ComplianceBusiness
Ausgabe 3 // September 2017

Cyberangriffe – ein unterschätztes Risiko für Unternehmen

IT-Sicherheit als wichtiger Faktor für den wirtschaftlichen Erfolg

Von Anna Coenen

Kein Tag vergeht, an dem Medien nicht über Cyberangriffe unterschiedlichster Art berichten. Jüngst sind weltweit Unternehmen und Konzerne Viren namens „Wannacry“ und „Petya.A“ zum Opfer gefallen. Mit massiven Attacken legten Erpresser oder Saboteure die Computersysteme Dutzender Banken, Unternehmen, Flughäfen, Krankenhäuser und sogar Teile des Atomkraftwerks Tschernobyl lahm. Zeitgleich berichteten die Medien über eine Berufungsverhandlung vor dem Oberlandesgericht München. Im Mittelpunkt des Verfahrens stand ein sogenannter „Fake President Fraud“: Die Betrüger hatten die damalige Buchhalterin dazu gebracht, 1,9 Millionen Euro nach Hongkong zu überweisen.

Das Internet vereinfacht und beschleunigt Abläufe – doch Unternehmen sind gut beraten, sich auf Angriffe vorzubereiten.

© Gangis Khan/istock/Thinkstock/Getty Images

EDV als Dreh- und Angelpunkt eines jeden Unternehmens

Computer sind aus dem heutigen Wirtschaftsleben nicht mehr wegzudenken. Vom Schriftverkehr über die Planung, Kalkulation, Konstruktion bis hin zur Produktion und zum Rechnungswesen sind sie das Rückgrat eines jeden Unternehmens. Denn wenn die IT einmal ausfällt, läuft in einem Unternehmen oftmals gar nichts mehr oder alles sehr schleppend. Zugleich bietet die heutige Technik jedoch ausreichend Möglichkeiten, technische Geräte sowie Mitarbeiter zu manipulieren.

Spionage, Manipulation und Datendiebstahl

Die „klassischen“ Viren und Schadprogramme sind schon lange nicht mehr en vogue bei Hackern. Aktuell am häufigsten verwendete Angriffsmittel oder -methoden sind Ransomware und der sogenannte „Fake President Fraud“.

Ransomware ist eine Software, die sämtliche Dateien des betroffenen Computers verschlüsselt und ein Erpresserschreiben der Täter auf dem Computer der Opfer des angegriffenen Unternehmens hinterlegt; sie legt oftmals das gesamte Computersystem eines Unternehmens lahm. Die Erpressersoftware wird wie ein Virus über infizierte E-Mail-Anhänge, beim Surfen im Internet oder beim Ausprobieren von Apps auf den Computern installiert. Im Anschluss fordern die Täter dann regelmäßig Zahlungen, um die Systeme wieder freizuschalten.

ComplianceBusiness
Ausgabe 3 // September 2017

Kommen die erpressten Unternehmen dieser Forderung nicht nach, drohen ihnen Produktionsausfälle, Datenverluste sowie Industriespionage.

Beim „Fake President Fraud" nehmen die Täter eine fremde Identität an und wenden sich per E-Mail an einen ausgesuchten Mitarbeiter. Sie geben sich etwa als deren Chef, als Rechtsanwalt oder Berater des Unternehmens aus. Oftmals wird ein Mitarbeiter ausgewählt, der im Rahmen seiner Tätigkeit einen gewissen Entscheidungsspielraum hat. Er wird aufgefordert, umgehend eine Zahlung zu veranlassen. Vorgegebener Anlass ist regelmäßig eine Legende, wie etwa ein Forschungsprojekt oder eine geplante Unternehmenstransaktion, das hochgeheim zu behandeln ist. Typischerweise gehen die E-Mails zu Uhrzeiten oder in Situationen ein, zu denen Absprachen mit anderen entscheidungsbefugten Mitarbeitern nur schwer möglich sind.

Unternehmen in der Pflicht

Das Bedrohungs- und Gefährdungspotential für Unternehmen durch Cyberangriffe ist enorm und wächst unaufhörlich. Da eine Vielzahl digitaler Angriffe jedoch unentdeckt bleibt oder aus Angst vor Reputationsschäden verschwiegen wird und strafrechtliche Ermittlungsverfahren gegen die regelmäßig unbekannten Täter im Sande verlaufen, liegt es bei den Unternehmen, sowohl präventive als auch repressive Maßnahmen zur Schadensminimierung zu ergreifen.

Der Vorstand oder Geschäftsführer eines jeden Unternehmens verantwortet, dass unabhängig von der Unternehmensgröße aktiv Schutzmaßnahmen ergriffen, Abwehrsysteme entwickelt und implementiert werden. Nur wenn er nachweislich sämtliche Sicherheitsmaßnahmen umgesetzt hat, kann er sich von der Haftung für Pflichtverletzungen exkulpieren. Welche Maßnahmen geeignet sind, ein Unternehmen vor Cyberangriffen zu schützen, hängt vom konkreten Einzelfall ab, wie etwa der Größe des Unternehmens, der Branche, in der das Unternehmen agiert, der Art der zu verarbeitenden Daten sowie den gesetzlich einschlägigen Vorschriften (Bundesdatenschutzgesetz, Telemediengesetz, Kreditwesengesetz etc.). Ein effektives Sicherheitskonzept muss neben technischen Sicherungsmaßnahmen auch organisatorische und personelle Maßnahmen berücksichtigen.

Risikofaktor Mensch

Oftmals verkannt wird der Hauptrisikofaktor Mensch: Unternehmen müssen das Bewusstsein der Mitarbeiter hinsichtlich Cyberangriffen schärfen. Primär sind die Mitarbeiter regelmäßig zu schulen, sie müssen sich bei ihrer alltäglichen Arbeit stets der drohenden Gefahren insbesondere in der E-Mail-Kommunikation bewusst sein. Klare Regelungen bezüglich der E-Mail-Kommunikation und Zahlungsanweisungen müssen getroffen werden. Erfolgversprechende Maßnahmen sind beispielsweise das Verbot, E-Mails von unbekannten Absendern zu öffnen, eine Unterschriftenrichtlinie für die Freigabe von Zahlungen und das Vier-Augen-Prinzip konsequent und ausnahmslos für alle unternehmensbezogenen Angelegenheiten einzuführen und umzusetzen. Zudem bedarf es einer eindeutigen Regelung bezüglich der Auswahl und Verwendung sicherer Passwörter.

Darüber hinaus hat es sich bewährt, einen Ansprechpartner im Unternehmen zu benennen, der von Mitarbeitern in Zweifelsfällen kontaktiert werden kann und sich des jeweiligen Sachverhalts dann annimmt.

Vorbereitet sein auf den Ernstfall

Das Wissen um die Gefahr eines Cyberangriffs und die damit einhergehenden Risiken reicht jedoch nicht aus. Mindestens genauso wichtig und unerlässlich wie die Implementierung und Weiterentwicklung eines Sicherheitskonzepts ist ein stets aktualisierter und auf das Unternehmen zugeschnittener Notfallplan für den Ernstfall. Die (mittlere) Führungsebene muss so sensibilisiert sein, dass sie den Notfallplan ohne Zögern, aber zugleich mit der erforderlichen Ruhe umsetzt. Es dürfen keinerlei Unsicherheiten bestehen, wie im Fall eines Cyberangriffs zu reagieren ist. Primäre Ziele der Reaktionsmaßnahmen bei einem Cyberangriff sind die Begrenzung des eingetretenen Schadens oder die Verhinderung weiterer Schäden (intern und extern) sowie die Rückkehr in den normalen Geschäftsbetrieb.

Musterlösungen verbieten sich – jedes Unternehmen ist anders, das gilt ganz besonders für die EDV- und IT-Struktur. In der Vergangenheit haben sich in der Praxis folgende repressive Mindestmaßnahmen bewährt:

ComplianceBusiness
Ausgabe 3 // September 2017

- Festgelegte Meldewege: Die Mitarbeiter müssen wissen, wer ihr Ansprechpartner ist – etwa in der IT-, der Compliance-, der Rechtsabteilung oder aber (gerade in kleineren Unternehmen) bei einem externen IT-Dienstleister. Diese Ansprechpartner müssen im Verdachts- oder Ernstfall die erforderlichen Sicherheitsmaßnahmen in die Wege leiten, Mitarbeiter sensibilisieren und gegebenenfalls auch außenstehende Betroffene (Kunden, Lieferanten, Banken, Aufsichtsbehörden etc.) informieren.

- Bei Angriffen mit Ransomware sind zudem technische Sofortmaßnahmen zwingend erforderlich. Zunächst einmal muss das betroffene System identifiziert werden. Im Anschluss sollten zur Schadensminimierung die infizierten Systeme umgehend vom Netz getrennt werden: Netzwerkstecker, Akkus und WLAN-Adapter sollten entfernt bzw. deaktiviert und die Stromversorgung unterbrochen werden. Die entsprechende Anweisung muss durch eine hierfür eingerichtete Stelle erfolgen; die Mitarbeiter dürfen hier nicht dezentral und in Eigenverantwortung handeln müssen.

- Ferner gilt es von Anfang an, Spuren zu sichern, beispielsweise durch die Sicherung der verdächtigen E-Mail (Screenshot) oder durch die forensische Sicherung von Zwischenspeichern und Festplatten. Um weitere Datenverluste zu verhindern, ist es ratsam, forensische Sicherungen – bevor Reparaturversuche oder Neustarts der betroffenen Systeme unternommen werden – von Fachleuten durchführen zu lassen.

- Sowohl der Angriff als auch die ergriffenen Maßnahmen sollten in Form eines sog. Ereignisprotokolls dokumentiert werden.

Rechtliche Konsequenzen und Möglichkeiten

Im Anschluss an die Sofortmaßnahmen zur Abwehr des Angriffs oder der Schadensminimierung müssen Unternehmen unverzüglich ihren gesetzlichen und vertraglichen Informationspflichten nachkommen. Andernfalls drohen zivilrechtliche Forderungen sowie Bußgelder und Strafverfahren. Auch die zuständigen Aufsichtsbehörden müssen informiert werden. Im Betrugs-, Erpressungs- sowie Ausspähungsfall ist es zudem empfehlenswert, Strafanzeige zu erstatten. Denn ohne Kenntnis können die Ermittlungsbehörden eine Straftat nicht aufklären. Selbst wenn die Ermittlungen erfolglos verlaufen und der Strafanspruch nicht erfüllt werden kann, dienen die Erkenntnisse aus Ermittlungsverfahren als Grundlage für die Optimierung bestehender und Entwicklung neuer Präventionsmaßnahmen.

Darüber hinaus sollten betroffene Unternehmen prüfen, ob im Zusammenhang mit dem Cyberangriff Schadensersatz- und Versicherungsansprüche gegen oder für das Unternehmen entstanden sind, und diese gegebenenfalls abwehren oder durchsetzen.

Fazit

Das Bedrohungs- und Gefährdungspotential von Cyberangriffen ist enorm und nimmt durch neue technische Entwicklungen von Tag zu Tag zu. Dennoch vertrauen viele Unternehmen, unabhängig von ihrer Größe, darauf, dass es die anderen trifft, und ignorieren die Gefahr möglicher Cyberangriffe und der damit einhergehenden finanziellen als auch materiellen Schäden.

Aufgrund der zunehmenden Professionalisierung und Weiterentwicklung, die sich bei Cyberangriffen abzeichnet, dürfen sich jedoch auch bereits sensibilisierte Unternehmen nicht auf der einmaligen Schaffung eines Sicherheitskonzepts ausruhen. Dieses ist stets an die rasante technische Weiterentwicklung und Aufrüstung der Angreifer anzupassen. Denn die Vergangenheit zeigt und lehrt: Was heute noch als sicher gilt, kann morgen bereits ein Risiko darstellen und unzureichend sein.

Anna Coenen,
Rechtsanwältin,
Heuking Kühn Lüer Wojtek,
Düsseldorf

a.coenen@heuking.de
www.heuking.de