ComplianceBusiness
Ausgabe 2 // Juni 2019

Schutzlos ausgeliefert?

Cybersecurity hat kein Erkenntnisproblem, sondern ein Handlungsproblem: Risikofaktor Mensch

Von Bodo Meseke

Wurde Ihr Unternehmen schon einmal gehackt? Falls ja, wissen Sie, dass klassische Schutzmaßnahmen wie Firewalls nicht ausreichen. Falls nein, sollten Sie sich darauf vorbereiten, dass es jederzeit passieren kann.

„Heute gibt es nur noch zwei Arten von Unternehmen: jene, die wissen, dass sie gehackt wurden, und jene, die das noch feststellen werden." Dieser Satz des früheren FBI-Direktors James Comey ist nach wie vor hochaktuell. Um es deutlich zu sagen: Einen 100%igen Schutz gibt es nicht und wird es vermutlich nie geben. Dies ist jedoch kein Grund zu resignieren. Denn auch Ihr Unternehmen kann sich gegen Cybergefahren wappnen. Sie sollten das Thema nur zügig angehen.

Cybersecurity wird immer wichtiger – das gilt für alle Branchen und Geschäftsbereiche. Wer der Ansicht ist, dass Hackerangriffe nur virtuellen Schaden anrichten, hat die vergangenen Jahre verschlafen. Denn das ist längst nicht mehr so: Als Hacker zum Beispiel die Steuerung eines Hochofens bei einem deutschen Stahlhersteller kaperten, hat sich das unmittelbar auf die laufende Produktion ausgewirkt. Dabei kam dieser Angriff keinesfalls aus dem Nichts: Mitarbeiter erhielten gefälschte E-Mails, sogenanntes Spear-Phishing, und so hackten die Angreifer das Büronetzwerk der Fabrik. Von dort aus arbeiteten sie sich bis zu den netzgebundenen Steueranlagen vor, und es gelang ihnen, diese während des laufenden Betriebs zu manipulieren. Ein Hochofen ließ sich dadurch nicht geregelt herunterfahren, wodurch die Anlage stark beschädigt wurde.

Das Thema Cybercrime ist aktuell wie nie und hat sich mittlerweile zu einem illegalen Wirtschaftszweig ausgewachsen, denn Kriminalität im Internet ist vor allem eines: extrem lukrativ.

Was lernen wir daraus? Der Faktor Mensch bleibt neben technischen Aspekten ein großes Risiko und Einfallstor. Klassische Sicherheitsmaßnahmen scheitern, wenn Mitarbeiter Zugangsinformationen weitergeben oder unbedarft auf verlockende Mailanhänge klicken. Solche Angriffe können nur abgewehrt werden, wenn die

ComplianceBusiness
Ausgabe 2 // Juni 2019

Aufgaben und Funktionen risikokritischer Abteilungen strikt getrennt bleiben.

Erkenntnis- oder Handlungsproblem?

Die Sicherheitsmaßnahmen reichen noch lange nicht aus – dessen sind sich auch Firmen in Deutschland bewusst, die Vorreiter der Technologiebranche. Das belegt eine EY-Studie aus dem Jahr 2017 (Datenklau: Virtuelle Gefahr, echte Schäden. Eine Befragung von 450 deutschen Unternehmen). Cybersecurity hat ganz offensichtlich kein Erkenntnisproblem, sondern vielmehr ein Handlungsproblem. Führungskräfte wissen, dass es Sicherheitslücken gibt, trotzdem reagieren sie zu wenig. Für manche Entscheider ist Cybersecurity nach wie vor ein reines Technikthema, das zwar mit jedem bekannt gewordenen Angriff kurz hochkocht, dann aber rasch wieder von der Agenda verschwindet. Dass auch die eigene Organisation massiv gefährdet ist, scheint in den Köpfen der Chefs nicht nachhaltig präsent zu sein.

Denn Führungskräfte stecken in einem Dilemma: Ausgaben für IT-Sicherheit werfen keine Gewinne ab, jedenfalls nicht auf den ersten Blick. In der Logik kurzfristiger Profitabilität ist der Aufbau einer Cybersecurity-Infrastruktur also unattraktiv. Prävention, Schutz und Vorsicht waren noch nie wirklich sexy. Dabei kostet ein Datenleck Unternehmen im Schnitt rund 3 Millionen Euro, wie das Ponemon-Institut in einer Studie zu Cyberrisiken errechnet hat. Oft nämlich dauert es mehrere Wochen, bis sich der Betriebsablauf nach einem Angriff wieder normalisiert.

Digitale Vernetzung – Chance und Risiko

Hinzu kommt Folgendes: Im Zuge der Datenschutzgrundverordnung (DSGVO) können Strafen von bis zu 4 Prozent des Jahresumsatzes verhängt werden, wenn sich etwa bei einem Datenleck herausstellt, dass Unternehmen falsch auf Bedrohungen reagiert haben. Abgesehen davon, ist die Frage nach Datensicherheit ganz grundsätzlich mit dem Ziel einer langfristig gesunden Unternehmensentwicklung verbunden.

Nicht nur Nationalstaaten oder globale Konzerne sind mögliche Ziele digitaler Kriegsführung (Cyberwarfare). Ebenso betroffen sind kleine und mittlere Unternehmen, die stark in Forschung und Entwicklung investieren. Sie stecken in einer Zwickmühle: Viele wollen sich schnell und umfassend digitalisieren, um in der Industrie 4.0 Schritt zu halten. Computer, Produktionsanlagen, Logistik, Roboter, Wartungsfirmen, Lieferanten – alle sollen digital miteinander kommunizieren können. Schnittstellen zu schaffen ist dabei nicht das Problem. Vor lauter Euphorie wird aber oft vergessen, ein umfassendes Sicherheitskonzept zu integrieren. Hierbei fühlen sich kleine und mittlere Unternehmen oft alleingelassen.

Dabei ist die Sicherheitsfrage umso relevanter, je mehr Geräte miteinander vernetzt werden. Heute haben viele Unternehmen ihre IT ausgelagert und vertrauen auf die Clouds von Dienstleistern, die höhere Sicherheitsstandards bieten. Hacken Angreifer jedoch einen IT-Spezialisten, legen sie damit zugleich etliche Unternehmen lahm.

Digitale Forensik als Lösungsansatz

In Sachen Informationssicherheit stehen wir vor einem Paradigmenwechsel. Das bisher führende Prinzip "Prevent & Protect" (abwehren und schützen), tritt gegenüber einem "Detect & Respond" (aufklären und antworten) zurück. Die Anforderungen an IT-Systeme steigen stetig: Sie müssen heute viel mehr leisten, als nur Gefahren aus der Defensive heraus abzuwehren. Durch aktives Suchen sollen Eindringlinge möglichst früh erkannt werden. Gibt es Spuren verbrecherischen Handelns, so ist dieses nachzuverfolgen, und es gilt – falls der Angriff noch läuft –, den Schaden einzudämmen. Ganz augenscheinlich muss die IT stets gut gerüstet sein, falls Eindringlinge ihre Defensivsysteme überwinden. Dies ist durchaus vergleichbar mit einer Erkältung: Wir wissen, dass sie uns immer wieder erwischen wird. Proaktive Prävention ist hier der einzige Weg.

Zwar gibt es nicht die eine goldene Lösung zur ganzheitlichen Bekämpfung von Cybercrime, doch bietet die Digitale Forensik ein wertvolles Instrumentarium. Sie wird auch als Computer- oder IT-Forensik bezeichnet und hat sich als Teilgebiet der kriminalistischen Forensik etabliert. Mit dieser Disziplin gelingt es, digitale Verbrechen gerichtsfest nachzuweisen. Zum Verständnis ein Bild: An einem realen Tatort werden Fingerabdrücke und andere Spuren gesichert. IT-Forensiker arbeiten ähnlich, sie suchen in der virtuellen Welt nach digitalen Spuren und Hinweisen für eine Straftat. Tatort ist hier allerdings das Computernetzwerk, und als digitale Zeugen dienen Datenanalyseverfahren. Anstelle von Fingerabdrücken gibt es Hashwerte, das sind Zahlen- und Buchsta-

ComplianceBusiness
Ausgabe 2 // Juni 2019

benkombinationen, die einer bestimmten Datenmenge (etwa einem JPEG) eindeutig zugeordnet werden können. Wird daran etwas geändert, verändert sich auch der Hashwert. Als wesentlicher Teilbereich der Incident Response (Vorfallreaktion) verfügt die Digitale Forensik über wirkungsvolle Werkzeuge. Sie helfen dabei, digitale Störungen und Gefahren frühzeitig zu entdecken, einzudämmen und zu dokumentieren.

Suchen, erkennen, antworten

Eine Umstellung auf "Detect & Respond" ist für Unternehmen sinnvoll. Anstatt immer wieder und immer mehr Geld für einzelne Schutzmaßnahmen auszugeben, wird in ein leistungsfähiges und ganzheitliches System investiert. Denn exzellente Vorbereitung ist im Krisenmanagement (fast) alles. Insgesamt ist es leichter, diesen Paradigmenwechsel zu vollziehen, wenn sich das Management bereits mit dem Thema auseinandergesetzt hat. Das heißt übrigens nicht, dass Unternehmen das nötige Know-how unbedingt selbst aufbauen müssen. Digitale Forensik lässt sich wie eine Dienstleistung im Sinne von Security as a Service einkaufen. Hier kommen – je nach Bedarf und in Rücksprache mit den Verantwortlichen – ausgewiesene Experten hinzu, die den Boden für IT-forensische Analysen bereiten, Abteilungen einbinden und dann im Notfall schnell Maßnahmen mit dem Unternehmen umsetzen können.

Das Thema Cybercrime ist aktuell wie nie und hat sich mittlerweile zu einem illegalen Wirtschaftszweig ausgewachsen, denn Kriminalität im Internet ist vor allem eines: extrem lukrativ. Darauf sollten sich Entscheider in Unternehmen einstellen. Auch die Digitale Forensik muss mit den rasanten technologischen Entwicklungen mithalten, indem sie die neuesten Methoden von Hackern genau kennt und ihre Mechanismen fortlaufend anpasst. Nicht nur die globale Datenmenge wächst jedes Jahr, sondern auch die damit verbundenen Risiken. Um als Unternehmen in unserer digitalisierten Welt gewappnet zu sein, braucht es die richtige Mischung aus menschlicher und technischer Kompetenz.

Sie sollten sich also fragen, was wichtiger ist: den maximalen kurzfristigen Gewinn zu erzielen und dafür ernsten Gefahren ausgesetzt zu sein oder einen Teil in den Schutz von Unternehmenswerten, geistigem Eigentum, Mitarbeitern – der eigenen Geschäftsfähigkeit – zu investieren? Zwar obliegt diese Entscheidung natürlich jedem Unternehmen selbst. Eine größere Sensibilität für digitale Gefahren und die Entwicklung eines adäquaten Notfallplans sind allerdings empfehlenswert, um im Ernstfall nicht kopflos und getrieben von externem Druck handeln zu müssen, sondern umsichtig und mit Augenmaß agieren zu können. Denn es geht nicht mehr nur darum, ob Ihr Unternehmen Opfer von Cybercrime wird, sondern darum, wie, wann und ob es gelingt, den Angriff frühzeitig zu erkennen und angemessen darauf zu antworten.

Bodo Meseke

Partner, Forensic & Integrity Services, Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft mbH, Frankfurt am Main

Bodo.meseke@de.ey.com

Was ist Digitale Forensik?

Die Digitale Forensik (auch IT- oder Computerforensik) identifiziert und analysiert kriminelle Handlungen unter Anwendung von Informationstechnologie. Kernelemente sind das gerichtsfeste Ermitteln, Sichern, Untersuchen und Dokumentieren digitaler Spuren. Zugleich dient die Arbeit eines IT-Forensikers dem Aufspüren von Lücken im IT-System. Spuren finden sich auf Festplatten in Computern ebenso wie auf Smartphones oder Smarthomegeräten. Standardisierte Techniken und Prozesse stellen sicher, dass die digitalen Beweise vor Gericht verwertbar sind. IT-Forensiker sind speziell ausgebildete Experten, deren Wissen sich wesentlich von dem eines IT-Administrators unterscheidet.

Hinweis der Redaktion: Mehr zu diesem Thema lesen Sie in dem Buch „Digitale Forensik. Praxiswissen Cybercrime für Manager“ von Bodo Meseke, das im Juni 2019 im Erich Schmidt Verlag erscheint.