IT-Forensik

– den Tätern auf der Spur.

Ihr starker IT-Partner.
Heute und morgen.

BECHTLE

In den vergangenen Jahren hat sich die IT-Forensik als eigenständige forensische Disziplin für die Untersuchung von Straftaten im Computerumfeld etabliert. Anstatt nach Fingerabdrücken und DNS-Spuren suchen diese Experten nach verdächtigen Dateien und Unregelmäßigkeiten im Netzwerkverkehr. Das Ziel ist jedoch dasselbe: Vorfälle aufklären, die Opfer schützen und die Täter dingfest machen.

Am 6. September 2020 entdeckte die britische Newcastle University einen Angriff auf ihre Server: Hacker hatten zwei Tage zuvor die Sicherheitsmechanismen der Universität überwunden und die Ransomware DoppelPaymer installiert.[1] Die Malware verschlüsselte daraufhin die Datenträger und löschte die Backup-Files. Anschließend verlangten die kriminellen Eindringlinge für die Entschlüsselung und Freigabe der Daten ein Lösegeld. Ein Universitätssprecher sagte, die Säuberung und Wiederherstellung der Systeme werde mehrere Wochen in Anspruch nehmen. Die IT-Abteilung arbeite mit dem Information Commissioner's Office (ICO, der britischen Datenschutzbehörde) und der Polizei zusammen, um Hinweise auf die Täter zu finden.

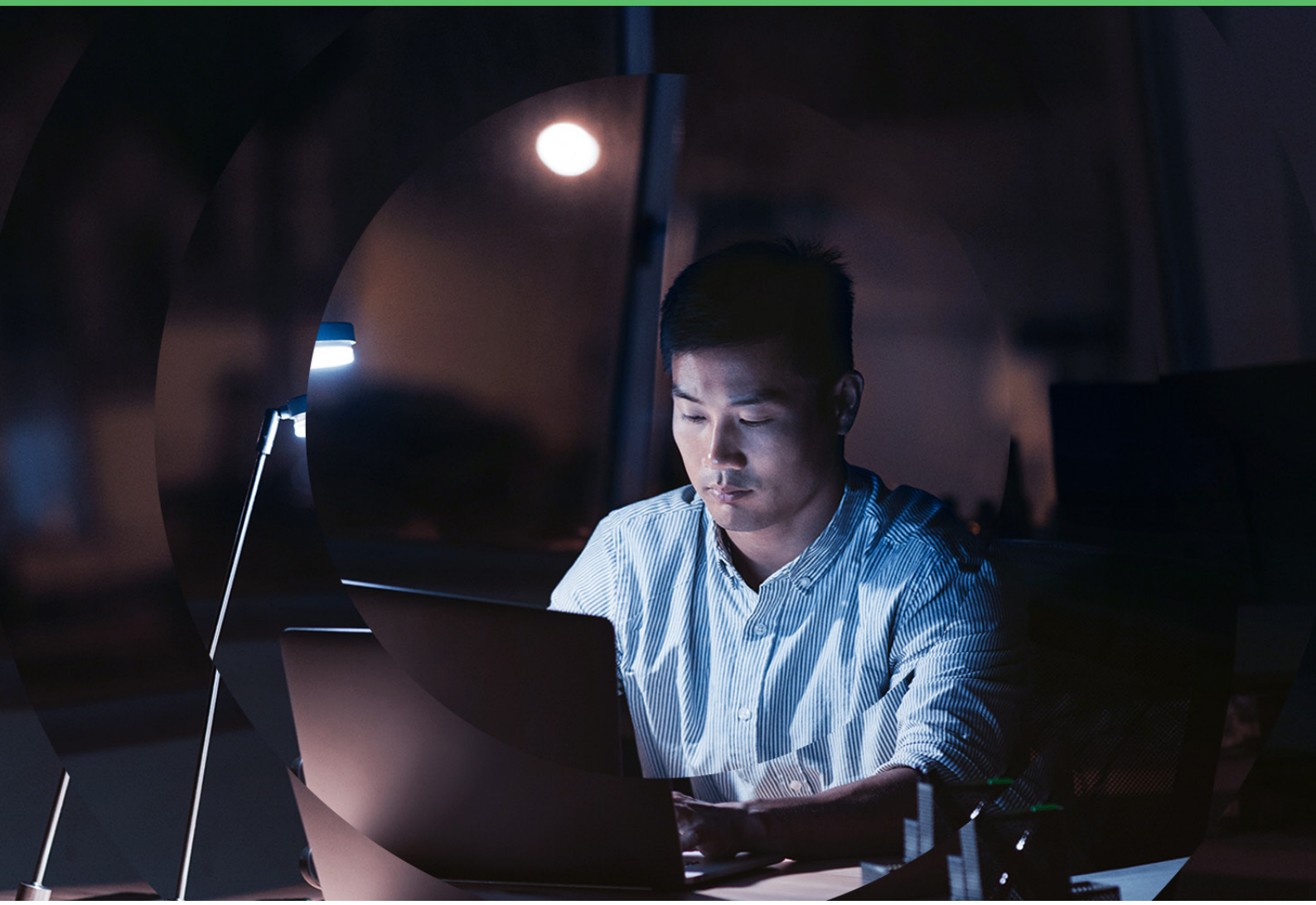
Wechsel nach Berlin: Die Firma BwFuhrparkService, die den Fahrdienst des Deutschen Bundestags bereitstellt, wurde Mitte August 2020 von einem Unbekannten gehackt.[2] Mit den Daten des Unternehmens ist es möglich, die Fahrten der Bundestagsabgeordneten nachzuverfolgen und sie damit eventuell zu erpressen. Außerdem könnten die Angreifer (und eventuell deren Kunden) einsehen, wer wann wohin gebracht werden möchte, und mit diesen Informationen Attentate planen. BwFuhrparkService gehört zu 75,1 % dem deutschen Verteidigungsministerium und zu 24,9 % der Deutschen Bahn. IT-Experten des Cyber Emergency Response Teams (CERT) der Bundeswehr waren vor Ort im Einsatz und ermittelten. Unterstützung bekamen sie dabei durch das CERT des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Das sind nur zwei Beispiele für erfolgreiche Hacker-Attacken. Wie viele es insgesamt pro Jahr sind, ist unbekannt – kaum ein Unternehmen, kaum eine Organisation geht mit Information zu Schäden durch Malware oder Datendiebstahl an die Öffentlichkeit. Die Security-Hersteller vermelden in ihren Threat Reports allerdings stetig steigende Zahlen an Angriffen mit Schadsoftware und anderen Versuchen, in Netzwerke einzudringen und an Daten zu kommen.

[1] **Irwin, Luke:** Newcastle University becomes latest ransomware victim as education sector fails to heed warnings. In: IT Governance Blog, 10.09.2020 (itgovernance.co.uk/blog/newcastle-university-becomes-latest-ransomware-victim-as-education-sector-fails-to-heed-warnings).

[2] **dpa:** Hackerangriff auf Bundeswehr-Fuhrpark und Bundestagsfahrdienst. In: Handelsblatt, 16.08.2020 (handelsblatt.com/technik/sicherheit-im-netz/it-hackerangriff-auf-bundeswehr-fuhrpark-und-bundestagsfahrdienst/26098924.html).

Cybercrime
– ein lukratives Geschäftsmodell.



In den meisten Fällen ist Geld das Motiv der Angreifer. Sie versuchen vor allem, mit Ransomware die Systeme von Unternehmen zu verschlüsseln, sodass die gespeicherten Daten nicht mehr lesbar sind. Erst nach Zahlung eines Geldbetrags (das englische Wort „ransom" bedeutet so viel wie „Lösegeld") wollen sie die Daten wieder freigeben. Die geforderten Beträge reichen bis hin zu einigen Millionen US-Dollar. In einem Interview mit der Süddeutschen Zeitung[3] erklärte die amerikanische IT-Sicherheitsexpertin Sherrod DeGrippo vom Security-Anbieter Proofpoint, dass sich in den vergangenen

[3] **Muth, Max:** „Fallen zwei oder drei Gangs weg, kommen fünf neue". In: Süddeutsche Zeitung, 07.09.2020 (sueddeutsche.de/digital/hacker-emotat-ransomware-degrippo-1.5023581).

Jahren ein regelrechter Markt für Hacker-Dienstleistungen entwickelt habe, getragen von Organisationen, die zunehmend wie seriöse Unternehmen auftreten. Manche haben sogar eine eigene Support-Abteilung, die beim Bitcoin-Transfer behilflich ist. Mithilfe solcher Gruppen kann heute jede Person einen gezielten Angriff gegen beliebige Unternehmen starten.

Teilweise versuchen die Kriminellen, die gestohlenen Daten auf dem Schwarzmarkt zu verkaufen. Das geschieht vor allem dann, wenn sie bei ihrem Angriff auch Passwörter erbeutet haben. Viele Datendiebstähle bei Unternehmen werden auch von Konkurrenten oder Geheimdiensten fremder Staaten organisiert. In solchen Fällen besteht das Ziel meist darin, neue technische Entwicklungen auszuspionieren. Und schließlich gibt es auch rein politisch motivierte Angriffe. Das bekannteste Beispiel dürfte der vermutlich vom israelischen Geheimdienst entwickelte Stuxnet-Virus sein, der im Jahr 2010 die iranischen Atomanlagen sabotierte.

In diesem Zusammenhang ist allerdings der Hinweis wichtig, dass die große Mehrzahl an Sabotageakten und unbefugten Zugriffen auf vertrauliche Daten nicht von außen kommt, sondern von innen, durch die eigenen Mitarbeiter. Häufig steckt dahinter Unzufriedenheit mit der Arbeitssituation oder dem Gehalt, manchmal ist auch einfach nur Neugier oder eine versehentliche Fehlbedienung der Auslöser. Die häufigste Ursache für den Diebstahl oder die Beschädigung von Unternehmensdaten ist, dass die Mitarbeiter Zugriffsrechte besitzen, die sie gar nicht haben sollten. In vielen Unternehmen werden neuen Mitarbeitern einfach die Rechte von Kollegen aus der gleichen Abteilung zugewiesen. In den folgenden Jahren kommen durch Abteilungswechsel oder Projektarbeit weitere Rechte hinzu, gleichzeitig bleiben die bestehenden Berechtigungen erhalten. Irgendwann hat ein Mitarbeiter dann Zugriffsrechte, die er schon längst nicht mehr benötigt.

Um die internen Datendiebstähle zu verhindern, ist ein strikt eingehaltenes und die komplette IT-Landschaft abdeckendes System an Zugriffsrechten erforderlich, eventuell mit Unterstützung einer Software für das Berechtigungsmanagement. Eine regelmäßige Rezertifizierung der Berechtigungen verhindert zudem, dass die Zahl der Zugriffsberechtigungen immer weiter zunimmt. Oberstes Ziel ist es, den Mitarbeitern Zugriff nur auf Daten zu gewähren, die sie tatsächlich für ihre Arbeit benötigen. Sollte es dennoch zu Datendiebstählen kommen, muss sichergestellt sein, dass die Zugriffe durch ein automatisch arbeitendes Reporting dokumentiert sind.

IT-Forensik:
Sichern, analysieren, vorbeugen.

Für Unternehmen, Behörden und andere Organisationen ist es wichtig, dass sie herausfinden, wie der Schaden in der IT entstehen konnte, wo die Schwachstellen im eigenen Sicherheitskonzept liegen und natürlich wer den Schaden verursacht hat. Für die Aufklärung solcher Fälle hat sich daher eine eigene Fachrichtung etabliert, die IT-Forensik. Sie ist „ein Teilgebiet der Forensik und beschäftigt sich mit der methodischen Analyse von Vorfällen auf IT-Systemen und der gerichtsverwertbaren Sicherung der Beweise".[4]

Die Geschichte der IT-Forensik reicht zurück bis in die 1980er Jahre, als mit dem Aufkommen der Personal Computer auch die ersten Computerverbrechen begangen wurden. Zunächst handelte es sich noch um vergleichsweise milde Vergehen wie etwa das Cracken von Kopierschutzmechanismen, begangen von Einzeltätern. Ab 2002/2003 begann sich die kriminelle Szene aber zu professionalisieren und in Gruppen zu organisieren. Deren vorrangiges Ziel war nun der Gelderwerb.

Gleichzeitig entwickelte sich aber auch die IT-Forensik weiter und begann nun, strukturierte Analysen zur Aufklärung und zur Beweissicherung durchzuführen. Methodisch folgen sie heutzutage immer dem gleichen Muster und umfassen die Schritte Identifizierung, Datensicherung, Analyse, Dokumentation und Aufbereitung. Die amerikanische Forensik hat dafür das S-A-P-Modell definiert; die Abkürzung steht für Secure (sichern), Analyse (analysieren) und Prevent (vorbeugen).

[4] **Luber, Stefan; Schmitz, Peter:** Was ist IT-Forensik? In: Security Insider, 12.11.2018 (security-insider.de/was-ist-it-forensik-a-774063).

- **Secure:** In der ersten Phase führen die Forensiker zunächst eine Bestandsaufnahme des Vorfalls durch und klären die Ausgangslage. Es folgt eine Sicherung aller Daten, die mit dem Vorfall in Verbindung stehen. Dabei achten die Spurensicherer darauf, dass die Zusammenhänge für einen Dritten klar erkennbar sind. Oft legen sie ein forensisches Duplikat der Daten an, etwa einer Festplatte mit Logdateien oder dem Code eines eingeschleusten Makros. Dieses Duplikat versehen sie dann mit einem Write-Blocker, der sämtliche Veränderungen an den Daten verhindert. Die auf diese Weise konservierten Daten sind später ein wichtiges Glied in der Beweiskette, wenn es darum geht, den Vorfall nachzuvollziehen und die Verursacher zu überführen. Gleichzeitig muss geklärt werden, ob das IT-System trotz der Kompromittierung weiter in Betrieb bleiben kann oder abgeschaltet werden muss.

- **Analyse:** Anschließend beginnt die Analyse der gesicherten Daten. Ziel ist es, den genauen Ablauf zu rekonstruieren, die Ursachen und die Verantwortlichen zu bestimmen. Die dabei angewendeten Methoden richten sich nach dem Sachverhalt im konkreten Fall und entsprechen jeweils dem neuesten Stand der Wissenschaft und Technik. Das Vorgehen der Ermittler muss jederzeit für Dritte nachvollziehbar sein.

- **Prevent:** Im letzten Schritt fassen die Forensiker die Ergebnisse in einem Bericht zusammen. Er enthält Informationen wie den chronologischen Ablauf des Vorfalls, die Identität des Täters und seine Ziele, den Umfang des Schadens sowie die Umstände, welche die Tat begünstigt haben. Darüber hinaus können die Analysten in ihrem Bericht aus diesen Fakten Schlussfolgerungen ziehen und Empfehlungen für das weitere Vorgehen geben. Auch diese Informationen müssen für Dritte logisch und nachvollziehbar sein.

Angreifer entdeckt – abwehren oder einfrieren?

Bei der Reaktion auf einen Angriff auf die IT-Strukturen muss eine schwierige Entscheidung getroffen werden. Zum einen hat für das Unternehmen in der Regel die unverzügliche Wiederherstellung des Geschäftsbetriebs höchste Priorität. Dazu muss die IT-Abteilung oder die Security die Ursache im Rahmen der Incident Response möglichst schnell und umfassend beseitigen. Die Forensiker hingegen benötigen oft etwas mehr Zeit, in der sie umfassend Beweise sammeln und sichern können. Ihnen ist daher tendenziell daran gelegen, den unsicheren Zustand noch eine Weile beizubehalten und ihn gewissermaßen zu konservieren.

Falls dieser Konflikt nach einem Angriff auf die Datenbestände eines Unternehmens auftreten sollte, muss man für die Lösung jeweils den konkreten Fall betrachten. Oft wird es technisch gar nicht möglich sein, einen bestimmten Zustand zu konservieren oder, wie oben beschrieben, zu duplizieren. In anderen Fällen, etwa nach der Entdeckung einer Malware, die sich im Netzwerk ausbreitet, wird es aus Sicherheitsgründen sogar ratsam sein, sofort Gegenmaßnahmen zu ergreifen und Systeme abzuschalten. Ansonsten besteht die Gefahr, dass die Malware weitere Systeme befällt und sich eventuell sogar auf die Netze von Zulieferern und Partnern ausbreitet. Der dadurch entstehende wirtschaftliche Schaden ist für die meisten Unternehmen nicht mehr auffangbar.

Im Konfliktfall ist es enorm hilfreich, einen erfahrenen externen Forensik-Experten hinzuzuziehen. Er kann besser abschätzen, welche Maßnahmen jetzt und hier Priorität haben, und dann in Abstimmung mit den internen Verantwortlichen die weiteren Schritte planen. Bechtle zum Beispiel bietet Unternehmen an, sie bei forensischen Untersuchungen zu unterstützen. (Weitere Informationen dazu finden sich am Schluss dieses Whitepapers.)

BSI-Leitfaden:
Gerichtsfeste Beweissicherung.

Das Bundesamt für Sicherheit in der Informationstechnik hat 2010 erstmals einen Leitfaden IT-Forensik[5] vorgelegt, eine mehr als 300 Seiten starke Anleitung für forensische IT-Analysen, die sich an die Betreiber von IT-Anlagen, Administratoren, Sicherheitsverantwortliche, aber auch Strafverfolgungsbehörden richtet. Der Leitfaden entwickelt ein praxistaugliches Modell für die IT-Forensik, aus der die Anwender Empfehlungen und Handlungsanweisungen ableiten können. Das Kompendium zeigt auf, welche Daten im System zu einem Vorfall gespeichert sind, und beschreibt die beweissichere Gewinnung und Aufbereitung. Um die Anleitungen konkret nachzuvollziehen, muss der Anwender keine spezielle forensische Software besitzen, stattdessen liefert der Leitfaden Kriterien, anhand derer sich forensische Produkte beurteilen lassen.

Von eminenter Bedeutung für die juristische Aufarbeitung eines Verbrechens ist, dass die gesammelten Beweise gerichtsverwertbar sind. Das bedeutet zunächst einmal, dass sie mit legalen Mitteln und auf legalem Wege erworben wurden. Zudem können bereits einfache Formfehler dazu führen, dass ein Gericht Beweise für unzulässig erklärt, da sie nicht auf korrekte Art und Weise erhoben wurden. Es empfiehlt sich daher unbedingt, bei einem Vorfall einen geschulten Forensiker heranzuziehen. Seine Aufgabe ist es dann unter anderem, eine schlüssige Beweiskette für die eventuelle Vorlage vor Gericht zusammenzustellen.

Mittlerweile hat die IT-Forensik mehrere Unterdisziplinen herausgebildet. So unterscheidet man heute etwa zwischen einer Computerforensik, die sich auf die Analyse von Hardware spezialisiert hat, und einer Datenforensik, die Datenbanken und andere Datenbestände untersucht. Außerdem gibt es weitere Spezialdisziplinen wie etwa eine Betriebssystem- oder Cloud-Forensik, die jeweils eigene Methoden entwickelt haben.

Zu den forensischen Methoden gehört nicht zuletzt die Wiederherstellung gelöschter Dateien. Dabei werden häufig Firmen hinzugezogen, die sich auf die Rettung beschädigter Datenträger spezialisiert haben. Andere Methoden umfassen etwa die Auswertung von Logdateien und die Live-Überwachung eines Computers oder Netzwerks.

[5] **BSI:** Leitfaden „IT-Forensik". Version 1.0.1, März 2011 (bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/IT-Forensik/forensik_node.html).

Unfall oder Vorfall?
Support-Fälle unter der Lupe.

Gemäß dem Leitfaden des BSI eignet sich die IT-Forensik nicht nur für die Aufklärung von Straftaten. Mit den Methoden dieser Disziplin lässt sich auch eine allgemeine Vorfallsbearbeitung einrichten – die Branche kennt das unter dem englischen Begriff „Incident Response". Wenn es Aufgabe der IT-Forensik ist, suspekte Vorfälle aufzuklären, dann stellt die Incident Response die grundsätzliche Frage: Liegt überhaupt ein böswilliger Eingriff in die IT vor? In den Blick geraten damit nicht nur verdächtige oder bestätigte Angriffe, sondern auch die Warn- und Alarmmeldungen, die jedes komplexere System ausgibt. Praktisch bedeutet das, dass IT-Forensik ein starkes Werkzeug bei der Behandlung von Support-Fällen ist.

Das BSI führt als Beispiel eine doppelt vergebene IP-Adresse in einem lokalen Netzwerk an. Ein solcher Fehler produziert in den Logdateien lange Listen mit Fehlermeldungen. Gleichzeitig sind eventuell einige Geräte oder auch ganze Netzwerkabschnitte nicht erreichbar. Die Suche nach dem Verursacher gestaltet sich jedoch recht schwierig, sie kann aber mit einem streng methodischen Vorgehen und den Mitteln der IT-Forensik beschleunigt werden. Erweist sich die Fehlkonfiguration schließlich als ein Versehen, kann die IT-Abteilung anschließend über Maßnahmen nachdenken, wie sich solche Störfälle in Zukunft vermeiden lassen. Sollte sich jedoch herausstellen, dass ein Mitarbeiter den Fehler absichtlich

herbeigeführt hat, um dem Unternehmen zu schaden, liegen dank des forensischen Vorgehens auch gleich die benötigten gerichtsverwertbaren Beweise vor.

Wichtig ist die forensische Aufklärung von Verbrechen im IT-Umfeld sowohl in wirtschaftlicher wie auch in rechtlicher Hinsicht. Ökonomisch gesehen ist es von höchster Bedeutung, möglichst schnell die Ursachen zu beseitigen, die zu dem Schaden geführt haben. Nur so kann sichergestellt werden, dass sich der Vorfall nicht wiederholt und der finanzielle Verlust noch größer wird.

Außerdem muss das Unternehmen klären, ob und welche Daten gestohlen wurden und welcher wirtschaftliche Schaden durch den Verlust entstanden ist. An dieser Stelle kommt der juristische Aspekt ins Spiel: Laut Art. 5 der Europäischen Datenschutzgrundverordnung (DSGVO) müssen personenbezogene Daten umfangreich geschützt sein. Wenn ein Unternehmen diesen Aspekt des Datenschutzes vernachlässigt hat, kann es im Fall eines Verlusts oder einer unrechtmäßigen Verarbeitung zur Verantwortung gezogen werden – was hohe Strafen nach sich ziehen kann. Die DSGVO sieht Geldstrafen von bis zu 20 Millionen Euro oder, im Fall eines Unternehmens, 4 % des Umsatzes des vorangegangenen Geschäftsjahres vor. Insofern ist es gut, wenn das Unternehmen im Fall eines erfolgreichen Hacker-Angriffs nachweisen kann, dass es die gespeicherten Daten bestmöglich geschützt hat, um zu verhindern, dass sie in fremde Hände gelangen.

Falls der Vorfall keine personenbezogenen Daten betrifft, kann das Unternehmen eine nüchterne Abschätzung des wirtschaftlichen Schadens vornehmen, und zwar sowohl für den aktuellen Fall wie auch für eventuelle Wiederholungen. Dabei spielt auch die Bedeutung der betroffenen Daten für den wirtschaftlichen Erfolg des Unternehmens eine Rolle. Wichtig ist, dass für eine solche Einschätzung die Managementebene des Unternehmens einbezogen wird. Gleichzeitig sollte die IT-Abteilung berechnen, was es kosten würde, die Sicherheitslücke zu stopfen, die den Vorfall ermöglicht hat. Im Zuge des sogenannten Vulnerability Managements, das sich mit Patches und generell dem Umgang mit allfälligen Verwundbarkeiten befasst, ist dann eine Aussage möglich, ob vorbeugende Maßnahmen, die eine Wiederholung verhindern können, überhaupt notwendig und rentabel sind.

Art. 5, Abs. 1f DSGVO

„Personenbezogene Daten müssen [...] in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen“.

Meldepflichten:
Die ersten 72 Stunden entscheiden.

Die DSGVO und andere Regelwerke etwa zum Schutz kritischer Infrastrukturen (KRITIS) schreiben nicht nur die Meldung von datenschutzrechtlich relevanten Vorfällen vor, sondern machen auch Vorgaben für die Organisation der Verantwortlichkeiten und die Abfolge, wer wann informiert werden muss. So muss laut DSGVO jedes Unternehmen, das in großem Maße personenbezogene Daten verarbeitet und/oder Daten verarbeitet, deren Missbrauch besonders einschneidend für die Betroffenen wäre, einen betrieblichen Datenschutzbeauftragten bestellen. Sobald eine Verletzung des Datenschutzes festgestellt wird, ist er sofort zu benachrichtigen.

Außerdem ist das Unternehmen verpflichtet, innerhalb von 72 Stunden eine Meldung bei der zuständigen Datenschutzbehörde zu machen. Die DSGVO lässt dabei nur eine Ausnahme zu, nämlich wenn der Vorfall „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt" (Art. 33, Abs. 1 EU-DSGVO). Dazu ist wiederum eine Risikoabschätzung erforderlich, die laut Gesetz ohnehin Vorschrift ist. Im Rahmen dieser Abwägung müssen die Verantwortlichen klären, ob eine Schutzverletzung personenbezogener Daten stattgefunden hat, wie viele Personen davon betroffen sein könnten und um welche personenbezogenen Daten es sich genau handelt.

An dieser Stelle kommt abermals die IT-Forensik ins Spiel, da ihre Methoden sich hervorragend dazu eignen, diese Fragen schnell und effizient zu klären. Da der Gesetzgeber den Unternehmen für die Meldung lediglich 72 Stunden Zeit gibt, sollten sie möglichst sofort nach Entdeckung eines datenschutzrelevanten Vorfalls reagieren und einen Forensik-Experten hinzuziehen. Hilfreich ist auch ein vorsorglich aufgestellter Reaktionsplan, der definiert, was einen Datenschutzvorfall ausmacht, und bestimmten Mitarbeitern klar festgelegte Rollen und Aufgaben zuweist. Das erleichtert nicht nur die Einhaltung der Meldefrist, sondern unterstützt auch die IT-Abteilung bei der Analyse und der Sicherung von Beweisen.

Die gesammelten Informationen gehen zunächst an den Datenschutzbeauftragten, der sie dann an die zuständige Behörde weiterleitet. Sein Bericht sollte auch die Sicherheitsmaßnahmen aufführen, die das Unternehmen zuvor getroffen hatte, um Schutzverletzungen zu verhindern.

Doch mit diesem Bericht ist die Informationspflicht in den meisten Fällen noch nicht vollständig erfüllt. Sollte sich nämlich herausstellen, dass aufgrund der Datenschutzverletzung voraussichtlich ein hohes Risiko für die betroffenen Personen besteht, müssen auch diese gemäß Art. 34 EU-DSGVO „unverzüglich" benachrichtigt werden. Das ist beispielsweise dann erforderlich, wenn Hacker Kontodaten oder Passwörter abgezogen haben. Ausnahmen von dieser Pflicht gibt es lediglich dann, wenn die Daten für den Angreifer unzugänglich sind, beispielsweise weil sie sicher verschlüsselt wurden, wenn das Risiko mittlerweile nicht mehr besteht oder die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall muss stattdessen eine öffentliche Bekanntmachung oder eine vergleichbare Maßnahme erfolgen.

Sonderregelungen für kritische Infrastrukturen.

Bereits vor der Datenschutz-Grundverordnung, nämlich im Juli 2015, trat das IT-Sicherheitsgesetz in Kraft. Es verpflichtet die Betreiber kritischer Infrastrukturen (KRITIS), Sicherheitsvorfälle dem BSI zu melden. Zu dieser Kategorie von Unternehmen und Organisationen gehören große Betriebe aus dem Energiesektor, der Wasserwirtschaft, der Informationstechnik, aus dem Bereich Gesundheit und Ernährung, aus dem Finanz- und Versicherungswesen sowie Telekommunikationsbetreiber. Für diese Sektoren hat die Bundesregierung Schwellenwerte definiert, um die jeweils wichtigsten Unternehmen zu identifizieren. Diese werden in eine regelmäßig aktualisierte Liste aufgenommen und entsprechend benachrichtigt.

Für die KRITIS-Unternehmen gelten bei Datenschutzverletzungen besonders strenge Meldepflichten. Sie müssen eine Kontaktstelle angeben, die im Falle eines Cybersecurity-Vorfalls der Behörde ein Formular mit weiteren Informationen übermittelt. Ein Beispielformular des BSI[6] zeigt, wie die Meldung etwa bei der Entdeckung der Ransomware Locky aussehen müsste. Auch beim Ausfüllen dieses Formulars kann die IT-Forensik wertvolle Hilfe leisten und beispielsweise Informationen dazu liefern, was die Ursache für den Ausfall eines Systems war.

[6] **BSI:** Muster eines ausgefüllten Meldeformulars für KRITIS-Betreiber gemäß § 8b Absatz 4 BSIG (bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Meldeformular_BSIG8b_Muster.pdf).

Forensische Unterstützung durch Bechtle.

Setzen Sie sich einfach mit uns in Verbindung und erfahren Sie mehr zum Thema oder über unsere vielen Services und Lösungen rund um das Thema IT-Security:

security.ls@bechtle.com

Die IT-Forensik ist eine hochkomplexe Disziplin, die erfahrene Spezialisten erfordert. Der Zeitdruck, den etwa eine Ransomware-Attacke erzeugt und der durch die DSGVO-Bestimmungen zusätzlich verschärft wird, macht ein langsames Herantasten an das Thema praktisch unmöglich. Learning by Doing ist keine Option. Die Festanstellung eines Forensik-Experten ist jedoch lediglich für größere Unternehmen und Konzerne sinnvoll, die mehrere Male im Jahr das Ziel von Hacker-Angriffen sind und regelmäßig Störfälle und Datenschutzverletzungen verzeichnen. Kleine und mittelständische Firmen sind besser beraten, wenn sie auf externes Know-how zurückgreifen. Das gilt umso mehr, als Forensiker zu den meistgesuchten IT-Spezialisten überhaupt gehören und daher entsprechend teuer sind.

Die Bechtle AG hat zur Unterstützung ihrer Kunden beim Thema IT-Sicherheit in den vergangenen Jahren das Bechtle Competence Center Cyber Crime & Defense aufgebaut. Hier arbeiten auch Spezialisten für IT-Forensik, die Unternehmen und Organisationen zur Hand gehen, wenn sie ein Sicherheitskonzept formulieren und umsetzen müssen. Sie beraten auch zum Einsatz konkreter Tools, die zum Beispiel mit künstlicher Intelligenz den Netzwerkverkehr überwachen und automatisch auf verdächtige Aktivitäten hinweisen.

Ihr starker IT-Partner.
Heute und morgen.

BECHTLE