Sophos-Serie zu IT-Sicherheit und Recht:

Der Chef haftet für alles! Oder?

IT-Security gelingt nicht nur mithilfe von Technologie, sondern beruht auch auf Bewusstsein für die Rechtslage, entsprechendem Verhalten und intensiver Aufklärung der Mitarbeiter. Auch diese können bei Security-Fehlverhalten unter Umständen persönlich haftbar gemacht werden.

Wiesbaden, 11. Oktober 2017 Je mehr Parteien und Prozesse durch einen IT-Sicherheitsfall betroffen sind – Unternehmen, Arbeitsabläufe, Lieferungen, Kunden etc. – desto komplexer werden die Rechtsverhältnisse. Wer haftet beispielsweise, wenn durch Fahrlässigkeit von Mitarbeitern Security-Vorfälle ausgelöst werden, die Schaden für das Unternehmen oder Dritte nach sich ziehen? Sophos beleuchtet gemeinsam mit Rechtsanwalt Sebastian Müller mögliche Szenarien.

Der Klassiker: Notebook verloren

Der Verlust des Notebooks ist ebenso bereits ein Klassiker in Sachen Datenverlust wie der acht- und arglos geöffnete E-Mail-Anhang mit schadhaftem Inhalt. Beide Beispiele können ernsthafte Folgen für das geschädigte Unternehmen, den auslösenden Mitarbeiter selbst sowie davon betroffene Dritte haben. Ein Beispiel: Das Notebook eines Außendienstmitarbeiters wird gestohlen. Auf dem Gerät befinden sich unverschlüsselt Vertriebsdaten, Angebote, Preiskalkulationen sowie Kundendaten. Die vertraulichen Daten werden vom Dieb gelesen und öffentlich gemacht oder verkauft. Das Unternehmen ist nun verpflichtet, sowohl die zuständige Aufsichtsbehörde als auch alle Kunden zu informieren, deren sensible Daten auf dem Notebook waren. Möglicherweise wird nun in bestimmten Fällen auf eine Klage verzichtet, etwa wenn keine kritischen Daten abhanden gekommen sind und kein hoher Schaden entstanden ist. Geht es jedoch um Firmengeheimnisse wie Konstruktionspläne oder Forschungsergebnisse können die Schadenersatzklagen in die Millionen gehen. „Als einfache vorbeugende Maßnahme gegen ein solches Szenario sollte aus technischer Sicht grundsätzlich eine Verschlüsselung der Laptop-Festplatten das Mittel der Wahl sein“, erläutert Michael Veit, IT-Sicherheitsexperte bei Sophos. „Was die Mitarbeiter angeht, so sollte der Arbeitgeber klare IT-Sicherheitsrichtlinien definieren, die auch den Umgang mit den eingesetzten Laptops und den darauf befindlichen Daten klar regeln und diese den Mitarbeitern unmissverständlich und nachweislich kommunizieren.“

Der Trend: Ransomware – sensible Daten in Geiselhaft

Ist im Falle des Laptops eine Verschlüsselung die beste Lösung zum Schutz, ist sie in einem anderen, zunehmend beliebten und ganz perfiden Szenario die Bedrohung: Ransomware. Von Cyberkriminellen als harmlos scheinender E-Mail-Anhang ins Unternehmen geschleust, entfaltet Ransomware seine schädliche Wirkung, sobald jemand arglos den Dateianhang öffnet. Sofort werden sämtliche Dateien auf dem Dateiserver inklusive der vorhandenen Backups verschlüsselt. Die Unternehmensdaten werden quasi in Geiselhaft genommen, gegen die Zahlung eines Lösegelds versprechen die Kriminellen, die Daten wieder zu entschlüsseln. Der Schaden für den Zeitraum, in dem die Daten nicht zugänglich sind, kann je nachdem, um welche Branche und Art der Daten es sich handelt, verheerend sein: Prozesse könnten eingefroren werden, Termine und Lieferungen platzen, Löhne nicht ausgezahlt, lebenswichtige Behandlungen nicht fortgeführt werden...die Liste ließe sich endlos weiter führen. Technisch sind die nächsten Schritte in einem solchen Fall klar: Aufgrund der eingeschleusten Ransomware müssen die Systeme im ersten Schritt gesäubert werden, im zweiten Schritt gilt es, die Daten wieder verfügbar zu machen. Rechtlich mag es komplizierter aussehen. Ein Kunde kann grundsätzlich wegen etwa nicht

eingehaltener Liefertermine vom Vertrag zurücktreten und im Voraus gezahlte Beträge zurückfordern. Zudem kann er Schadensersatz wegen Nichterfüllung der vereinbarten Leistung verlangen. Dies gilt insbesondere dann, wenn der Kunde durch die späte Lieferung selbst einen Schaden vorweisen kann.

Die Rechtslage: Konsequenzen für den Arbeitgeber und den Mitarbeiter

Beide beschriebenen Szenarien können sowohl für das Unternehmen, durch das der Schaden verursacht wurde als auch für den Mitarbeiter, dessen Fahrlässigkeit (die natürlich nachgewiesen werden muss) seinen Arbeitgeber in die missliche Situation gebracht hat erhebliche rechtliche Folgen haben. Sofern nämlich geschädigte Kunden den Eintritt des Schadens und dessen Höhe beweisen können und vertraglich nicht etwas Abweichendes vereinbart wurde, können sie vom schädigenden Unternehmen Schadensersatz fordern. Auch dem verursachenden Mitarbeiter kann Strafe drohen. „Hatte der Arbeitgeber den betreffenden Mitarbeiter zuvor nachweislich und hinreichend über die Gefahren und den Umgang mit den Daten belehrt, kann er sich den gezahlten Betrag im Rahmen des so genannten innerbetrieblichen Schadensausgleichs zurückerstatten lassen“, sagt Rechtsanwalt Sebastian Müller aus Magdeburg. „Dies gilt aber nach ständiger Rechtsprechung uneingeschränkt nur, wenn der Mitarbeiter vorsätzlich oder grob fahrlässig gehandelt hat. Im Falle der mittleren Fahrlässigkeit setzt das Gericht im Streitfall eine so genannte Haftungsquote nach billigem Ermessen fest, nach der bestimmt wird, zu welchen Anteilen der Arbeitnehmer und der Arbeitgeber den Schaden tragen müssen.“ Damit trägt der Arbeitgeber letztlich dennoch das Hauptrisiko, denn selbst wenn das Gericht den Mitarbeiter wegen vorsätzlicher oder grob fahrlässiger Schädigung dazu verurteilt, seinem Arbeitgeber den Schadensbetrag zurück zu zahlen, ist kaum davon auszugehen, dass dieser die volle Summe erhält. „Ein Schadenfall in Millionenhöhe wird von einem Arbeitnehmer mit durchschnittlichem Verdienst kaum realisierbar sein. Da hilft auch ein gerichtlich erwirkter Titel nicht weiter,“ so Müller. Dennoch wird ein Fehlverhalten nicht ohne weitere Konsequenzen für den Mitarbeiter bleiben. Neben den eben beschriebenen Haftungsrisiken muss der unachtsame Mitarbeiter mit einer Abmahnung oder schlimmstenfalls auch Kündigung des Arbeitsverhältnisses rechnen.

Fazit: Sensibilisierung von Unternehmen und Mitarbeitern

„Unternehmen stehen in der Pflicht, sowohl ihre eigenen Daten als auch die Daten von Dritten zu schützen. Dies gilt natürlich bereits heute und verschärft sich aber ab Mai 2018 nochmals. Dann nämlich tritt die neue Datenschutz-Grundverordnung (EU-DSGVO) in Kraft“, sagt Michael Veit, IT-Sicherheitsexperte bei Sophos. „Unternehmen sollten daher spätestens jetzt beginnen, sich und ihre Mitarbeiter mit geeigneter Security schützen sowie regelmäßige Schulungen und klare Sicherheitsrichtlinien implementieren. Aber auch die Mitarbeiter sind in der Verantwortung. Aktives Fragen, Informieren sowie die Teilnahme an Security-Schulungen helfen, Schaden und die persönliche Haftbarkeit auf ein Minimum zu reduzieren.“

Dieser Artikel ist Teil einer von Sophos initiierten Reihe, die sich mit der rechtlichen Seite von IT-Sicherheitsvorfällen in Unternehmen beschäftigt.

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. Weitere Informationen unter www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +172 4536839
sophos@tc-communications.de