Cyberkriminalität

Attacken aus dem Internet

Vor wenigen Wochen hatte die überwiegende Mehrheit der allein in Deutschland 20 Millionen Kunden des amerikanischen Internetauktionshauses ebay die beunruhigende Aufforderung im elektronischen Postkorb, umgehend ihre Passwörter zu ändern. Das weltweit aktive Unternehmen mit einem Jahresumsatz von ca. zwölf Milliarden US Dollar war Ziel eines Hackerangriffs, bei dem sensible Kundendaten ausgespäht wurden. Im Gegensatz zu der Cyberattacke gegen ebay nahm die Mehrheit der Deutschen die NSA-Affäre noch mehr oder weniger gelassen auf und wähnte sich in der trügerischen Sicherheit, für derartige Spionageaktivitäten nicht interessant genug zu sein. Doch spätestens mit dem „Fall ebay" ist es erschreckende Gewissheit: Mit dem Betreten des World Wide Web wird der Nutzer zu einem potentiellen Opfer von Cyberkriminalität. Das deutsche Cyber Universe wird regelmäßig von Hackern aus aller Herren Länder infiltriert, und ein Großteil dieser illegitimen Besucher hat weitaus andere Interessen als nur das Lesen fremder E-Mails.

Unsere „Cybernation" sitzt auf einem Pulverfass …

… und die Lunte glimmt bereits. Jeden Tag nutzen Millionen von Bundesbürgern das Internet und vertrauen darauf, dass ihre Geheimnisse in Form von Zugangscodes und Passwörtern auch geheim bleiben. Während man in den deutschen Haushalten regelmäßig mindestens einen Computer vorfindet, bleibt die Suche nach einer einsatzbereiten und aktuellen Virenschutzsoftware oftmals erfolglos. Kein Wunder also, dass Trojaner und andere Schadprogramme „mithören", wenn der Computernutzer sich in seinem e-Mail-Account einloggt, seine Facebook-Seite öffnet, Einkäufe bei Amazon tätigt, bei einer Internetauktion mitbietet oder seine Bankgeschäfte online erledigt. In jedem Fall kommt die Cyberkriminalität dem altbekannten Hase-und-Igel-Rennen gleich. Die Softwareentwickler konkurrieren mit den Hackern im zeitlichen Wettkampf um die Daten(un)sicherheit. Ein beliebtes Ziel der Hacker ist seit langer Zeit der Internet Explorer von Microsoft. Die regelmäßige Taktfrequenz der MS-Updatepakete verdeutlicht den Wettlauf zwischen Herstellern und Einbrechern eindrucksvoll.

Auch wenn der unerlaubte Zugriff auf ein Bank- oder auf ein Kreditkartenkonto für den Privatmann sehr ärgerlich ist, so beschränkt sich der Schaden in den meisten Fällen auf einige Hundert bis ein paar Tausend Euro. Im Vergleich zu den Schäden, die sowohl deutschen als auch international tätigen Firmen durch Internetattacken zugefügt werden, handelt es sich dabei um kollaterale Bagatellereignisse. Bei der Frage nach der Datensicherheit und der Einschätzung der Cyberrisiken durch deutsche Unternehmen, stimmt eine Schlagzeile der Süddeutschen vom 31. Juli 2014 nachdenklich. Der Stuttgarter Elektronikkonzern Bosch hat laut dieser Meldung gegen Schäden aus Cyberattacken mit einer Versicherungssumme von 100 Mio. Euro vorgesorgt. Ein Versicherungsvertrag dieser Größenordnung zur Bedeckung von Cyberrisiken war bis vor Kurzem undenkbar. Auch wenn Einzelheiten zu dem Versicherungskonsortium, das dieses Risiko unter Führung der Allianz gezeichnet hat, dünn gesät sind, so zeigt diese Meldung, dass die Unternehmensleitung von Bosch das Risiko von Schäden als Folge von Hacker-Attacken sehr hoch bewertet. Das Risiko hoher Schäden durch einen kriminellen Angriff aus dem Internet ist den Verantwortlichen wohl bewusst. Die Sorge geht um bei den deutschen Unternehmen; gleichwohl wird regelmäßig der Mantel des Schweigens über eingetretene Schadenfälle gedeckt und im Fall eines Diebstahls von Kundendaten der betroffene Personenkreis diskret über die Notwendigkeit neuer Passworte informiert, betroffene Kreditkarten werden ausgetauscht oder neue Konten eingerichtet.

Der Versicherungsmakler im Fadenkreuz?

Auch und gerade der Finanz- und Versicherungsmakler verfügt über eine Fülle hochsensibler Informationen seiner Kundenverbindungen. Neben der Aufzeichnung von Personal- und Vertragsdaten, werden regelmäßig auch Bankverbindungen, Informationen zu Depotkonten, Auszahlungsaufträge und vieles mehr auf den Servern in den Büros der Vermittlerschaft abgespeichert. Bevor der Versicherungsmakler seine Kunden zum Thema Datensicherheit und Versicherungslösungen für den Fall der Fälle berät, sollte er sich selbst erst einmal die Frage nach dem Datenschutz in seinem eigenen Büro, potentiellen Schwachstellen in seinem EDV-System und dem Umfang potentieller Schadenfälle stellen. Auch Finanz- und Immobilienmakler, Steuerberater, Buchhaltungsbüros oder EDV-Dienstleister (Fremdwartungsrisiken) halten äußerst sensible Daten vor. Eine Hackerattacke kann nicht nur zu einem hohen Eigenschaden, sondern auch zu empfindlichen Fremdschäden mit nachfolgend gleichermaßen höchst peinlichen wie hohen Schadenersatzforderungen gegen den Dienstleister führen.

Das Risiko eines Cyberangriffs ist zwischenzeitlich in der Wahrnehmung vieler Firmen angekommen. Die Frage nach der potentiellen Gefährdung des eigenen Unternehmens bzw. die Wirksamkeit der getroffenen Schutzmaßnahmen werden von einigen Unternehmen zwischenzeitlich kritisch auf den Prüfstand gestellt. Die Stadtwerke Ettlingen hatten sich in diesem Zusammenhang zu einer ungewöhnlichen Vorgehensweise entschieden und den deutschen IT-Spezialisten Felix „FX“ Lindner und sein Team von Recurity Labs mit einem freundschaftlichen Angriff auf die Schaltzentrale des Energieversorgers beauftragt. Bereits nach wenigen Tagen hatten Lindner und sein Team das System der Stadtwerke Ettlingen gehackt. Im Fall eines kriminellen Cyberangriffs hätten Lindner und seine Mitarbeiter alle Kontroll- und Steuerfunktionen des Energieversorgers übernehmen und damit die Stromversorgung einer ganzen Region lahmlegen können.

Alexander Schrehardt
Geschäftsführer
Consilium Beratungsgesellschaft für betriebliche Altersversorgung mbH

Katja-Christine Böhme
Versicherungsfachwirtin
KCB Versicherungsmakler, Adelsdorf

Die Liste potentiell bedrohter Unternehmen ist vor allem bei kleinen und mittelständischen Unternehmen unendlich lang. Während internationale Global Players ganze Fachabteilungen für ihre Datensicherheit vorhalten können, sind viele kleine und mittelständische Unternehmen mangels finanzieller und personeller Kapazitäten auch weiterhin in puncto Datensicherheit mit Scheuklappen unterwegs. Aber nicht nur von den Unternehmen werden das Risiko von Cyberangriffen und die weitreichenden Folgen derartiger krimineller Attacken erkannt. Auch der Gesetzgeber will nunmehr diesem Problem mehr Aufmerksamkeit widmen und mit Hilfe eines IT-Gesetzes betroffene Unternehmen zur Meldung von Cyberangriffen verpflichten. Natürlich ist es von der Meldung eines Ereignisses bis zu dessen erfolgreicher Abwehr im Vorfeld ein weiter Weg. Die Tatsache, dass sich sowohl Unternehmen als auch der Gesetzgeber dem Problem stellen, ist jedoch zumindest als ein optimistischer Fingerzeig zu werten.

Versicherungslösungen für den „Cyber Worst Case“

Die Folgen einer erfolgreichen Hackerattacke können für das betroffene Unternehmen fatal und im schlimmsten Fall sogar existenzbedrohend sein. Neben dem eigenen IT-Schaden katapultieren Verstöße gegen gesetzliche und/oder vertragliche Datenschutzverpflichtungen oder auch die Weitergabe eines infiltrierenden Virus, z.B. viam e-Mail, an die EDV-Systeme von Kunden oder Geschäftspartnern Schadenersatzforderung unter Umständen in astronomische Höhen. Aber nicht nur monetäre Schadenersatzforderungen können das Unternehmen in hohem Maße belasten. Auch langjährige Rechtsstreitigkeiten z.B. über patentrechtliche Verletzungen oder Vertragsstrafen können zu einem Image- und nachfolgend zu einem Vertrauensschaden der betroffenen Unternehmen führen. Keine wirksame Vorsorgemaßnahme bietet eine Versicherungslösung, die sich auf eine finanzielle Entschädigung im Schadenfall kapriziert. Im Schadenfall muss die Schadenregulierung von einer Rechts- und PR-Beratung flankiert werden. Bei der Regulierung von Schäden stellt sich ferner die Frage, für welche Schäden ein Anspruch auf eine Versicherungsleistung besteht. Bedeckt der Versicherungsschutz z.B. auch den Betriebsunterbrechungsschaden, im Fall eines erpresserischen Cyberattacke auch ein eventuell gefordertes Lösegeld und vor allem Maßnahmen zur Verbesserung der Sicherheit und damit zur Vermeidung weiterer erfolgreicher Angriffe? Wie immer das individuelle Anforderungsprofil und der Vorsorgebedarf eines Unternehmens auch sein mögen, eine schnelle Umsetzung von geeigneten Sicherheitsmaßnahmen und ein ausreichend dimensionierter Versicherungsschutz erscheinen als das Gebot der Stunde. ■