Datum: 09.04.2015

Handelszeitung

Handelszeitung
8021 Zürich
043/ 444 59 00
www.handelszeitung.ch

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 37'909
Erscheinungsweise: wöchentlich

Themen-Nr.: 999.013
Abo-Nr.: 1085867
Seite: 40
Fläche: 46'791 mm²

Attacken auf Schweizer Firmen nehmen zu

Cyber-Risiken Hacker aus aller Welt nehmen Schweizer Firmen ins Visier. Vorausschauende Unternehmer passen ihre IT-Sicherheitsstrategien an und versichern sich.

CARIN GANTENBEIN

Global verursachen Cyber-Attacken bald so hohe Kosten wie Naturkatastrophen. 2013 waren es bereits 113 Milliarden Dollar gegenüber 140 Milliarden Dollar bei Naturkatastrophen. Bei Naturgefahren wissen die Betroffenen in der Regel um die Gefahr und versuchen, sich zu schützen, so gut es geht. Unser Bewusstsein für die Gefahren aus dem Cyberspace – Datendiebstahl, Hackerangriffe oder gezielte Systemunterbrüche – entwickelt sich hingegen erst.

Dabei sind besonders Firmen in Ländern wie der Schweiz ein geeignetes Ziel für Cyber-Attacken: Ein wohlhabendes Land mit vielen erfolgreichen, national wie auch international tätigen Unternehmen, die sich häufig noch in Sicherheit wiegen und dem Thema nur bedingt Aufmerksamkeit schenken. So verwundert es nicht, dass die Schweiz in den vergangenen Jahren weltweit unter den zehn Ländern mit den häufigsten Cyber-Attacken war.

Sicherheitsnetz knüpfen

Erst Anfang Februar 2015 warnte die Melde- und Analysestelle Informationssicherung des Bundes (Melani), dass KMU vermehrt ins Visier von Internetbetrügern geraten, weil sich viele von ihnen ungenügend gegen Gefahren aus dem Cyberspace schützen.

Dies liegt auch daran, dass diese Angriffe im Verborgenen ablaufen. In den USA werden Unternehmen im Durchschnitt zwei Mal täglich attackiert. Davon sind wir hierzulande noch entfernt, aber bei zwei physischen Einbruchsversuchen pro Tag würden Unternehmer ihre Firmengebäude ziemlich sicher in eine Festung verwandeln. Im Informatikbereich hingegen zeigen Unternehmer Nonchalance, bis es zu spät ist. Erschwerend kommt hinzu, dass die Angriffe erst mit grosser Verspätung bemerkt werden. Sie bleiben laut einer aktuellen Studie durchschnittlich 229 Tage lang unentdeckt. Ein Einbruchsversuch an Neujahr würde erst am 18. August entdeckt!

Für IT-Experten gibt es nur zwei Gruppen von Firmen: Firmen, die bereits Opfer von Cyber-Attacken geworden sind, und Firmen, denen das noch bevorsteht. Firmen, die die IT-Sicherheit ernst nehmen, haben in der Vergangenheit viel in die Prävention investiert, etwa in Firewalls und Antivirenprogramme. Doch Viren ändern sich in der Regel schneller, als Abwehrprogramme und Firewalls mithalten können. Zudem hat sich die Bedrohungslage geändert: Einige Attacken sind bereits so ausgefeilt, dass man sich kaum mehr vor ihnen schützen kann. Mehr und mehr werden Schlüsselpersonen in Unternehmen Opfer von massgeschneiderten Attacken. Unternehmen müssen daher bei der Prävention bereits auch an den Ernstfall denken (siehe Kasten). Tritt dieser ein, muss die Firma sich so rasch wie möglich vom Angriff erholen. Heute braucht es statt einer Schutzmauer ein Sicherheitsnetz – geknüpft bereits vor dem Krisenfall und mit Experten, auf die man zurückgreifen kann. Das hilft, den Schaden zu begrenzen, die Ursache des Lecks zu erkennen und möglichst rasch wieder in den Modus Operandi zurückzukehren. Das ist ein fundamentaler Richtungswechsel. Aber er ist nötig: Cloud Computing, Smartphones, «Internet der Dinge» – immer mehr Geräte und Infrastrukturen werden mit dem Internet verbunden. Mit der Vernetzung wächst die Abhängigkeit – und das Risiko, Opfer einer kostspieligen Cyber-Attacke zu werden. Dabei spielt die Branche immer weniger eine Rolle. Es kann jeden treffen.

Jede Firma muss den Schutz der eigenen Daten optimieren.

Ein Beispiel: Durch eine gezielte Hackerattacke wird das IT-Netzwerk einer Firma über Tage lahmgelegt. Umsatz- und Gewinnverluste sind die Folge. Dazu kommt, dass das System von einem IT-Fachmann repariert werden muss, die Sicherheitslücke im IT-System gefunden und gestopft werden muss und verlorene Daten wieder hergestellt werden müssen. Das kommt teuer. Noch teurer wirds, wenn persönliche Daten von Kunden gestohlen wurden. Dies kann je nach anwendbarer Rechtsordnung zu Klagen gegen das Unternehmen führen, die Prozess- und Verteidigungskosten zur Folge haben. Je nach Ausgang des Prozesses wird ein Unternehmen zu Schadenersatz verurteilt. Zudem können Meldepflichtkosten anfallen. In den USA sind Unternehmen seit über zehn Jahren verpflichtet, ihre Kunden zu informieren, wenn persönliche Daten wie Kreditkarteninformationen oder Daten aus dem Gesund-

Datum: 09.04.2015

Handelszeitung

Handelszeitung
8021 Zürich
043/ 444 59 00
www.handelszeitung.ch

Medienart: Print
Medientyp: Publikumszeitschriften
Auflage: 37'909
Erscheinungsweise: wöchentlich

Themen-Nr.: 999.013
Abo-Nr.: 1085867
Seite: 40
Fläche: 46'791 mm²

heitswesen verloren gehen. Für börsenkotierte Firmen gelten verschärfte Bedingungen. Darum sind Cyber-Versicherungen in den USA heute selbstverständlich. Fast jedes dritte Unternehmen dort hat einen solchen Versicherungsschutz.

Bald Meldepflicht in der EU

In der EU sieht die geplante Datenschutz-Verordnung ebenfalls eine Meldepflicht beim unerlaubten Veröffentlichen von personenbezogenen Daten vor. Bei Nichteinhaltung könnten Strafen in Höhe von 100 Millionen Euro oder 5 Prozent des weltweiten Umsatzes der Firma fällig werden. Davon wären auch Schweizer Firmen mit Kunden aus dem EU-Raum betroffen. So oder so: Bereits heute wollen immer mehr Schweizer Unternehmen diese Art von Risiken nicht eingehen und sich versicherungstechnisch vor Cyber-Attacken schützen. Das ist möglich. Einige grosse Versicherer bieten heute Versicherungslösungen an. Zurich baut dabei auf ihre langjährige Erfahrung mit solchen Risiken vor allem aus den USA auf und stellt dem Kunden ein Netzwerk von internen und externen Experten zur Verfügung – präventiv und im Schadenfall. Die Kosten für einen solchen Versicherungsschutz hängen vor allem vom Firmenumsatz und dem Umfang an sensitiven Daten ab.

Fazit: Jede Firma muss den Schutz ihrer Daten selbst in die Hand nehmen. Es lohnt sich, sich dabei auch mit dem Thema Cyber-Attacken auseinanderzusetzen und präventiv ein Sicherheitsnetz für den Ernstfall zu knüpfen. Denn Schweizer Unternehmen sind überdurchschnittlich gefährdet. Gut zu wissen: Zumindest die finanziellen Folgen von Cyber-Angriffen lassen sich heutzutage versichern.

Carin Gantenbein, Leiterin Berufshaftpflicht, Zurich Schweiz, Zürich.

FÜNF-PUNKTE-PLAN

Cyber-Risiken minimieren

- Definieren Sie Ihre «kritischen Vermögenswerte»: Was müssen Sie schützen (zum Beispiel Kunden- und Mitarbeiterdaten, Patente)?
- Definieren Sie Ihren Risikoappetit: Wie viel Risiko sind Sie bereit, auf sich zu nehmen?
- Analysieren Sie das Gefahrenpotenzial Ihrer Firma: Was sind mögliche Gefahren von aussen und was sind Ihre internen Schwachstellen (zum Beispiel IT-Infrastruktur, Mitarbeiter)?
- Basierend auf Ihrem Risikoappetit: Definieren Sie geeignete Massnahmen, um Ihre «kritischen Vermögenswerte» zu schützen und das Risiko auf ein akzeptables Niveau zu bringen.
- Planen Sie für den Notfall: Zum Beispiel Krisenmanagementpläne bei Geschäftsunterbruch.