AssCompact
Das Fachmagazin für Risiko- und Kapitalmanagement

30. Januar 2019

Cyberschäden können Manager den Job kosten

Vor externen Hackerangriffen und internem IT-Missbrauch können Manager ihre Unternehmen nur schwer schützen. Dabei steigt mit den Cybergefahren auch ihr persönliches Haftungsrisiko. Das kann Folgen für den D&O-Schutz haben, wie Theodoros Bitis erläutert, Director Cyber & Crime Unit bei der Howden Germany GmbH.

Von Mitte Mai bis Juli 2017 wilderten Hacker unbemerkt beim US-Finanzdienstleister Equifax und stahlen die persönlichen Daten von fast 143 Millionen US-Kunden: Kreditkarten- und Sozialversicherungsnummern, Adresse, Geburtsdatum und Namen. Genug Daten für Betrüger, um Käufe oder Kreditanträge mit den gestohlenen Identitäten zu tätigen. Das Datenleck kostete zwei Monate später den damaligen Equifax-Chef Richard Smith den Job, der IT- und der Sicherheitschef waren zuvor schon in den Zwangsruhestand geschickt worden. Neben dem Imageverlust musste die Auskunftei einen Schaden von weit mehr als 300 Mio. US-Dollar hinnehmen.

Alles kann gehackt werden

Equifax ist überall. Regierungen, Behörden, Konzerne, Mittelständler, selbst die Kioskbetriebe von nebenan können Opfer eines Hackerangriffs werden. Die Täter machen schnelle Beute, oft in Millionenhöhe, und hinterlassen schwere Schäden. Einen absolut sicheren Schutz gibt es nicht. „Alles kann gehackt werden“, warnt Sandro Gaycken, Leiter des Digital Society Institute an der ESMT Berlin, der auch die Bundesregierung berät. Dabei muss es sich noch nicht einmal um gezielte Hackerangriffe handeln. Locky, WannaCry oder NotPetya – immer häufiger werden Unternehmen eher zufällig Opfer einer Ransomware-Attacke, bei der Hacker im breiten Stil Verschlüsselungstrojaner in Umlauf bringen. Schäden können auch eigene Mitarbeiter anrichten, die von innen heraus die IT manipulieren.

Cyberrisiken erfordern ein Krisenmanagement

Für Manager bedeuten diese Cyberrisiken eine Herausforderung: Sie müssen mit einem maßgeschneiderten Krisenmanagement einen möglichen Schaden bei Verdachtsfällen abwenden oder bei einem ernsten Vorfall eventuelle Folgeschäden minimieren. Manager sind dazu verpflichtet, ein – ganz wichtig – konzernweites Cyberrisikomanagement einzurichten, aufrechtzuerhalten und stets neuen Gegebenheiten anzupassen. Eine Chef-Aufgabe, die sie zwar delegieren können, aber persönlich überwachen müssen. Dabei reicht es nicht, der dann zuständigen Abteilung die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hinzulegen, sondern es gilt immer die Einzelfallprüfung. Eine Dokumentation hilft, im Falle von Schadensersatzklagen oder behördlichen Prüfungen die getroffenen Maßnahmen zu belegen.

Manager haften, wenn das Cyberrisikomanagement nicht stimmt

An diesem Punkt kann der Manager schnell in eine Haftungsfalle tappen. Hat er intern noch keine Maßnahmen angestoßen oder erweisen sich die bereits getroffenen Risikomaßnahmen als lückenhaft, droht den Unternehmensleitern der Vorwurf des Organisationsverschuldens. Das kann schnell zu Innenhaftungsfällen führen, also Schadensersatzansprüche des Arbeitgebers gegen die eigenen Führungskräfte auslösen, genauso wie Außenhaftungsfälle begründen, bei denen externe Dritte Ansprüche geltend machen, etwa Kunden, die wegen Datenschutzverstößen Schadensersatz fordern.

Bestandsversicherungen decken Cyberrisiken nicht ausreichend ab

Da selbst das beste Cyberrisikomanagement weder 100%-igen Schutz vor Kriminellen bietet, die heutzutage sehr kleine und zeitlich eng begrenzte Einfallstore nutzen, noch dem statistisch größten Risiko entgegenwirkt, dass Täter aus der eigenen Belegschaft kommen, verlassen sich viele Manager darauf, dass bei Schäden die Bestandsversicherungen des Unternehmens greifen. Was sie dabei außer Acht lassen: Herkömmliche Sachversicherungen decken lediglich Ertragsausfälle ab, die aufgrund einer sachschadenbedingten Betriebsunterbrechung entstehen. Das Problem: Die allermeisten Cyberattacken führen nur sehr selten zu einem Sachschaden. Ransomware-Erpresser blockieren durch Viren den Rechnerzugriff, sodass der Betrieb ohne Entschlüsselungscode nicht mehr in Gang kommen kann. Der Betriebsunterbrechungsschaden entsteht folglich ohne Sachschaden. Im Schadenfall lehnen daher die Sachversicherer die Deckung mangels substanzieller Einwirkung auf die IT-Systeme ab.

Herkömmlicher Schutz gilt nur für gezielte Attacken

Die Praxis hat auch gezeigt, dass Cyberausschnittsdeckungen, die im Rahmen von Sachversicherungs- oder Vertrauensschadenversicherungspolicen optional oder zum Teil sogar standardmäßig erhältlich sind, den Firmen ebenfalls keinen hinreichenden Schutz bieten. Derartige Bausteine greifen meist nur bei zielgerichteten Eingriffen in die EDV. Als zielgerichtet gilt jedoch ein Eingriff nur dann, wenn Kriminelle das Unternehmen als konkretes Angriffsziel ausgemacht haben. Bei einem Großteil der Ransomware-Attacken handelt es sich bei den Firmen jedoch ja eher um Zufallsopfer.

Cyberschäden stellen D&O-Versicherung vor Herausforderungen

Als Folge des nicht hinreichenden Versicherungsschutzes herkömmlicher Policen wenden sich Unternehmen und deren Manager bei Cyberschäden dann für die Schadenregulierung an den D&O-Versicherer. Aber: Der D&O-Versicherer bietet zunächst Deckung für die Abwehr der im Raume stehenden Schadensersatzansprüche, braucht aber viel Zeit. Diese Verzögerungen können in schwerwiegenden Fällen sogar die Liquidität einer Firma gefährden, weil die Schadenregulierung auf sich warten lässt. Hinzu kommt, dass sich Manager mit jahrelangen Rechtsstreitigkeiten auseinandersetzen müssen und bei diesem hochsensiblen Thema langfristig unter dem Druck der Öffentlichkeit stehen. Die D&O-Praxiserfahrung zeigt zudem, dass langwierige Streitigkeiten häufig in Vergleiche mit sehr überschaubaren Beträgen münden. Die Vergleichsbeträge stellen in der Regel nur einen sehr kleinen Bruchteil des Gesamtschadens für das Unternehmen dar, die kaum weiterhelfen. Manager laufen zudem Gefahr, dass Versicherer anlässlich der offenkundigen Sicherheitslücken in der Unternehmens-IT ihren D&O-Versicherungsschutz mit gravierenden

Deckungseinschränkungen versehen, etwa durch Bedingungsausschlüsse oder Deckungssummenreduzierungen. Im Worst Case kann sogar die Kündigung der D&O-Unternehmenspolice drohen.

Individuelle Cyberrisiken genau analysieren und gezielt versichern

Wer sich als Manager vor Cyberrisiken umfassend schützen möchte, sollte von einem Spezialmakler genau analysieren lassen, welche Cyberschäden die konventionellen Bestandsversicherungen tatsächlich abdecken und, um Lücken zu schließen, eine Cyberversicherung abschließen. Selbst für nicht zielgerichtete Attacken und daraus resultierende Ertragsausfälle gibt es gute Cyberschutzkonzepte. Sie tragen auch dafür Sorge, dass Manager bei der Entwicklung eines optimalen Krisenmanagements von IT-Experten unterstützt werden und im Ernstfall sofortigen Deckungsschutz erhalten. Zu ihrem eigenen Schutz sollten Manager zudem ihr Unternehmen dazu auffordern, die D&O-Deckungssumme zu erhöhen oder aber zusätzlich zur firmenfinanzierten D&O-Police eine persönliche Managerhaftpflichtversicherung auf eigene Rechnung abschließen.

Den Beitrag lesen Sie auch in AssCompact 01/2019, Seite 40 f., und in unserem ePaper.

.

Theodoros Bitis