

Fachinformation

Hoffen Sie noch, oder wurden Sie schon gehackt?

„Cyber-Angriffe finden täglich statt und werden zunehmend professioneller und zielgerichteter ausgeführt.“ Das ist eine der wichtigsten Schlussfolgerungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) in ihrem kürzlich veröffentlichten „Bericht zur Lage der IT-Sicherheit in Deutschland 2014“. Diese „Schattenseite“ der Digitalisierung wird gerne von Unternehmen ausgeblendet. Mit der Vereinfachung der Prozesse, einer zunehmenden Automatisierung von Arbeitsschritten und damit erzielbaren Kosten- und Zeiteinsparungen treten die Vorteile so deutlich zu Tage, dass damit der Blick für die Gefahren – insbesondere, wenn es keine eigene IT-Abteilung im Unternehmen gibt – fehlt. Daneben existiert ein latentes, aber trügerisches Sicherheitsgefühl, weil die Bedrohung nicht fassbar ist. Hinzu kommt, dass erfolgreiche Angriffe lange oder sogar gar nicht bemerkt werden.

Aber selbst konservative Annahmen gehen davon aus, dass im vergangenen Jahr mindestens jedes dritte Unternehmen weltweit Ziel von Angriffen aus dem Internet war. Beim finanziellen Schaden reichen die Schätzungen für Deutschland für das vergangene Jahr von 40 Millionen bis weit über 20 Milliarden Euro. Gerade für kleine und mittlere

Unternehmen können die Schäden existenzbedrohend werden. Laut einer Kaspersky Lab Studie kostet ein Angriff im Durchschnitt rund 41.000 Euro. Und kleine Unternehmen sind einfache Ziele und über digitale Strukturen auf einem „globalen Markt“ verfügbar.

Sichern vor „Versichern“

Wohl wissend, dass der technischen Aufrüstung in die IT-Sicherheit von Unternehmen Grenzen gesetzt sind, sollten Sie - in Abstimmung mit Ihren internen oder externen IT-Dienstleistern - sämtliche verfügbaren und leistbaren Sicherheitsmaßnahmen ausschöpfen. Mit eben solchen Maßnahmen lässt sich bereits ein beachtliches Schutzniveau erreichen, welches bis zu 80 % der gängigen Angriffe abwehrt¹. Ergänzend dazu empfiehlt sich eine interne Analyse und monetäre Bewertung Ihrer Risiken. Auf Grundlage einer solchen Risikoanalyse lässt sich eine Entscheidung treffen, ob Sie als Unternehmen, die verbleibenden Sicherheitsrisiken selber tragen können, oder ob Sie diese Risiken mit Hilfe einer Versicherung weitergeben wollen.

¹ BSI-Studie: „Die Lage der IT-Sicherheit in Deutschland 2014 – Lösungsansätze“, S. 38



VGA

Versicherungskonzepte für
Handel und Dienstleistung

VGA-Konzept deckt mögliche Kosten und schützt Ihre Reputation

Die VGA begleitet Sie bei der Erstellung Ihrer Risikoanalyse und bietet Ihnen eine Absicherung der verbleibenden Risiken. Denn im Ernstfall gilt es, anfallende Kosten zu decken und den Ruf des Unternehmens zu schützen. Hierbei wird zwischen Eigenschäden, die innerhalb Ihres Unternehmens anfallen, und Drittschäden unterschieden. Letztere entstehen, wenn Ihr Unternehmen von geschädigten Dritten auf Schadenersatz in Anspruch genommen wird.

Eigenschaden Szenario – Hacker erbeuten Kreditkartendaten

Ein mittelständisches Unternehmen, welches seit einigen Jahren erfolgreich auf Onlinehandel gesetzt hat, wird seit einigen Monaten unbemerkt gehackt. Erst nachdem Banken und ein Kreditkartenunternehmen auf unautorisierte Buchungen bei einer Vielzahl von Kunden aufmerksam machen, beginnt die Suche des Unternehmens nach der IT-Sicherheitslücke. Obwohl dem Vorfall höchste Priorität eingeräumt wird, kann die Ursache erst nach einigen Wochen gefunden und behoben werden. Zwischenzeitlich ist der Fall von der lokalen Presse öffentlich gemacht worden, woraufhin behördliche Ermittlungen veranlasst werden. Während dieser Zeit brechen die Umsätze des Unternehmens stark ein. Wochen später ist der Sachverhalt Gegenstand der Gesellschafterversammlung.

Weitere Kostenbeispiele:

- Kosten für forensische Dienstleistungen zur Identifizierung personenbezogener Daten und zur Ursachenforschung auf Ihrer Serverlandschaft
- Kosten durch gesetzliche Informationspflichten
- Rechtsverteidigungskosten nach einem Datenschutzverstoß
- die Befriedigung der Ansprüche von Dritten nach einem Datenschutzverstoß
- PR-Aktivitäten zur Wiederherstellung der Reputation Ihres Unternehmens

Ausblick

Cybercrime ist heute schon allgegenwärtig. Alle Anwendergruppen – Wirtschaft, Wissenschaft, Verwaltung und Bürger – sind davon betroffen. Solange Kriminelle die Möglichkeit haben, auf diesem Weg Geld zu verdienen, werden sie diese nutzen und ihre Methoden weiterentwickeln.

Bleiben Sie daher nicht tatenlos und stellen sich der Herausforderung, Ihr Unternehmen so gut es geht zu schützen. Nehmen Sie dazu auch unsere Expertise und die unserer Partner in Anspruch.

Wir freuen uns auf Ihren Anruf.

VGA GmbH

www.vga.de

Telefon:

(030) 59 00 99 940