AUSGABE 03
MÄRZ 2024

THOUVENIN
WEKA

DATENSCHUTZ

FÜR SCHWEIZER UNTERNEHMEN UND INSTITUTIONEN

DATENSCHUTZ AKTUELL

Cyberattacke: Was muss in der Praxis gemacht werden?

Mehr dazu auf Seite 3

DATENSCHUTZ IM ARBEITSVERHÄLTNIS

Mitarbeitende: das schwächste Glied in der Cybersicherheit?

Mehr dazu auf Seite 7

DATENSCHUTZ UND IT

Cyberattacken: Praxisbeispiele und datenschutzrechtliche Abwägungen

Mehr dazu auf Seite 9

Editorial

Von Marco S. Meier, RA, MLaw, CIPP/E | Counsel bei THOUVENIN Rechtsanwälte KLG

LIEBE LESERIN, LIEBER LESER

Ich freue mich sehr, Sie zu dieser Ausgabe des WEKA-Newsletters «Datenschutz» zu begrüssen.

Fast täglich kann man in den Medien lesen, dass ein Unternehmen Opfer eines Cyberangriffs wurde. Auch das Bundesamt für Cybersicherheit verzeichnete 2023 einen Anstieg der gemeldeten Vorfälle um 30% bei knapp 50 000 eingegangenen Meldungen. Da die Meldungen beim Bundesamt für Cybersicherheit in der Regel nicht verpflichtend sind und nicht alle Fälle in den Medien publik werden, ist von einer deutlich höheren Dunkelziffer auszugehen. Wie verschiedene Fälle in der Vergangenheit gezeigt haben, können Cyberangriffe gravierende Folgen bis hin zum kompletten Stillstand des Betriebs oder Konkurs haben.

Vor diesem Hintergrund ist es für Unternehmen nicht nur von besonderer Bedeutung, dass sie auf den Ernstfall vorbereitet, sondern auch, dass die rechtlichen Rahmenbedingungen, insbesondere ggf. bestehende Meldepflichten an Behörden, bekannt sind. Neben den rechtlichen Anforderungen bestehen in der Praxis zahlreiche Herausforderungen, welche für die Bewältigung einer solchen Krisensituation von zentraler Bedeutung sind. Dazu gehören die Vorbereitung und das Training. Zur Vorbereitung sollte man sich bewusst sein, wie solche Angriffe funktionieren und wo die Hauptangriffspunkte im Unternehmen liegen. Bei dieser Analyse liegt oft der Schluss nahe, dass neben verwendeten Systemen die Mitarbeitenden ein für Angreifer einfaches Ziel darstellen. Insofern ist es wichtig, dass neben der Existenz eines Notfallplans Mitarbeitende sinnvoll geschult werden, sodass der Notfallplan im besten Fall nicht zum Einsatz kommen muss. Sollte es trotz aller Vorkehrungen vorkommen, dass eine Cyberattacke erfolgreich ist, stellt sich die Frage, in welchen Fällen eine Meldung an die zuständigen Behörden notwendig ist und wie eine solche Meldung aus datenschutzrechtlicher Sicht an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten gemacht werden muss.

Diese Ausgabe des WEKA-Newsletters «Datenschutz» fokussiert auf diese Fragestellungen und gibt praxisbezogene Hinweise zur Vorbereitung und Bewältigung von Cyberangriffen:

Der erste Beitrag von Rehana Harasgama **«Cyberattacke: Was muss in der Praxis gemacht werden?»** befasst sich praxisnah mit der Frage, wie im Falle einer Cyberattacke vorgegangen werden sollte.

Im zweiten Beitrag zeigt Simon Schneiter auf, warum und wie Mitarbeitende geschult werden sollten. Der Beitrag «**Mitarbeitende: das schwächste Glied in der Cybersicherheit?»** erörtert, wie Mitarbeitende zielführend und nachhaltig geschult werden können.

Abschliessend setzt sich der Beitrag **«Cyberattacken: Praxisbeispiele und datenschutzrechtliche Abwägungen»** von Dirk Spacek mit drei konkreten Beispielen auseinander und zeigt auf, wann der zuständigen Behörde gemeldet werden muss.

Ich wünsche Ihnen eine aufschlussreiche, spannende Lektüre.

Marco S. Meier, RA, MLaw, CIPP/E
Herausgeber

DER HERAUSGEBER

Marco S. Meier ist Counsel bei der Anwaltskanzlei THOUVENIN Rechtsanwälte KLG und ist spezialisiert auf Informations- und Kommunikationstechnologierecht (ICT). Er berät und vertritt seine Klienten in sämtlichen Bereichen des IT-, Datenschutz-, Cybersecurity- und Immaterialgüterrechts sowie in technologiebezogenen Compliance-Fragen. Als ausgebildeter Informatiker und Certified International Privacy Professional Europe (CIPP/E) hat er umfassende Erfahrung bei der Durchführung von Datenschutz-Compliance-Projekten, sowohl nach Schweizer Recht als auch nach der EU-Datenschutz-Grundverordnung, in Software- und Lizenzfragen sowie Technologie- und Outsourcing-Projekten in verschiedenen Branchen. Die Beilegung von Streitigkeiten im ICT-Bereich sowie die Beratung im Werberecht sind weitere Schwerpunkte seiner Tätigkeit.

www.thouvenin.com

m.meier@thouvenin.com

Cyberattacke: Was muss in der Praxis gemacht werden?

Jedes Unternehmen, unabhängig von seiner Grösse oder seinem Tätigkeitsfeld, kann Ziel einer Cyberattacke sein. Daher ist es wichtig, dass ein Unternehmen angemessene Datensicherheitsmassnahmen ergreift und einen Notfallplan implementiert. Hierzu gehören u. a. die Einführung und das Testen eines Notfallplans, die Investition in Datensicherheit, die Schulung von Mitarbeitenden und die Einhaltung der gesetzlichen und vertraglichen Pflichten. Ein wichtiger Aspekt des Notfallplans sind die gesetzlichen und vertraglichen Meldepflichten gegenüber Aufsichtsbehörden, betroffenen Personen und Kunden.

Von Rehana Harasgama

Was ist eine Cyberattacke?

Der Begriff «Cyberattacke» ist nicht rechtlich definiert und kann je nach Rechtsordnung und Rechtsprechung variieren. Für diesen Beitrag wird vom folgenden Verständnis ausgegangen:

> Eine Cyberattacke ist ein zielgerichteter, digitaler Angriff durch Umgehung von Datensicherheitsmassnahmen auf die Computer, Informationssysteme, Netzwerke oder Daten eines Unternehmens, um diese zu beschädigen, zu stören oder unrechtmässig auf sie zuzugreifen.

Es gibt unterschiedlichste Taktiken (von einfachen Betrugsversuchen bis hin zu hochentwickelten Kampagnen, die auf kritische Infrastrukturen und internationale Konzerne abzielen) und Methoden (z. B. Social Engineering, Ransomware, Spionage, Denial-of-Service-Angriffe, Malware oder Phishing) von Cyberattacken, und die Anzahl Cyberattacken hat in den letzten Jahren aufgrund der Zunahme von Automatisierungen und künstlicher Intelligenz (KI oder AI) stark zu genommen.

Cyberattacken haben in der Regel schädliche Absichten, wie z. B. der Diebstahl von Daten, die Lahmlegung von Systemen, finanzieller Schaden oder die Stiftung von Unruhe. Ein solcher Angriff kann auch von verschiedensten Akteuren ausgelöst werden, wie z. B. Hacker, Konkurrenten, eigene Mitarbeitende oder irgendwelche Drittpersonen.

Welche datenschutzrechtlichen Fragen stellen sich?

Wenn ein Unternehmen von einer Cyberattacke betroffen ist, stehen zunächst die betriebsinternen Fragen und Probleme im Vordergrund. Jedoch dürfen die datenschutzrechtlichen Meldepflichten nicht vergessen gehen.

Die Meldepflichten gemäss Schweizer Datenschutzrecht sind in Art. 24 DSG verankert. Sie werden nur ausgelöst, wenn eine Verletzung der Datensicherheit («Data Breach») im Sinne des DSG vorliegt.

Eine Verletzung der Datensicherheit liegt vor, wenn dadurch Personendaten (z. B. Namen, Adressen, Kreditkartenangaben, Geburtsdatum, Personaldossiers, Gesundheitsdaten etc.) aus Versehen oder widerrechtlich gestohlen, gelöscht oder verändert werden oder wenn eine unbefugte Person auf diese Daten zugreift. Es gibt im Schweizer Recht und international zahlreiche (nicht nur datenschutzrechtliche) Meldepflichten, die durch eine Cyberattacke ausgelöst werden können: Meldepflichten gegenüber der FINMA, Meldepflichten gemäss der EU-Datenschutz-Grundverordnung, Meldepflichten gemäss der europäischen NIS-2-Richtlinie oder anderen Verordnungen der EU (welche auch auf Schweizer Unternehmen anwendbar sein können) sowie die Meldepflichten für Anbieter kritischer Infrastrukturen in der Schweiz gemäss dem neuen Informationssicherheitsgesetz, das dieses Jahr in Kraft treten soll. Ausserdem können vertraglich vereinbarte Meldepflichten ausgelöst werden, welche oft mit der Bezahlung einer Vertragsstrafe kombiniert sind.

Bei einer Cyberattacke ist in der Regel von einem Data Breach auszugehen, da in den meisten Fällen Personendaten betroffen sind, sei es von den eigenen Mitarbeitenden, Lieferanten oder Kunden. Somit werden die Meldepflichten gemäss DSG grundsätzlich ausgelöst.

Gemäss Art. 24 DSG gibt es drei unterschiedliche Meldepflichten, die durch eine Cyberattacke ausgelöst werden können:

1. **Meldepflicht gegenüber dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten** («EDÖB»)
2. **Meldepflicht gegenüber den betroffenen Personen,** also z. B. Mitarbeitende, Lieferanten oder Kunden

3. Wenn ein Unternehmen für andere Unternehmen Personendaten bearbeitet (z. B. als Cloud-Provider, Anbieter von HR-Software oder weil es für Kunden die Lohnbuchhaltung übernimmt), also Auftragsbearbeiter ist, gibt es nur eine **Meldepflicht gegenüber dem Auftraggeber.** Dieser ist wiederum dafür verantwortlich, die anderen Meldepflichten zu erfüllen.

Die **Meldepflicht gegenüber dem EDÖB** wird nur ausgelöst, wenn die Cyberattacke zu einem hohen Risiko für die Mitarbeitenden, Lieferanten oder Kunden (also die betroffenen Personen) führen könnte. Dies kann der Fall sein, wenn sehr sensible Daten (z. B. Gesundheitsdaten) oder ein grosses Volumen an Daten betroffen sind, wenn besonders schützenswerte Personen betroffen sind (z. B. Kinder, Bankkunden oder Patienten) oder wenn es zu einem Identitätsdiebstahl kommen könnte. In einem solchen Fall müssen dem EDÖB folgende Informationen «so rasch als möglich» (in der EU gilt eine Frist von max. 72 Stunden) geliefert werden:

- Art der Verletzung
- Zeitpunkt und Dauer der Verletzung (falls möglich)
- Kategorien und Anzahl der betroffenen Daten (falls möglich)
- Kategorien und Anzahl der betroffenen Personen (falls möglich)
- Folgen und Risiken der Verletzung
- Geplante oder getroffene Massnahmen
- Namen und Kontaktdaten einer Ansprechperson

Diese Informationen können auch etappenweise mitgeteilt werden, solange der Data Breach an sich rasch gemeldet wird. Für diese Meldung gibt es ein Online-Formular, das ausgefüllt werden kann: https://databreach.edoeb.admin.ch/report. Die Meldung gegenüber dem EDÖB ist für mindestens zwei Jahre aufzubewahren.

Cyberattacken, die erfolgreich abgewendet werden oder nicht zu einem «hohen Risiko» führen, müssen nicht gemeldet werden. Eine Dokumentation des Vorfalls ist jedoch in jedem Fall empfohlen.

Die **Meldung gegenüber den betroffenen Personen,** z. B. Mitarbeitende, Lieferanten oder Kunden, ist gemäss Schweizer Recht nur notwendig, wenn dies ihrem Schutz dient oder sie selber Massnahmen ergreifen können, um die Risiken einzudämmen, wie z. B. ihre Kreditkarte sperren, ihre Bank informieren oder Passwörter ändern.

Auftragsbearbeiter haben ihrem Auftraggeber jegliche Data Breaches zu melden, damit der Auftraggeber selber entscheiden kann, ob eine Meldung gegenüber dem EDÖB oder den betroffenen Personen notwendig ist.

WICHTIGER HINWEIS

Achtung: Wie bereits oben erwähnt, können andere gesetzliche oder vertragliche Meldepflichten bestehen, die schneller oder weniger schnell ausgelöst werden. So ist es wichtig, dass ein Unternehmen genau weiss, wann was ausgelöst wird und wem was gemeldet werden muss.

PRAXISTIPP

Ein Unternehmen sollte eine Liste aller Meldepflichten (inkl. Voraussetzungen, Meldeinhalt und Fristen) und Behörden führen, das regelmässig überprüft und aktualisiert wird.

Drohen Sanktionen, wenn ein Unternehmen einen Data Breach nicht meldet?

Nach dem DSG drohen keine Bussen, wenn eine Verletzung der Datensicherheit nicht gemeldet wird. Wenn der Vorfall jedoch publik wird, ist es möglich, dass sich ein Unternehmen einer Untersuchung des EDÖB stellen muss oder die betroffenen Personen zivilrechtliche oder vertragliche Schritte ergreifen (wie z. B. Schadenersatzklagen oder Konventionalstrafen). Das grösste Risiko bildet wohl das Reputationsrisiko, welches durch eine nicht erfüllte Meldepflicht ausgelöst werden kann.

Gemäss europäischem Datenschutzrecht kann eine Busse bis zu EUR 10 Mio. oder 2% des weltweit erzielten Jahresumsatzes drohen.

Was ist eine Notfallplanung?

Ein guter Notfallplan ist ein entscheidendes Werkzeug für Unternehmen, um effektiv auf Cyberattacken zu reagieren. Dabei sollte ein solcher Plan genau auf die Bedürfnisse des Unternehmens zugeschnitten sein und nicht einfach nur einmal schriftlich festgehalten und nie wieder angeschaut werden, sondern regelmässig getestet und aktualisiert werden.

Zu einem guten Notfallplan gehören folgende Eckpunkte: Team («Incident Response Team») und Verantwortlichkeiten definieren, Tools und Ressourcen festlegen, gesetzliche und vertragliche Meldepflichten sowie die meldepflichtigen Behörden kennen, bei Bedarf Abschluss einer Cyberversicherung, Vorgehen detailliert festhalten und einen groben Kommunikationsplan für den Fall der Fälle festlegen.

Ein effektiver Notfallplan beinhaltet die frühzeitige Erkennung und Bewertung von Sicherheitsvorfällen, die Umsetzung von Sofort- und Langzeitmassnahmen zur Schadenseindämmung, die Identifizierung und Eliminierung der Bedrohungsursache sowie die Wiederherstellung normaler Betriebsabläufe. Wichtig sind auch die detaillierte Dokumentation und Analyse des Vorfalls, die Verbesserung von Präventionsstrategien, die Einhaltung rechtlicher Bestimmungen, wie z. B. der Datenschutz, sowie regelmässige Schulungen und Übungen für das Personal.

Wie ist nun konkret vorzugehen?

Das konkrete Vorgehen bei einer Cyberattacke hängt von den spezifischen Umständen ab wie der Art der Cyberattacke, den betroffenen Systemen, dem Business des Unternehmens oder den betroffenen Daten. Jedoch sollten die folgenden grundlegenden Schritte in der Praxis umgesetzt werden (diese Schritte lassen sich nicht immer genau voneinander abgrenzen, und die Reihenfolge kann je nach Vorfall variieren):

- **Sofortige Reaktion:** Unternehmen sollten unverzüglich auf eine festgestellte Cyberattacke reagieren. Die betroffenen Systeme sollten so rasch wie möglich unterbrochen oder von anderen Systemen getrennt werden, um eine weitere Ausbreitung des Angriffs zu verhindern, und das Incident Response Team sollte umgehend informiert werden.

ACHTUNG

Wenn ein Unternehmen eine Cyberrisikoversicherung hat, sollte auch sofort geprüft werden, welche Schritte gemäss der Versichrung initial vorzunehmen sind. Üblicherweise muss die Meldung gegenüber der Versicherung sofort erfolgen, und die Auswahl der rechtlichen und technischen Experten steht einem Unternehmen nicht immer frei.

- **Identifikation und Ersteinschätzung des Angriffs:** Das Incident Response Team sollte sodann die Art der Cyberattacke sowie das Ausmass des Schadens vorläufig eruieren. Dies ist für die Identifizierung der nächsten Schritte hilfreich. Die Ersteinschätzung kann sich im Verlauf der weiteren Untersuchung verändern, wenn klar ist, welche Systeme genau betroffen sind, was genau passiert ist, was für Daten genau betroffen sind etc.
- **Regelmässige Berichterstattung:** Das Incident Response Team ist für die regelmässige Berichterstattung gegenüber der Geschäftsleitung und/oder dem Verwaltungsrat verantwortlich. Die Geschäftsleitung und/oder der Verwaltungsrat sollten von Anfang an miteinbezogen werden, da sie am Ende die Entscheidträger sind.
- **Einsatz von Experten:** Das Incident Response Team sollte danach die im Notfallplan definierten Experten hinzuziehen, um den Vorfall detailliert zu untersuchen, den Schaden genauer zu definieren und die Gegenmassnahmen einzuleiten. Hierzu gehört, z. B. die Back-ups zu konsultieren, um die Systeme so rasch wie möglich wieder in Betrieb zu nehmen und den Geschäftsgang zu sichern.
- **Beweissicherung:** Das Incident Response Team sollte gemeinsam mit den Experten und zuständigen Forensikern alle Daten und Beweise, die mit der Cyberattacke zusammenhängen, sichern. Dies ist für die vertiefte Untersuchung und die rechtlichen Schritte gegen die Täter oder auch zur Verteidigung gegen Ansprüche Dritter bedeutsam.
- **Planung und Implementierung von Massnahmen:** Das Incident Response Team sollte in einem nächsten Schritt prüfen, welche (Gegen-) Massnahmen implementiert werden sollen, um die Schwachstellen zu adressieren, die Daten zu sichern, die Systeme wieder in Betrieb zu nehmen und den Geschäftslauf wieder aufzunehmen. Die identifizierten (Gegen-)Massnahmen sollten so rasch als möglich umgesetzt werden.
- **Überprüfung der Compliance:** Das Incident Response Team sollte im Rahmen der Untersuchung des Vorfalls zugleich prüfen, ob die Datensicherheit den rechtlichen oder regulatorischen Vorgaben sowie dem Stand der Technik entspricht. Wenn dies nicht der Fall ist, kann dies zu einer Busse führen. Ausserdem sollten erkannte Schwachstellen so schnell wie möglich behoben werden.
- **Rechtliche Schritte:** Zudem sollte geprüft werden, ob das Unternehmen rechtliche Schritte einleiten will, z. B. die Anzeige der Täter. Dies zeigt auf der einen Seite, dass das Unternehmen den Vorfall ernst nimmt, und kann auf der anderen Seite der Wiedererlangung von Verlusten und zur Abschreckung weiterer Angriffe dienen. Die Einleitung rechtlicher Schritte ist nicht immer einfach, da oft ungenügende Beweise vorhanden sind.

- **Überprüfung von Kundenverträgen oder Verträgen mit Dritten:** Das Incident Response Team sollte die Kundenverträge auf allfällige Meldepflichten hin sowie die Verträge mit Dritten (wie Cloud-Anbietern oder IT-Dienstleistern) nochmals genau prüfen, um mögliche Haftungsfragen zu klären.
- **Kommunikationsstrategie:** Gemäss der im Notfallplan vorgesehenen Kommunikationsstrategie sollten interne und externe Stakeholder (wie Mitarbeitende, Lieferanten oder Kunden) über den Vorfall informiert werden, damit kein Vertrauensverlust resultiert, weil sie anderweitig davon erfahren. Wie oben beschrieben, kann es gesetzliche oder vertragliche Informationspflichten geben, die in jedem Fall zu erfüllen sind. Intern sollten Mitarbeitende darauf aufmerksam gemacht werden, dass sie den Vorfall vertraulich zu behandeln haben und nicht mit Externen (auch nicht mit Familienmitgliedern) besprechen sollten, bevor das Unternehmen eine solche Kommunikation freigibt.
- **Meldung gegenüber Behörden:** Sofern gesetzliche Meldepflichten greifen, sollte das Incident Response Team den Vorfall den zuständigen Behörden melden. Dies kann dazu führen, dass Behörden in verschiedenen Kantonen oder Ländern informiert werden müssen, was entsprechend zu koordinieren ist. Aus diesem Grund ist es wichtig, bereits vorgängig zu wissen, welche Behörden informiert werden müssen. So können allfällige sehr kurze Meldefristen eingehalten werden (gemäss EU-Datenschutzrecht wären es max. 72 Stunden seit Erkennung des Vorfalls).
- **Überprüfung und Anpassung der Sicherheitsstrategie:** Sobald die Untersuchung abgeschlossen ist und allfällige Informations- und Meldepflichten erfüllt wurden, sollte das Incident Response Team gemeinsam mit den zuständigen Personen die Sicherheitsstrategie des Unternehmens überprüfen und allfällige erkannte Schwachstellen beheben.

- **Regelmässige Überprüfung der getroffenen Massnahmen:** Rechtliche Rahmenbedingungen und die technologischen Möglichkeiten für Cyberattacken ändern sich ständig, daher ist es wichtig, die Compliance-Anforderungen sowie die getroffenen Massnahmen regelmässig zu überprüfen und anzupassen.
- **Dokumentation:** Die Meldung sowie der Vorfall sollten intern dokumentiert werden. Insbesondere sollten die gewonnenen Erkenntnisse («Lessons Learned») festgehalten werden, damit zukünftige Vorfälle dieser Art vermieden werden können.
- **Schulung und Bewusstsein:** Schliesslich sollten die Mitarbeitenden regelmässig, aber insbesondere nach einem solchen Vorfall erneut im Hinblick auf Cyberrisken und -attacken geschult werden. Ein Unternehmen ist auf das Bewusstsein der Mitarbeitenden angewiesen, denn viele Verletzungen der Datensicherheit können auf ungenügendes Bewusstsein seitens der Mitarbeitenden zurückgeführt werden.

Fazit: Planen, testen, Ruhe bewahren und ausführen

In aller Regel ist jedes Unternehmen, das von einer Cyberattacke getroffen wird, im ersten Moment überrascht und überfordert. Genau aus diesem Grund ist es wichtig, gut vorbereitet zu sein und einen Notfallplan zu haben, der regelmässig getestet wird. Zur guten Vorbereitung gehört auch die regelmässige Schulung der Mitarbeitenden.

Bei einer eingetretenen Cyberattacke ist es wichtig, dass das Incident Response Team die Ruhe bewahrt und den Notfallplan umsetzt. Dabei ist es wichtig, den Notfallplan nicht nur digital vorliegen zu haben, sondern auch physisch, falls die gesamten Systeme ausfallen und sonst nicht darauf zugegriffen werden kann. Ein ruhiges und systematisches Vorgehen ist dabei unerlässlich.

Die ersten Schritte nach dem Vorfall sind die entscheidenden, insbesondere die sofortige Reaktion auf den Vorfall, indem die Systeme unterbrochen oder getrennt werden, und die Involvierung des Incident Response Teams.

Alle anderen Schritte verlangen gute Teamarbeit, dabei spielt jede involvierte Person eine wesentliche Rolle, um die laufende Geschäftstätigkeit so schnell wie möglich wieder aufzunehmen und das Vertrauen der Kunden zu bewahren.

Take Home Message:

- Gute Vorbereitung (Team definieren und Notfallplan implementieren)
- Sofortige Reaktion
- Identifikation und Ersteinschätzung des Angriffs
- Beweissicherung
- Planung und Implementierung von (Gegen-)Massnahmen
- Überprüfung der Compliance und bestehender Verträge
- Kommunikation und Meldung
- Überprüfung und Anpassung der Sicherheitsstrategie und der getroffenen Massnahmen
- Dokumentation
- Schulung und Bewusstsein

AUTORIN

Rehana Harasgama ist Expertin im Schweizer und internationalen Technologie-, Cybersecurity- und Datenschutzrecht. Sie ist auch Dozentin für Datenschutz an der Universität St. Gallen (HSG).

Mitarbeitende: das schwächste Glied in der Cybersicherheit?

Unzählige Untersuchungen zeigen, dass die allermeisten Cybersicherheitsvorfälle auf menschliche Fehler zurückzuführen sind. Adäquate Schulungen können helfen, dieses Risiko zu verkleinern und damit die Sicherheit des Unternehmens zu stärken. Warum die Mitarbeiterausbildung in diesem Bereich so wichtig ist und wie effektive Awareness-Programme auszugestalten sind, wird in diesem Artikel dargelegt.

Von Simon Schneiter

Vor 24 Jahren programmierte ein junger Philippiner ein Stück Computercode, welches weltberühmt werden sollte. Im Mai 2000 breitete sich das Loveletter-Virus explosionsartig per E-Mail aus. Damals waren E-Mails mit schädlichen Anhängen noch weitgehend unbekannt, und so ist es verständlich, dass Millionen von Menschen in der Hoffnung auf eine nette Liebesbotschaft das Virus ausführten. Rund ein Vierteljahrhundert später sind die Menschen weitaus besser informiert über Themen wie Phishing, Computerviren und Hacker. Oder?

Schwächstes Glied

Leider wird immer noch sehr häufig etwas angeklickt, was sich schlussendlich als schädlich herausstellt. Unzählige Studien zeigen, dass der sogenannte menschliche Fehler immer noch die mit Abstand grösste Risikoquelle für Cybersicherheitsvorfälle ist. Das Sicherheitsunternehmen Tessian hat zusammen mit dem Stanford-Professor Jeff Hancock eine Studie namens «Psychology of Human Error 2022» durchgeführt, in welcher aufgezeigt wurde, dass ganze 88% der Datensicherheitsverletzungen auf Fehler der Mitarbeitenden zurückzuführen sind. Gemäss dem Global Risk Report des WEF aus dem Jahr 2022 sind es sogar 95%.

Investitionen in angemessene technische Sicherheitslösungen sind unerlässlich. Aber selbst die allerbesten technischen Massnahmen nützen wenig, wenn Mitarbeitende mit ihren Zugangsdaten falsch umgehen, auf Phishing-Mails hereinfallen oder Vorschriften zum Umgang mit sensiblen Daten nicht beachten.

Rechtliche Vorgaben

Unternehmen, die in regulierten Branchen tätig sind, sind oft mit Anforderungen konfrontiert, welche eine Schulung der Mitarbeitenden in den Bereichen Datenschutz und -sicherheit explizit oder implizit vorsehen. Und auch das neue Datenschutzgesetz macht implizit eine Mitarbeiterschulung notwendig – wie sonst sollen die organisatorischen Massnahmen zur Datensicherheit greifen?

Wirksame Schulungen

Einmal pro Jahr 45 Minuten Frontalunterricht oder ein webbasiertes Training? Dass das kaum wirksam ist, dürfte heute den meisten Entscheidungsträgern klar sein. Wer es dabei belässt, macht Mitarbeiterschulungen oft nur, um entsprechenden Vorgaben zu genügen, und nicht, um die Sicherheit des Unternehmens effektiv zu stärken.

Eine wirksame Schulung muss über die reine Wissensvermittlung hinausgehen. Es gilt, das Bewusstsein für Cybersicherheit zu fördern und die Mitarbeitenden dazu zu bringen, in diesem Sinne zu denken und zu handeln. Um dies zu erreichen, sollten Schulungen die folgenden Hauptmerkmale aufweisen.

- **relevant und zielgerichtet:** Die Schulungsinhalte sollten zielgruppengerecht, das heisst auf die spezifischen Rollen und Zuständigkeiten der Mitarbeitenden zugeschnitten sein und sich mit den Sicherheits-

herausforderungen befassen, denen sie bei ihrer täglichen Arbeit begegnen. Es ist wichtig, die unterschiedlichen Kenntnisse der Mitarbeitenden zu berücksichtigen und Schulungen anzubieten, die für alle zugänglich und relevant sind.

- **ansprechend und interaktiv:** Klassenzimmeratmosphäre ist nicht besonders förderlich für die Aufmerksamkeit. Interaktive und ansprechende Methoden wie Simulationen, Rollenspiele und Gamification sowie der geschickte Einsatz unterschiedlicher Medien können einen aktiven und intensiven Lernprozess begünstigen.
- **kontinuierlich statt einmalig:** Es gibt gleich zwei gute Gründe, um Schulungen kontinuierlich und mehrmals jährlich stattfinden zu lassen. Erstens verblasst die Wirkung einer einmaligen Schulung meist relativ schnell, und bloss durch mehrmaliges Wiederholen werden Wissen und Know-how im Gedächtnis effektiv verankert. Zweitens entwickelt sich die Bedrohungslandschaft ständig weiter, und das Bewusstsein der Mitarbeitenden muss damit Schritt halten.
- **messbar und nachvollziehbar:** Eine wirksame Schulung sollte sich positiv auf die Sicherheitslage des Unternehmens auswirken. Die Anzahl der absolvierten Schulungen des Personals zu messen, ist jedoch eine eher schlechte Kennzahl dafür. Aussagekräftiger sind Kennzahlen wie z. B. die Phishing-Anfälligkeit, die Anzahl der Sicherheitsvorfälle und der Sensibilisierungsgrad der Mitarbeitenden. Letzterer lässt sich mit entsprechenden Tests und/oder Umfragen erheben.

PRAXISTIPP

«Öfter, aber weniger»

In der Praxis hat sich der Ansatz bewährt, Inhalte in kleinere Schulungssequenzen aufzugliedern und diese über das Jahr verteilt den Mitarbeitenden zu präsentieren. Idealerweise geschieht dies auf eine zielgerichtete, multimediale und interaktive Art.

PRAXISTIPP

Phishing-Simulationen

Gemäss einer Studie von IBM beginnen 41% aller erfolgreichen Angriffe mit einer Phishing-Mail. Dementsprechend sind Phishing-Simulationen ein äusserst nützliches Tool, um das Bewusstsein der Mitarbeitenden für diese Gefahr zu schärfen, das gewünschte Verhalten zu schulen, und nicht zuletzt, um die Effektivität der Schulungsmassnahmen messen zu können. Heutzutage sind solche Tests nicht mehr mit übermässig viel Aufwand verbunden. Es stehen etliche Tools und Services zur Verfügung, mit welchen sich auch gross angelegte und regelmässige Phishing-Kampagnen nahezu vollständig automatisieren lassen.

Wichtige Vorbildfunktion

Es mag abgedroschen klingen, dass Personen in Führungspositionen mit gutem Vorbild vorangehen sollen. Untersuchungen zeigen jedoch klar, dass es so ist. Führungskräfte beeinflussen das Verhalten und die Einstellung der Belegschaft. Sie tun dies mit dem, was sie sagen und wie sie es sagen – viel mehr jedoch noch mit ihrem Verhalten. Dementsprechend ist ihr Einfluss auf den Erfolg der Schulungsmassnahmen kaum zu unterschätzen. Und genau dies gilt es dem Management bewusst zu machen. Auf welche Art dies idealerweise geschieht, ist abhängig von der Unternehmenskultur und den jeweiligen Persönlichkeiten. Einige Organisationen setzen auf spezielle Management-Awareness-Schulungen, andere auf dedizierte Risiko-Workshops und wieder andere auf bilaterale Gespräche zwischen den für die IT-Sicherheit verantwortlichen Personen und der Unternehmensleitung.

Aufwand reduzieren

Cybersicherheitsschulungen sind wichtig. Demgegenüber stehen jedoch oft limitierte personelle Ressourcen und etliche andere ebenso wichtige Aufgaben. Hier kann es sich lohnen, in Tools und Services zu investieren, welche die Aufwände signifikant senken. Es gibt etliche Anbieter, welche Kombinationen von vorgefertigten webbasierten Trainings in Kombination mit (teil-)automatisierten Phishing-Simulationen anbieten. Einige davon liefern sogar passende Inhalte, mit welchen auch andere Kanäle bespielt werden können (Info-Mails, Printplakate, Games etc.). Und wenn finanzielle Ressourcen die grössere Herausforderung sind, so lassen sich mit ein wenig Recherche etliche Quellen mit frei verfügbaren Inhalten finden.

Fazit

Cyberattacken können jeden treffen. Die Eintrittswahrscheinlichkeit und das potenzielle Schadensausmass lassen sich aber durch gezielte Massnahmen senken. Eine besonders wichtige Massnahme ist die Schulung der Mitarbeitenden – zumal die allermeisten Cyberangriffe immer noch auf menschliches Versagen zurückzuführen sind. Dabei sollte auf zielgerichtete und relevante Schulungsinhalte gesetzt werden, welche ansprechend und attraktiv präsentiert werden. Das zu vermittelnde Wissen und Know-how sollte besser in kleineren Häppchen, dafür öfter serviert werden. Vorgesetzte müssen sich ihrer Vorbildfunktion bewusst sein und diese wahrnehmen. Und die Effektivität der Schulungen gilt es mit adäquaten Kennzahlen zu messen.

AUTOR

Simon Schneiter, M.A. HSG (Informations-, Medien- und Technologiemanagement), Head GRC & Information Security Consulting bei ensec AG.

Cyberattacken: Praxisbeispiele und datenschutzrechtliche Abwägungen

Cyberattacken sind keine Seltenheit mehr. Nicht nur hat deren Anzahl zugenommen, sondern vor allem deren Grad an Raffiniertheit hat sich erhöht. Besondere Achtsamkeit ist deshalb heutzutage aus Unternehmenssicht gefragt. Unternehmen müssen substanzielle Ressourcen einsetzen, um sich gegen solche Angriffe zu schützen. Das Schadenspotenzial ist gross bis fallweise enorm. Aus datenschutzrechtlicher (und auch kunden- bzw. vertragsrechtlicher) Sicht stellt sich dabei öfters die prekäre Frage, ob Meldungen an Behörden erfolgen oder ob eventuellsogar Kunden über diese Vorfälle informiert werden müssen. Sind personenbezogene Daten durch einen solchen Angriff kompromittiert, kann sich unter Umständen eine Meldepflicht aus Art. 24 DSG oder aus noch weiteren Erlassen ergeben. Der nachfolgende Beitrag soll drei ausgewählte Praxisbeispiele[1] vorführen und die sich stellenden Abwägungen für Leser etwas näherbringen.

Von Dirk Spacek

Praxisbeispiel 1: Ransomware-Angriff

Eine Gesellschaft stellt fest, dass ihre ganze IT-Systemumgebung (E-Mails, CRM, VDI) gesperrt ist. Auf dem Bildschirm erscheint eine Mitteilung von einer Gruppe «LIMEHACK», die eine Ransomewareforderung von CHF 10 Mio. erhebt, nach deren Bezahlung die Sperrung sämtlicher Prozesse wieder freigegeben würde. Für Bezahlungszwecke wird ein Link angegeben, der eine Bezahlung in Bitcoin vereinfacht ermöglichen solle. Die Gesellschaft schaltet umgehend einen Forensik-Experten ein, um den Angriff auf die Infrastruktur zu überprüfen, zu beheben und weitere Massnahmen vorzuschlagen. Die Mitarbeiter sind über den Vorfall bereits informiert. Das Management der Firma kommuniziert temporär nur über ihre privaten E-Mail-Adressen, zumal das Firmennetzwerk (inkl. E-Mail) nicht mehr funktioniert.

Aus datenschutzrechtlicher/kundenvertragsrechtlicher Sicht sind gewisse Ergänzungsfragen zu stellen. So ist etwas in Erfahrung zu bringen, ob ein Zugriff auf Personendaten im Netzwerk der Gesellschaft überhaupt wahrscheinlich stattfand oder ob lediglich ein z. B. Virus die Systemumgebung lahmlegt, ohne dass Dritte überhaupt Zugang zu den darin befindlichen Daten haben könnten. Oftmals ist diese Frage nicht eindeutig zu beantworten bzw. im Zusammenspiel mit IT-Forensikern zu suchen. Manchmal lässt sich z. B. feststellen, dass ein unbefugter Dritter Zugang zu Daten erhalten oder diese sogar heruntergeladen hat. Manchmal lässt sich dies nicht oder noch nicht feststellen. Aus Sicht von Art. 24 DSG ist der technische Befund wohl nicht so entscheidend, denn lässt sich ein Zugriff nicht eindeutig feststellen, kann er auch nicht eindeutig ausgeschlossen werden bzw. muss aus Sorgfaltsüberlegungen mit der Eventualität eines solchen Zugriffs gerechnet werden. Erscheint ein unbefugter Zugriff auf Daten wahrscheinlich, ist im Zweifel von einem solchen auszugehen. Eine oftmals in diesem Zusammenhang vorgenommene Prüfung ist, ob Daten der Gesellschaft irgendwo im sogenannten Darknet auftauchen. Letzteres dürfte ein Indiz sein, dass ein Zugriff auf Daten stattgefunden hat. Auch dürfte ein erfahrener IT-Forensiker prüfen, ob die Gruppierung «LIMEHACK» bekannt ist und im Verkehr bereits öfters durch solche Angriffe aufgetreten ist. Bei in der Vergangenheit bekannterweise stattgefundenen unbefugten Zugriffen dieser Gruppe (Ruf) sollte im Zweifel auch beim vorliegenden Angriff von einem möglichen Datenzugriff ausgegangen werden.

Territorial sollte auch die Frage gestellt werden, wo die z. B. betroffenen Kunden- oder Mitarbeiterdaten des Vorfalls ansässig sind? Sind diese z. B. auch in der EU ansässig, ist auf diese mutmasslich auch die DSGVO anwendbar und sind Meldungen nicht nur in der Schweiz, sondern gegebenenfalls auch bei Datenschutzaufsichtsbehörden in der EU vorzunehmen.

Nun besteht die Meldepflicht in der Schweiz gemäss Art. 24 DSG grundsätzlich nur dann, wenn diese voraussichtlich zu einem hohen Risiko für betroffene Personen führt, und sie ist «so bald als möglich» zu erstatten. Auch wenn in der Schweiz keine fixe Zeitvorgabe besteht – anders in der EU unter der DSGVO, wo Meldung innert 72 Stunden ab Beginn des Vorfalls zu erstatten ist –, ist mit einem ähnlichen Zeitraster von mehreren Tagen bis ca. einer Woche realistisch zu rechnen. Im Faktor Risiko (insbesondere dem

1 Die Praxisbeispiele basieren auf realen vom Verfasser betreuten Fällen, aber in abgewandelter Form.

«hohen» Risiko) liegt ein Abwägungskriterium für die Meldepflicht. Nun können zur Beurteilung dieses Faktors verschiedene Faktoren herangezogen werden wie z. B. Wahrscheinlichkeit des Datenzugriffs, Sensitivität der betroffenen Daten, Quantität der zugegriffenen Daten (z. B. bei Kundendaten fünf Datensätze von 10 000 oder die gesamte Datenbank mit allen Datensätzen) und gegebenenfalls auch noch der Umstand, ob Betroffene über den Vorfall informiert wurden. Liegt z. B. ein nachweislicher Zugriff nur auf ein HR-System der IT-Umgebung vor (also alle Mitarbeiter hiervon betroffen sind), und sämtliche Mitarbeiter wurden darüber informiert, ist das Risiko, dass diese z. B. Opfer von späteren betrugsähnlichen Delikten des Angreifers werden könnten, wieder etwas reduziert. Dieses Kriterium unterscheidet die Schweiz auch von der EU, wo im Unterschied in der DSGVO gefordert wird, dass der Datenzugriff ein «Risiko» für die Betroffenen schafft und nicht ein «hohes» wie in der Schweiz. Als nicht überzeugend erscheint es, von einem tiefen Risiko auszugehen, weil sich der Sachverhalt noch nicht technisch genau rekonstruieren lässt. Es ist weitaus üblich, dass sich Cyberangriffe anfänglich technisch nicht schlüssig rekonstruieren lassen, doch das hat weniger Einfluss auf die Meldepflicht als möglicherweise auf den Zeitpunkt, innert dessen die Meldung zu erstatten ist. Im Übrigen ist es durchaus üblich, «vorsorgliche Datenverletzungsmeldungen» zu erstatten, mit der Bemerkung, der Sachverhalt werde noch genauer abgeklärt und eine definitive Klärung/Meldung erfolge zu einem späteren Zeitpunkt (ca. drei bis vier Wochen später).

Zu unterscheiden von der Meldepflicht unter dem DSG sind sektorspezifische Meldepflichten, die sich aus Spezialerlassen ergeben, oder eine solche, die sich aus vertragsrechtlichen Gesichtspunkten gegenüber dem Kunden ergeben. Beispielsweise sind Banken über jegliche Cyberattacken meldepflichtig, egal welches Risiko dabei besteht, gemäss der FINMA-Aufsichtsmitteilung 5/2020 und ab 2025 voraussichtlich auch als «kritische Infrastrukturbetreiberin» gemäss dem neuen Informationssicherheitsgesetz, welches dann in Kraft treten dürfte. Nebst diesen sektorspezifischen Pflichten können auch vertragsrechtliche Anhaltspunkte bestehen, die eine Meldung an Kunden erforderlich machen. So sehen gewisse Dienstleistungsverträge eine solche Meldepflicht an den Kunden vor, oder die allgemeine Sorgfaltspflicht und Schadensminderungspflicht eines Beauftragten macht es erforderlich, dass man einen Kunden über eine Kompromittierung seiner Daten informiert. Ein Beispiel für Gefahrenpotenzial, welches beim dienstleistenden Unternehmen eine Schadensminderungspflicht aufleben lässt, sind Zahlungsdaten von Kunden (z. B. Kreditartennummern, Transaktionsauszüge). Anzumerken ist, dass die Meldepflicht an Kunden unabhängig von einer allfälligen Meldepflicht an die Datenschutzaufsichtsbehörden gemäss Art. 24 DSG besteht. So bedingt weder die eine Meldung die andere. Zwar ist möglich, dass die Datenschutzaufsichtsbehörden nach eingehender Prüfung zum Schluss kommen, dass sie eine Mitteilung an Kunden empfehlen/nahelegen, doch muss dies nicht immer der Fall sein. Handkehrum kann eine Meldung an die Datenschutzaufsichtsbehörden nicht zwingend erforderlich sein, eine Meldung an Kunden aber z. B. aufgrund solcher expliziten Pflichten im Vertragswortlaut schon.

Wie geht ein Unternehmen nun mit der Gretchenfrage um, ob es einer Lösegeldforderung Folge leisten soll, um die Herrschaft über seine blockierten Daten zurückzugewinnen. In den meisten Fällen sind dem Autor solche Fälle nicht bekannt geworden, zumal die Systeme heruntergeschaltet wurden und von einem Back-up-Server mit Daten eines Stands ca. vier Stunden vor dem Cyberangriff neu überspielt wurden. In den meisten Fällen war die Systemumgebung danach wieder 100% operativ mit nur wenigen Datenverlusten aufgrund der verstrichenen vier Stunden. Zeitgleich wurde die Ursache/das Eintrittstor des Angriffs diagnostiziert und Massnahmen eingerichtet, dass ein solcher Angriff in selber Form nicht mehr stattfinden kann. Handkehrum sind dem Autor Fälle bekannt, wo der Lösegeldforderung Folge geleistet wurde. Es gibt gute Gründe dafür, bekannten Gruppierungen Lösegelder zu überweisen, zumal diese einen gewissen Ruf im (kriminellen) Markt geniessen. Wird die sinngemässe Gegenforderung einer Entschlüsselung der Daten nicht erfüllt, steht die Reputation dieser Grup-

pierung auf dem Spiel. Darum können IT-Forensiker unter Umständen die Empfehlung einer Lösegeldbezahlung (wenn keine anderen technischen Optionen bestehen) manchmal erteilen. Aus rechtlicher Sicht zu prüfen ist dabei mehr der Umstand, dass so Geld an eine kriminelle Organisation übermittelt und je nachdem durch Bitcoin-Transaktionen die Nachverfolgung unkenntlich gemacht/verschleiert wird. Hier stellt sich aus rechtlicher Sicht bisweilen die Frage, ob dies den Tatbestand der Geldwäscherei erfüllen könnte. Dieser Aspekt kann hier aus Platzgründen nicht abschliessend beantwortet werden, doch sollte er im Einzelfall verifiziert werden.

Praxisbeispiel 2: Gehackte E-Mail

In einem Unternehmen wurden ca. drei E-Mails von Mitarbeitern gehackt und via «Forward»-Button an Kunden des Unternehmens weitergeleitet. Kritisch ist, dass in diesen internen Mitarbeiter-E-Mails Namen und Vornamen anderer Kunden des Unternehmens erwähnt werden. In anderen Worten, die Empfänger dieser drei gehackten und weitergeleiteten E-Mails wissen nun um – vertrauliche – Kundennamen des Unternehmens.

Was ist am vorliegenden Fall grundlegend anders als im ersten geschilderten Fall? Ein Cyberangriff (d. h. ein unbefugter Zugriff auf Daten des Unternehmens) hat unstrittig stattgefunden. Es steht ausser Diskussion, dass die Täter offenbar Zugriff zur E-Mail-Datenbank des Unternehmens gewinnen, diese E-Mails lesen und via «Forward»-Befehl an einen Dritten senden konnten. Auch ist unstrittig, dass personenbezogene Daten (Vor- und Nachname von Kunden) extrahiert und weitergeleitet wurden an unbefugte Dritte. Das bringt das Unternehmen in die unangenehme Lage, dass dieses die Vertraulichkeitsverpflichtungen gegenüber ihren zumindest drei Kunden nicht einhalten konnte. Wäre dieses Unternehmen nun eine Bank, läge sogar die Sachfrage einer Verletzung des Bankgeheimnisses auf dem Tisch (dies kann auch als Variante fahrlässig begangen werden).

Mit Blick auf die datenschutzrechtliche Meldepflicht stellt sich die Frage, ob hier von einem «hohen Risiko» für Betroffene auszugehen ist, welches die Meldepflicht auslöst, oder eher nicht. Zu erfragen ist in diesem Zusammenhang, welche genauen Daten der Kunden gegenständlich sind. Ein Beispiel: Fritz Müller, Hans Weber, Alexander Bauer. Nur diese Namen liegen vor, keine anderen Zusatzangaben (wie etwas Kontodaten, Zahlungsdaten oder Adresse bzw. ähnliche «Identifiers», welche diese Personen leichter eruierbar machen könnten). Die Namen kommen im Schweizer Telefonbuch ca. 20- bis 30-mal vor. Es ist mithin nicht einmal klar, welche dieser 20–30 Personen in der Briefkommunikation adressiert waren. Die Betroffenen sind eingrenzbar, aber nicht eindeutig individualisierbar. Hinzu gelangt, dass nur drei E-Mails gehackt bzw. nur drei Kundennamen der Gesellschaft tangiert waren (4000 Kunden der betroffenen Gesellschaft). Nach Auffassung des Autors dürfte bei diesem Gesamtbild unter Umständen von einem eher tiefen Risiko weiterer Rechtsverletzungen gegen die Betroffenen ausgegangen werden. Das Risiko könnte noch weiter reduziert werden, indem diese Betroffenen individuell über den Vorfall informiert werden (sodass sie adäquate Schutzmassnahmen treffen könnten) und die Empfänger der fälschlicherweise weitergeleiteten E-Mail auffordert, die Löschung der nicht für sie bestimmten E-Mail zu bestätigen. Diesfalls könnte aufgrund der getroffenen Massregeln von einem tiefen, weiteren Verletzungsrisiko der Betroffenen ausgegangen werden und auf eine Meldung an die datenschutzrechtlichen Aufsichtsbehörden eventuell verzichtet werden.

Die Situation könnte aber durchaus anders beurteilt werden, wenn grössere Mengen betroffen wären, die Namen wesentlich individualisierbarer wären (z. B. zwei bis drei Menschen in der Schweiz mit solchen Namen und zusätzlichen «Identifiers» wie Adresse, Telefonnummer) und auch kritische/sensitive Personendaten gegenständlich wären (wie etwa Zahlungs- und Transaktionsdaten, Personenprofile oder z. B. Lebensläufe in einem Bewerbungskontext). Auch in die Beurteilung hineinfliessen dürfte die Reputation der Tätergruppe – sollte diese diagnostizierbar sein. Hat diese in der Vergangenheit vergleichbare Angriffe getätigt, und sind die weitergeleiteten E-Mails und eventuell weitere Daten der Betroffenen andernorts auffindbar (z. B. im Darknet), dann liegen durchaus Hinweise auf ein hohes Risiko einer Persönlichkeitsverletzung der Betroffenen vor, und es sollte eine Meldung an die datenschutzrechtlichen Aufsichtsbehörden nicht unterlassen bleiben.

Praxisbeispiel 3: Gefälschte Rechnung (social engineering)

Ein Unternehmen kriegt eine Rechnung seines Lieferanten in der Schweiz. Die Rechnung wirkt 100% echt, die Zahlungsangaben leiten weiter auf ein Revolut-Konto in Litauen. Auch wenn der letzte Aspekt hätte Verdacht wecken müssen (der Lieferant in der Schweiz dürfte üblicherweise eine Bankverbindung aus der Schweiz angeben), bezahlt das Unternehmen eine Rechnung von CHF 20 000.–. In einem späteren Kontakt mit dem Lieferanten lässt sich feststellen, dass dieser Opfer einer Cyberattacke geworden ist. Seine Systeme wurden von Hackern infiltriert, deren Rechnungen als Vorlage für gefälschte Rechnungen verwendet und dem Unternehmen zugestellt. Das Unternehmen hat somit CHF 20 000.– fälschlicherweise auf das Revolut-Konto des Angreifers überwiesen. Ein immediate Kontaktaufnahme mit der Revolut-Bank in Litauen ergibt, dass der Kontoinhaber in Ungarn ansässig war und das Geld bereits abgehoben wurde. Dessen Identität ausfindig zu machen, gestaltet sich schwierig, weil die Bank nur auf dem Rechtshilfeweg bereit ist, Strafbehörden die Identität des Täters offenzulegen.

Es handelt sich hier um ein klassisches Betrugsschema, sogenanntes Social Engineering mithilfe von IT-Technologie (Hacken und Fälschen). Rechtlich betrachtet liegt beim Opfer (Unternehmen) gar kein Cyberangriff vor. Vielmehr war der Lieferant Opfer eines Cyberangriffs und das Unternehmen eher indirekt davon geschädigt als Opfer eines Betrugs. Eine Meldepflicht aus datenschutzrechtlicher Sicht besteht für das Unternehmen nicht. Vielmehr werden seine Bemühungen bei der Ausfindigmachung des Täters beschränkt, die sich in internationalen Betrugsfällen strafrechtlich als schwierig und langwierig erweisen. Der Lieferant hingegen wird sich mit der Frage auseinandersetzen müssen, ob er selbst einer datenschutzrechtlichen Meldepflicht untersteht.

Fazit: Sich zu stellende Fragen

Wie die bisherigen Beispiele gezeigt haben, gibt es keine schwarz-weisse Richtschnur, die Meldepflicht einer Cyberattacke rechtlich zu beurteilen. Im Zweifel können solche Meldungen auch präventiv erfolgen, ohne sicher zu sein, ob ein gesetzlich «hohes Risiko» besteht oder nicht. Zu überprüfen ist erst mal der genaue technische Vorgang des Angriffs (Auf welche Daten wurde unbefugt zugegriffen? Sind es überhaupt personenbezogene Daten oder reine Geschäftsdaten? Wurde überhaupt zugegriffen? War nur ein lokaler Laptop eines Mitarbeiters betroffen, oder fand ein Zugriff auf die ganze Systemumgebung des Unternehmens statt?) und hernach die Qualifikation der betroffenen Daten (Wie identifizierbar/individualisierbar sind Betroffene? Wie sensitiv sind die unbefugt zugegangenen Daten? Wurden Schutzmassnahmen zugunsten der Betroffenen getroffen, welche die Risiken für sie möglicherweise doch tiefer erscheinen lassen?). Wie eingangs geschildert, ist der Umstand, dass der Vorfall noch nicht technisch detailliert rekonstruiert werden konnte, kein überzeugendes Argument, um von einer Meldung an die Datenschutzbehörden abzusehen. Vielmehr ist es in der Praxis üblich und von den Behörden auch durchwegs akzeptiert, eine Art «provisorische Meldung» einzureichen unter dem Vorbehalt, dass diese später noch mit definitiven Abklärungen weiter ergänzt wird. Die Illiquidität eines Sachverhalts mag zwar ein längeres Zuwarten für gewisse Zeit rechtfertigen, doch sollte bei der plausiblen Wahrscheinlichkeit eines Angriffs lieber eine provisorische Meldung eingereicht und später konkretisiert werden. Nicht ausser Acht zu lassen sind spezialgesetzliche Meldepflichten, z. B. für regulierte Banken gegenüber deren Aufsichtsbehörden, welche unabhängig von konkreten Risiken gelten. Ferner ist auch separat zu prüfen, ob eine Meldung gegenüber Vertragspartnern/Kunden aus Sorgfalts- oder Schadensminderungspflichten geboten sein könnte, damit Letztere keine weiteren Folgeschäden erleiden könnten.

CHECKLISTE

- Was ist vorgefallen? Liegt ein unbefugter Datenzugriff (Breach) oder eine Kompromittierung von Personendaten überhaupt vor? Diese Frage ist im Zusammenarbeit mit IT-Verantwortlichen des Unternehmens und/oder externen Forensikern zu suchen.
- Falls ja, welche Art und Quantität von personenbezogenen Daten ist überhaupt betroffen? Liegen besonders schützenswerte Daten vor? Wie viele solcher Daten sind betroffen?
- Sind die betroffenen Kunden- oder z. B. Mitarbeiterdaten in der Schweiz oder in der EU ansässig? Je nach Antwort ist unter Umständen auch die DSGVO anwendbar und sind Meldungen in der EU nahegelegt.
- Wie weit identifizierbar oder individualisierbar sind Betroffene durch den Vorfall (Stichwort: Identifier und Umfang Daten) überhaupt?
- Liegt ein hohes Risiko der Verletzung personenbezogener Daten vor? Sind diese Daten gegebenenfalls auffindbar im Darknet (d. h. wurden konkret für Verletzungen eingesetzt)? Ist etwas über die Angreifergruppierung und bisherige Angriffe bekannt?
- Ist das Unternehmen speziell reguliert? Zum Beispiel eine Bank, die verschärften, spezialgesetzlichen Meldepflichten gegenüber Aufsichtsbehörden untersteht?
- Wurden Betroffene vom Vorfall informiert? Könnte man daraus schliessen, dass diesen hierdurch Schutz vor einer allfälligen Verletzung gewährt ist und darum für sie kein «hohes Risiko» besteht?
- Illiquidität des Sachverhalts (unklare Kenntnis über den genauen Hergang des Vorfalls) ist kein Freipass für die Unterlassung einer Meldung. Vielmehr kann auch eine «provisorische Meldung» erfolgen, die später noch konkretisiert bzw. ergänzt werden kann.

AUTOR

Dirk Spacek ist Partner und Co-Verantwortlicher der Praxisgruppen TMC und IP. Er befasst sich vornehmlich mit neuen Geschäftsmodellen im Medien-, Internet- und Technologiesektor, der Datenvermarktung und dem Immaterialgüterrecht.

IMPRESSUM

Verlag WEKA Business Media AG
Hermetschloostrasse 77
CH-8048 Zürich
www.weka.ch

Herausgeber Stephan Bernhard

Redaktion Marco S. Meier

Korrektorat Margit Bachfischer M.A., Bobingen

Layout/Satz Tonio Schelker

Publikation 10 × jährlich, Abonnement: CHF 98.– pro Jahr, Preise exkl. MWST und Versandkosten.
Als digitale Publikation erhältlich unter: www.weka-library.ch

Bildrechte www.istockphoto.com

Bestell-Nr. 9231