Cyberkriminalität - Gefahren und Risiken werden teilweise noch immer unterschätzt

Krisen-management

Von Frank Reidt

Frank Reidt

I. V. D.
Herne / Westfalen

Diplom- Kaufmann
Geschäftsführer

Risiko- und Versicherungsmanagement

Cyberkriminalität und Datendiebstahl befinden sich weiter auf dem Vormarsch. Allerdings sind zunehmend nicht nur staatliche Stellen und Großunternehmen von den Attacken betroffen. Vielmehr verlagert sich der Fokus immer weiter in Richtung Mittelstand. Hier können Hacker, Cyberkriminelle und Wirtschaftsspione noch fette Beute machen.

Auch ehemalige Mitarbeiter und Konkurrenten sind diesbezüglich schon auffällig geworden. Der Mittelstand ist gut beraten, wenn er angesichts der wachsenden Bedrohung und Risiken durch die steigende Cyberkriminalität die eigenen IT-Sicherheitsstrukturen optimiert und sich ausreichend versichert.

Fluch der digitalen Transformation: ohne konkrete IT-Schutzmaßnahmen geht nichts

Dies ist wichtig, da die Digitalisierung der Geschäftswelt mit einem Wandel einhergeht. Ob Big Data oder Automatisierung - Schlagwörter dieser Art stehen für eine Entwicklung, die das gesamte wirtschaftliche System in unterschiedlicher Form umwälzen. Dadurch ergeben sich auf der einen Seite ganz neue Möglichkeiten für den Mittelstand. So sind eine bessere Planung und Kontrolle, effizientere Prozesse und der Einsatz neuer Erkenntnisse im Bereich der Datenanalyse möglich.

"Die Entscheider in den mittelständischen Betrieben haben das Potenzial der Digitalisierung mittlerweile zwar erkannt und das eigene Unternehmen entsprechend transformiert, aber die damit einhergehenden Gefahren werden häufig immer noch übersehen respektive ignoriert. Dabei sollte die Umsetzung konkreter Schutzmaßnahmen immer einen wichtigen Teil der eigenen Digitalisierungsstrategie darstellen."

(Frank Reidt)

Krisen-
management

Studie des Max-Planck-Instituts belegt die Gefahr für KMU

Dass die Gefahr von Cyberkriminalität und Datendiebstahl auch im Mittelstand allgegenwärtig ist, belegt eine Studie des Max-Planck-Instituts für internationales und ausländisches Strafrecht, die in Zusammenarbeit mit den Landeskriminalämtern im Bereich Wirtschaftsschutz sowie dem Fraunhofer-Institut für System- und Innovationsforschung entstanden ist. Insgesamt 700 Strafakten wurden im Rahmen der Studie untersucht.

Zudem befragten die Ermittler bzw. Forscher rund 600 Mittelständler. Demnach ist jedes zweite mittelständische Unternehmen in Deutschland bereits mindestens einmal Opfer von Cyberkriminalität gewesen - oder aber es lagen zumindest erhebliche Verdachtsmomente vor. Am höchsten sind die Fallzahlen im Handel, in der Baubranche sowie im Bereich der industriellen Dienstleistungen.

Immer mehr Unternehmen aus der zweiten Reihe werden attackiert

Die Ergebnisse der Studie zeigen klar auf, dass - trotz der Schwerpunktbildung - für alle Unternehmensgrößen und Branchen Risiken bestehen. Unternehmen, die dabei weniger in der Öffentlichkeit stehen, wähnen sich häufig in Sicherheit. Das ist ein fahrlässiges Denken. Denn der heimische Mittelstand weckt mit seinen vielen Spezialisten und Hidden Champions durchaus Begehrlichkeiten bei den Cyberkriminellen.

Zudem suchen sich Hacker gezielt Unternehmen aus der zweiten Reihe für ihre Attacken aus. Sie rechnen hier mit weitaus weniger Widerstand bzw. Gegenwehr. Zumal die Täter oftmals mit den Gegebenheiten und den Schutzmaßnahmen in den Unternehmen bestens vertraut sind. So kam der Täter in fast jedem zweiten Fall der untersuchten Vorkommnisse aus den eigenen Reihen.

Unterschiedliche Herangehensweisen der Täter komplizieren den Schutz

Der Diebstahl und die Ausspähung von sensiblen Daten erfolgt dabei sowohl auf digitale als auch auf physische Art, bei der die Betriebsgeheimnisse direkt vor Ort kopiert oder einfach sofort via Mail verschickt werden. Gehen die Täter digital vor, attackieren sie das Netzwerk und verschaffen sich Zugang auf den kompletten Datenfundus eines Unternehmens.

Zum Einsatz kommen zum Beispiel Ausspähungsprogramme, Bot-Angriffe oder diverse Schadsoftware. Angesichts der vielfältigen Risiken stellt es daher keine Option dar, wenn man die Optimierung der unternehmenseigenen IT-Sicherheitsstruktur aufschiebt. Ganz im Gegenteil: Es sollte auf jeden Fall zeitnah gehandelt werden.

Versicherungen schützen vor Schadensersatzansprüchen und Regressforderungen

Entwendete Daten sind aufgrund des Informationsgehalts grundsätzlich geschäftsschädigend. Der Verlust von Daten kann letztendlich sogar die Existenz eines Unternehmens bedrohen. Hacker sind zum Beispiel durchaus in der Lage, eine Produktion für einen längeren Zeitraum lahmzulegen. Mit einem optimierten IT-Sicherheitsstandard kann man dabei in der Regel einen Großteil der Attacken abwehren. Allerdings ist ein umfassender Schutz - aufgrund der Kosten und des Aufwands - nicht immer möglich.

Unternehmen sollten sich daher auch eingehend mit dem Thema IT-Versicherung auseinandersetzen. Werden zum Beispiel personenbezogene Daten entwendet, reichen betroffene Kunden oftmals Schadensersatzansprüche ein. Dies kann sich schnell summieren. Möglich sind auch Regressforderungen, wenn ein Unternehmen nicht rechtzeitig liefern kann, weil dessen Produktion lahmgelegt wurde. Einem mittelständischen Unternehmen können solche Forderungen an die Substanz gehen.

Kompetenzberatung und Risikoanalyse legen die Probleme und Lösungen offen

Die reguläre Betriebsausfall-Versicherung greift nämlich in einem solchen Fall nicht, da es keinen vorangehenden Sachschaden - wie zum Beispiel einen Brand - gibt. Hier helfen nur spezielle Versicherungen gegen Cyberattacken. Welche Kombination aus IT-Sicherheitsmaßnahmen und vorbeugender Versicherungsschutz die beste Lösung darstellt, lässt sich im Rahmen einer umfassenden individuellen Experten-Beratung mit Risikoanalyse feststellen.

Krisen-management

"Je länger man damit wartet, einen optimalen Schutz vor der Bedrohung durch Cyberattacken und Datendiebstahl zu installieren, desto ausgeprägter ist die Gefahr, dass man Opfer eines solchen Verbrechens wird. Ohne entsprechende Sicherheitsvorkehrungen und Schutzmaßnahmen setzt man somit die Zukunft seines Unternehmens aufs Spiel."

(Frank Reidt)