährung des Attorney-Client-Privilege wird der beauftragte US-Anwalt vorab beraten.

IV. Abwicklungsphase und Aufarbeitung

Einen wichtigen Bestandteil des Incident Response Management bildet die abschließende Aufarbeitung des Sicherheitsvorfalls. Diese Aufarbeitung ist nicht nur zur Vermeidung zukünftiger Sicherheitsvorfälle unabdingbar, auch aus aufsichtsrechtlicher Sicht sollten erkannte Schwachstellen zur Verringerung von Datenschutzrisiken beseitigt werden, um aufsichtsbehördlichen Abhilfemaßnahmen zu entgehen.

Zu diesem Zweck sollten betroffene Unternehmen eine interne Untersuchung durchführen, um mögliche Ursachen für den Sicherheitsvorfall ausfindig zu machen. Nicht selten kann sich dabei herausstellen, dass geltende unternehmensinterne Policies nicht umgesetzt oder Hinweise auf mögliche Cyber-Risiken ignoriert wurden. In derartigen Fällen sind disziplinarische Maßnahmen gegen Mitarbeiter*innen oder sonstige Beauftragte, bis hin zur möglichen Beendigung der Zusammenarbeit anzudenken.

Dasselbe gilt in Fällen, in denen der Angriff intern auf (ehemalige) Mitarbeiter*innen zurückzuführen ist. Auch eine Prüfung möglicher Schadensersatzansprüche, die dem Unternehmen gegen Mitarbeiter*innen oder Dienstleister zustehen können,[44] sollte in Erwägung gezogen werden.

Schließlich sollten erkannte Sicherheitslücken zügig geschlossen werden, um eine eigene Haftung des Unternehmens zu vermeiden. Insoweit kann auch mit Schadensersatzforderungen gem. Art. 82 DS-GVO durch Betroffene zu rechnen sein, insbesondere wenn der Vorfall eine gesteigerte mediale Aufmerksamkeit erfährt.

Zuletzt sollten ggf. überarbeitete Policies und Sicherheitsmaßnahmen in Probeläufen, möglicherweise auch mit echtem, aber kontrolliertem Hacking durch sog. Purple- oder Red-Team-Operationen erprobt werden. Diese Testläufe können hilfreich sein, um Mitarbeiter*innen des Unternehmens mit den Abläufen vertraut zu machen und einen dann möglicherweise festgestellten Optimierungsbedarf umzusetzen.

43 Vgl. etwa Wadler v. Bio-Rad Laboratories, Inc., 212 F. Supp. 3d 829 (N.D. Ca. 2016).

44 So etwa, wenn externe Dienstleister eine offensichtliche Phishing-Mail öffnen und so der Angriff in Gang gesetzt wird.

Sollte es sodann zu einem tatsächlichen IT-Sicherheitsvorfall kommen, sind die Arbeitsabläufe besser eingeübt und können so im Ernstfall schneller umgesetzt werden.

V. Checkliste: Incident Response Management für Cyber-Sicherheitsvorfälle

- Frühzeitige Einbindung von IT-Forensiker*innen und spezialisierten Rechtsanwält*innen, am besten bereits vor Eintritt eines Sicherheitsvorfalls;
- Identifizierung und Schließung erkannter Sicherheitslücken, etwa durch Einrichtung neuer Accounts und Passwörter, Zweifaktorauthentifizierung zur zügigen Wiederherstellung der Handlungsfähigkeit etc.;
- Aufbereitung der Faktenlage und Dokumentation der Handlungsschritte und Gegenmaßnahmen;
- Durchsicht der von der Verletzung betroffenen Daten auf Grundlage einer Einwilligung der jeweiligen Betroffenen;
- Untersuchung einer Verpflichtung zur Meldung der Datenschutzverletzung nach DS-GVO und US-amerikanischem Recht, ggf. schrittweise Mitteilung;
- Handlungsanweisung an die Mitarbeiter*innen des betroffenen Unternehmens durch Aushändigung eines Kommunikationsprotokolls;
- ggf. Stellen von Strafanzeigen;
- interne Untersuchung und Prüfung etwaiger Folgen (Schadensersatzansprüche, Kündigungen etc.).

Schnell gelesen ...

- Cyber-Sicherheitsvorfälle lösen in transatlantischen Unternehmen komplexe und zeitkritische Verpflichtungen nach europäischem und US-amerikanischem Recht aus.
- Ein Incident-Response-Plan sollte bereits vor einem Sicherheitsvorfall ausgearbeitet und im Unternehmen zur Anwendung gebracht werden, um rechtzeitig und umfassend handeln zu können.
- Kommt es zu einem Cyber-Sicherheitsvorfall, erlaubt es der Einsatz spezialisierter IT-Forensiker*innen, das Ausmaß des Vorfalls schnell festzustellen und die Betriebsbereitschaft zügig wiederherzustellen.
- Das Bestehen von Melde- sowie Auskunftsverpflichtungen sollte zügig, aber sorgfältig geprüft werden und diese Pflichten sollten nur bei tatsächlichem Vorliegen der Voraussetzungen erfüllt werden.

Dr. Christian Schröder
ist Partner der IP/IT und Datenschutzpraxisgruppe der internationalen Wirtschaftssozietät Orrick, Herrington & Sutcliffe LLP in Düsseldorf und Mitglied des Wissenschaftsbeirats der ZD.

Tobias Lantwin
ist Wissenschaftlicher Mitarbeiter in der IP/IT und Datenschutzpraxisgruppe der internationalen Wirtschaftssozietät Orrick, Herrington & Sutcliffe LLP in Düsseldorf.