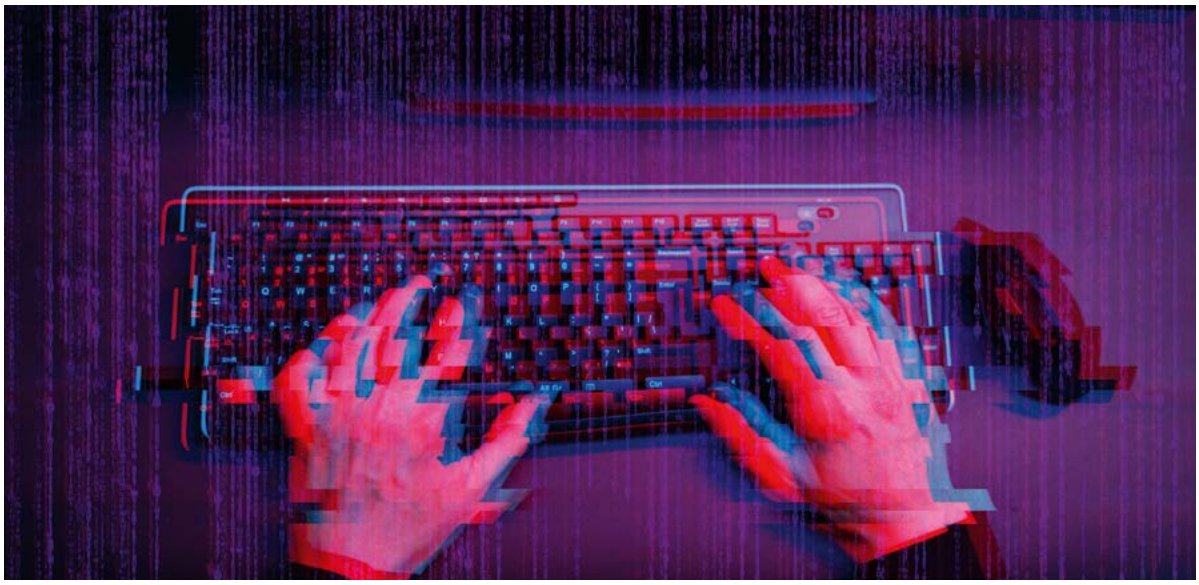
HACKER IM NETZ! WAS JETZT TUN?

Übersicht mit Handlungsempfehlung für den Fall der Fälle aus drei Blickwinkeln

Robin Brocks, Dr. Hauke Hansen, Suntka von Halen



Zu den größten Risiken, denen Unternehmen und Organisationen derzeit ausgesetzt sind, gehören Cyberattacken, die auf Daten und die Verfügbarkeit von IT-Systemen abzielen. Bereits 2019 erwarteten Experten, dass für das Jahr 2021 die Schäden durch Ransomware allein weltweit bei rund 20 Milliarden Euro liegen würden, wobei hier immer noch ein großes Dunkelfeld existiert.[1] Die wirtschaftlichen Einbußen durch gestohlene personenbezogene und sonstige vertrauliche Daten sowie der Diebstahl von geistigem Eigentum sind schwer oder auch gar nicht bezifferbar.

Wenn ein Cyberangriff ein Unternehmen trifft, muss alles sehr schnell gehen. Cybervorfälle verursachen schnell geschäftskritische Auswirkungen, daher ist das damit verbundene Krisenmanagement eine gesamtunternehmerische Aufgabe. Die Erfahrung zeigt, dass zu häufig die Verantwortung der internen IT überlassen wird. Dabei sind Verfügbarkeit und Führung durch das Managementteam, einschließlich des CEOs, unabdingbar.

Incident Response

Sollte der begründete Verdacht bestehen, dass unberechtigte Dritte IT-Systeme einer Organisation übernommen haben, ist ein ruhiges und überlegtes Vorgehen für den Erfolg der Aufklärung von oberster Priorität. In diesem Fall gilt nichts zu überstürzen. Um den Kreis der Eingeweihten klein zu halten, sollten nur wenige Personen von dem Verdacht erfahren. Im nächsten Schritt sollte schnellstmöglich professionelle Hilfe hinzugezogen werden.

Denn nicht jedes Unternehmen hat ein eigenes *Incident-Response-Team*. Der aus dem Englischen übernommene Begriff bezeichnet die „digitale Feuerwehr", die bei einem Vorfall ausrücken muss. Unterstützen können hier Dienstleister, die in

[1] Vgl. Cybercrime Magazine, unter https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

der Regel über das notwendige Personal, Wissen und Equipment inklusive professioneller Software für die gängigen Betriebssysteme wie Windows, Unix und MacOS verfügen, um beispielsweise eine digitale forensische Untersuchung durchzuführen.

Die Auswahl eines solchen Dienstleisters richtet sich nach der Art des Vorfalls und den Zeitzonen, in denen an dem Fall gearbeitet werden soll. Ein kleiner, regionaler Anbieter besitzt beispielsweise eher nicht die notwendigen Fähigkeiten, um international tätige Unternehmen auf mehreren Kontinenten nach dem „*follow-the-sun*"-Prinzip unterstützen zu können. Die gleichzeitige Untersuchung von mehreren hunderttausenden Servern und Laptops ist global nur einer Handvoll von spezialisierten Incident-Response-Dienstleistern möglich.

Zu den ersten Schritten einer erfolgreichen Incident Response gehört **Sichtbarkeit**. Erst wenn klar ist, welche IT-Systeme überhaupt kompromittiert sind, kann die darauffolgende **Eindämmung** erfolgreich sein. An dieser Stelle kommt zumeist EDR Software (Endpoint Detection and Response) zum Einsatz, um automatisiert jede Art von Schadsoftware zu stoppen.

Die Erfahrung zeigt, dass Unternehmen oftmals keine vollständige Inventarisierung vorhandener IT-Systeme in ihren Netzwerken haben, was nicht nur im Ernstfall besonders nachteilig ist. Denn gerade „vergessene", aber noch eingeschaltete Systeme von längst eingestellten Projekten werden oft zum Einfallstor für Cyberangriffe, da diese auch nicht mehr aktualisiert und abgesichert werden.

Sodann empfiehlt es sich in den Unternehmen bereits vorhandene Ereignisprotokolle, die Details der Kompromittierung aufgezeichnet haben, auszuwerten. Aufzeichnungen von Firewalls, Betriebssystemen oder einem SIEM (Security Incident and Event Monitoring) enthalten häufig wichtige Hinweise auf die Art des Cyberangriffs.

Erst wenn Sichtbarkeit vorhanden und der laufende Cyberangriff gestoppt ist, beginnen *Incident-Response-Teams* mit der Suche nach den Gründen für die erfolgreiche Kompromittierung („Root Cause Analysis"). Ursächlich für erfolgreiche Cyberangriffe sind zumeist:

- Nicht aktualisierte Systeme, die mit dem Internet verbunden sind. Sobald eine neue Sicherheitslücke publik wird, beginnen professionelle Akteure mit der Suche nach verwundbaren Systemen, um darüber in Unternehmensnetze einzubrechen.
- Professionelle manipulierte E-Mails („Whale Phishing"), die von vorhandenen Sicherheitsprodukten nicht erkannt werden. Im Fokus stehen dabei oft Vorstände und Führungskräfte mit beruflichem Bezug zu Unternehmensfinanzen und Produktentwicklung.
- Nutzung von manipulierter Software, wobei der Hersteller der Software zuvor erfolgreich angegriffen wurde und nun die manipulierte Software samt ihrer digitalen Hintertüren an zahlreiche Kunden ausliefert. Dies ist eine sogenannte „Supply Chain Attack", die über die Lieferbeziehung zu Hunderten gleichzeitig betroffener Kunden führen kann. Anfang 2021 war dies beim Unternehmen Solarwinds der Fall und zahlreiche deutscher Organisationen waren durch die Nutzung der Software von Solarwinds zum Opfer von Ausspähung geworden.

In den meisten Fällen kann die Ursache für den Cyberangriff festgestellt werden. Fehlende Ereignisprotokolle, von den Angreifern gelöschte oder auch versehentlich vom Unternehmen selbst überschriebene Daten machen mitunter jedoch eine genaue Ursachenbestimmung unmöglich.

Am Ende der Untersuchung steht die Anfertigung eines schriftlichen Berichts des *Incident-Response-Dienstleisters*. Dieser enthält üblicherweise die Ergebnisse der Investigation, eine Zeitachse der Ereignisse und Empfehlungen an das Unternehmen, wie ein solcher Cyberangriff in Zukunft verhindert werden kann. Die empfohlenen Maßnahmen können sowohl technischer, organisatorischer als auch prozessualer Natur sein.

Rechtliche Meldepflicht

Neben der *Incident-Response* sind im Fall eines Angriffs auf die IT-Infrastruktur diverse rechtliche Fallstricke zu beachten.

Wenn – wie das bei Ransomware-Angriffen mittlerweile üblich ist – nicht nur die IT-Systeme verschlüsselt, sondern zuvor auch umfangreich Unternehmensdaten abgezogen wurden, darf der Datenschutz nicht außer Acht gelassen werden. Ein solches Datenleck – oder im Jargon der Datenschutz-Grundverordnung (DSGVO) „eine Verletzung des Schutzes personenbezogener Daten" – führt zum einen zu einer Meldepflicht bei der Datenschutzbehörde. Zum anderen müssen unter bestimmten Umständen sämtliche betroffenen Personen informiert werden, deren Daten in die Hände der Hacker gelangt sind. In der Regel handelt es sich dabei um Mitarbeiter, Kunden und Lieferanten.

Die Meldepflicht gilt ausnahmsweise nicht, wenn nur geringe Risiken für die Betroffenen bestehen, deren Daten abhandengekommen sind. Die demnach notwendige Gefahrenprognose muss das Unternehmen selbst treffen, und das sehr schnell: Denn zwischen Bekanntwerden des Vorfalls und der Meldung gegenüber der zuständigen Datenschutzbehörde dürfen maximal 72 Stunden liegen. Dabei befinden sich Verantwortliche in einer Zwickmühle. Denn einerseits kann die unterlassene Meldung mit hohen Bußgeldern von bis zu vier Prozent des Jahresumsatzes oder 20 Millionen Euro sanktioniert werden, wenn der Fall später doch der Behörde zur Kenntnis gelangt. Andererseits kann ein vorschnelles Melden von Datenpannen gefährlich sein. Da die Datenschutzbehörden im Anschluss an eine Meldung regelmäßig mehr oder weniger umfangreiche Auskünfte über die IT-Sicherheit im Unternehmen verlangen, laufen Verantwortliche Gefahr sich durch eine Meldung selbst „ans Messer zu liefern".

Zwar sieht das Bundesdatenschutzgesetz vor, dass Selbstanzeigen wegen Datenschutzvorfällen von den Behörden nicht für Bußgeldverfahren verwertet werden dürfen. Das wird von manchen Datenschutzbehörden aber ignoriert: So verhängte der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg bereits Bußgelder, die sich auf den Inhalt einer solchen Meldung stützten. Er hält die Regelung im Bundesdatenschutzgesetz für europarechtswidrig und sieht sich daran nicht gebunden.

Durchaus überraschend: Mängel bei der Datensicherheit bilden einen der häufigsten Gründe, aus denen Datenschutzbehörden Bußgelder aussprechen. Die Opfer werden also zur Kasse gebeten. Zwei der höchsten Bußgelder, die unter der DSGVO überhaupt verhängt wurden, betrafen gehackte Unternehmen. (Hotelkette Marriott, 110 Millionen Euro, Fluglinie British Airways 200 Millionen Euro, beide Bußgelder später stark reduziert). Insofern sind Unternehmen gut beraten bei einem Cyberangriff kritisch zu prüfen, ob tatsächlich eine Meldepflicht besteht.

Cyberversicherung

Auch die Inhaber einer Cyberversicherung sollten sich nicht vorschnell in Sicherheit wähnen. Solche Policen – noch vor wenigen Jahren von den Versicherern als mehr oder weniger aufwandsneutrale „Dreingabe" für ein vermeintlich theoretisches Risiko betrachtet – entpuppen sich für die Anbieter zunehmend als Kostenfalle. Dementsprechend ist mitunter die Neigung hoch den Versicherungsschutz abzulehnen. Hier lohnt ein genauer Blick in die Vertragsbedingungen, denn die Regelungen unterscheiden sich je nach Anbieter erheblich. So lassen sich IT-Sicherheitsvorfälle häufig auf menschliches Versagen zurückführen. Versicherern, bei denen der Einwand grober Fahrlässigkeit nicht ausgeschlossen ist, steht damit je nach Fallgestaltung ein relativ einfaches Vehikel zur Verfügung Zahlungen abzulehnen. Auch lassen sich Versicherungen vor Abschluss des Vertrages von den Unternehmen zusichern, dass bei ihnen ein umfassendes Informationssicherheitsmanagementsystem (ISMS) besteht. Zudem setzt der Deckungsschutz häufig den Einsatz ganz bestimmter, vom Versicherer benannter IT-Spezialunternehmen voraus. Diese können sich zwar unter Umständen tatsächlich als kompetente und hilfreiche Dienstleister erweisen. Gleichzeitig erhalten diese von der Versicherung mandatierten Dienstleister aber umfassenden Einblick in die IT-Infrastruktur des Unternehmens - und damit auch in etwaig bestehende Sicherheitsdefizite. Finden diese Schwächen Eingang in den forensischen Bericht, den solche Unternehmen in der Regel anfertigen, steht dem Versicherer mitunter eine wahre Fundgrube an Gründen zur Verfügung den Versicherungsschutz wegen grober Fahrlässigkeit abzulehnen.

Unternehmen, die keine dedizierte Cyberversicherung besitzen, sollten ihre konventionelle Sach- oder Haftpflichtpolice prüfen. Mitunter sind hierdurch Cyberschäden abgedeckt, denn viele Versicherungsbedingungen wurden entworfen, als mit derartigen Schäden noch nicht zu rechnen war und diese von den Versicherungen nicht ausgeschlossen wurden. Man spricht hier von Silent-Cyber-Risiken.

Lösegeldzahlung und Geldwäsche

Zwar streben die meisten Unternehmen an, ihre Systeme und Daten ohne die kostenpflichtige „Hilfe" des Angreifers, also ohne Zahlung des verlangten Lösegeldes, wiederherzustellen. Dies gelingt umso besser, je stärker die Backups und ihre Speicherintervalle geschützt sind. Auch die zentralen Anlaufstellen der Staatsanwaltschaften für Cybercrime raten von solchen Zahlungen ab, und es gibt natürlich auch keine Garantie dafür nach der Zahlung den „rettenden" Schlüssel zu erhalten.

Gleichwohl wurden im vergangenen Jahr mehrere Hundert Millionen Euro an Lösegeldern bezahlt. Das geschah oftmals auch zur Zufriedenheit des erpressten Unternehmens, da viele Hacker an einem „vertrauenswürdigen" Image interessiert sind und nach einer

Lösegeldzahlung tatsächlich die Schlüssel zur Entschlüsselung der Unternehmensdaten übermitteln und keine Nachforderungen stellen. Mit einer solchen Zahlung begeben sich Unternehmen aber rechtlich auf „dünnes Eis“. Denn mit einer solchen Zahlung werden die kriminellen Aktivitäten der Tätergruppe gefördert und begünstigt. Unter Umständen kann hierin auch eine illegale Geldwäsche liegen. Die Lösegeldzahlung an Tätergruppen aus Embargoländern kann zudem einen Verstoß gegen außenwirtschaftsrechtliche Vorschriften bedeuten. Schließlich sollten Unternehmen mit US-Niederlassungen ganz besonders vorsichtig sein. Hier bestehen Bestrebungen die Zahlung von Lösegeldern gänzlich zu verbieten.

Geschäftsgeheimisse

Darüber hinaus drohen Rechtsfolgen auf weiteren Feldern: Nicht selten gehen Unternehmen strenge Pflichten ein Geschäftsgeheimnisse – zum Beispiel von Geschäftspartnern – gegen unbefugten Zugriff zu schützen. Mitunter verpflichten sich Unternehmen im Rahmen von Non-Disclosure-Agreements sogar dazu den Bruch eines solchen Geheimnisses an den Partner aktiv zu melden. Bei Verletzung drohen Vertragsstrafen.

Umgekehrt droht auch der rechtliche Schutz eigener Geschäftsgeheimnisse verloren zu gehen, denn das Geschäftsgeheimnisgesetz schützt nur solche Geheimnisse, die angemessen gegen unbefugten Zugriff gesichert sind. Bei einem Cyberangriff könnte sich also herausstellen, dass keine angemessenen Schutzmaßnahmen bestanden. Dann könnte das Unternehmen nicht einmal gegen einen Konkurrenten vorgehen, der sich das Geheimnis – etwa ein geheimes Produktionsverfahren – aus dem Darknet verschafft hat, wo Erpresserbanden ihre digitale Beute gern veröffentlichen, um Druck auf das bestohlene Unternehmen auszuüben.

Kommunikation im Krisenmanagement

Strategisches Ziel der Kommunikation im Krisenmanagement ist der langfristige Reputationsschutz. Aufgabe des Teams ist für konsistente Informationen und kontinuierliche Updates an interne und externe Zielgruppen zu sorgen und Sprechfähigkeit sowie die Kommunikationshoheit des Unternehmens sicherzustellen.

Zu Beginn der Response-Phase liegt die Priorität auf Schnelligkeit: Ein erstes kurzes Holding Statement muss den aktuell verfügbaren Sachstand enthalten und kann proaktiv oder auf Anfrage herausgegeben werden. Wichtigstes Ziel in dieser Phase ist das Unternehmen als aktiven Ansprechpartner zu etablieren, um die Kommunikationshoheit sicherzustellen und Gerüchte zu vermeiden.

Während parallel die wichtigsten Fragen und Antworten aufbereitet werden, sorgt das Kommunikations-Team dafür, dass sämtliche Kontaktpersonen des Unternehmens nach innen und außen – zum Beispiel im erweiterten Management, im Kundenservice oder im Vertrieb – das Holding Statement vorliegen haben und damit erste Anfragen beantworten können. So früh wie möglich sollte auch eine allgemeine interne Information folgen, die den Mitarbeitenden bei Bedarf Verhaltensregeln an die Hand gibt und zusätzlich Ansprechpartner im Kommunikationsteam für externe Anfragen nennt.

Nach Veröffentlichung einer Cyberattacke melden sich Mitarbeitende, Kunden, Journalisten und auch eine interessierte Öffentlichkeit mit unterschiedlichsten und teils sehr individuellen Fragen, dementsprechend müssen alle Touchpoints im Unternehmen so bald wie möglich Gesprächsleitfäden und FAQs bekommen, die kontinuierlich aktualisiert werden. Sie müssen zudem den Eskalationsprozess für besondere Anfragen kennen und diesen idealerweise trainiert haben.

Konsistenz und Kontinuität in der Kommunikation

Nach der zügigen ersten internen und externen Information sind Kontinuität und Konsistenz in der nächsten Phase Prioritäten für die Kommunikation. Die Forensik wird jetzt unter Umständen bereits einen besseren, wenn auch noch nicht abschließenden Blick auf die Situation haben. Nicht selten bringt diese Phase Erkenntnisse, die die erste Einschätzung noch einmal verändern – hier zeigt sich, wie wichtig es ist keine ungesicherten Infos herauszugeben oder Vermutungen zu formulieren.

In dieser Phase geht es darum Schritt für Schritt weitere verfügbare Informationen zur Verfügung zu stellen und einen angemessenen Dialog mit den jeweiligen internen und externen Zielgruppen aufzubauen. Mitarbeitende sollten über Intranet, Townhall- oder Teammeetings informiert werden. Wichtig ist hier nochmal eine Hilfestellung zum Umgang mit externen Anfragen oder Konversationen im persönlichen Umfeld, offline oder online sowie eine Social Media Policy zu geben. Kontinuierliches Monitoring von Print-, Online- und sozialen Medien hilft die korrekte Coverage der Fakten im Blick zu behalten und Spekulationen oder missverständliche Formulierungen rechtzeitig korrigieren zu können.

Schutz & Prävention

Längst schon geht es nicht mehr um die Frage, ob ein Unternehmen zum Opfer eines Cyberangriffs wird, sondern wann. Einen Notfallplan zu haben ist daher für jedes Unternehmen Pflicht. Die gute Nachricht ist, dass eine Vorbereitung auf die Bewältigung eines Cyberangriffs möglich ist. Für eine Prävention empfiehlt sich:

- Die Erstellung eines Incident-Response-Plans, der Zuständigkeiten, Aufgaben und Ansprechpartner in den Abteilungen des Unternehmens benennt inklusive einer guten und sorgfältigen Kommunikation.
- Allein schon aus Respekt gegenüber eigenen Teams und externen Zielgruppen ist eine gute und sorgfältige Kommunikation Pflicht: Anerkennen des Vorfalls (ohne verfrühtes Schuldeingeständnis), Begleitung des Krisenmanagements mit angemessenen Updates, Sichtbarkeit des CEO, verständliche Informationsschreiben, Aufzeigen von Learnings.
- Wenn es gelingt zu verdeutlichen, dass die Aufgabe ernst genommen wird, kann das Unternehmen eine Attacke nicht nur ohne größeren Reputationsschaden überstehen, sondern gestärkt daraus hervor gehen.
- Regelmäßige Übungen und Simulationen verschiedener Arten von Cyberangriffen und die notwendigen Maßnahmen zur Abwehr. Besonders sogenannte „Table-Top Exercises“ für technische Teams und auch für Manager haben sich als besonders effektiv erwiesen.
- Die Auswahl eines geeigneten *Incident-Response-Teams*, das über einen „Retainer“ genannten Vertrag kurze Reaktionszeiten und eine 24x7x365-Bereitschaft garantiert.
- Der Abschluss einer Cyberversicherung, die zumindest einen Teil der enormen Kosten übernimmt, die bei einem Cyberangriff entstehen können.

Über die Autoren

Dr. Hauke Hansen

ist Rechtsanwalt und Experte für Cybersicherheit, IT-Recht und Datenschutz. Er entwirft CyberSecurity-Strategien, um Unternehmer und Unternehmen vor Cyberattacken zu schützen und leistet ihnen Erste-Hilfe im Falle eines Cyberangriffs.

Robin Brocks

leitet das Incident Response Team von CrowdStrike für Europa, Afrika und dem Nahen Osten. Mit knapp 25 Jahren relevanter Berufserfahrung u.a. bei Lufthansa, Microsoft, Cisco und anderen großen Unternehmen ist er auch als Gutachter für IT-Forensik tätig. Er ist Reservist in der Digitalen Reserve der Bundeswehr und unterstützt auch hier gegen digitale Angriffe auf kritische Infrastrukturen.

Suntka von Halen

ist Director bei der Brunswick Group und Spezialistin für Restrukturierungs-, Krisen- und Veränderungskommunikation sowie Unternehmenspositionierung. Sie verfügt über langjährige Erfahrung in Beratung und auf Unternehmensseite und berät Kunden in internationalen Kommunikationsprojekten zu strategischen Fragen und in kritischen Situationen. Innerhalb von Brunswick's Cybersecurity-Praxisgruppe arbeitet sie als Co-Lead für Mandate in den Bereichen Crisis Preparedness und Crisis Response.