Cybersecurity – glücklich ist, wer nichts hat

SICHERHEIT Das Thema Cybersecurity geniesst grosse Medienpräsenz. Auch in allen IT-Projekten ist es omnipräsent. Und doch passiert es immer und immer wieder, und dahinter stecken nicht nur Geheimdienste und dunkle Mächte. So hat in Deutschland ein 20-jähriger Student die Accounts von ein paar hundert exponierten Persönlichkeiten gehackt. Was würden wohl bezahlte Wirtschafts-Hacker tun?

VON CHRISTOPH HILBER

Eine nicht repräsentative Umfrage bei Verwaltungsrätinnen und Verwaltungsräten durch P-Connect* hat ergeben, dass 68 Prozent der Firmen schon angegriffen wurden. Aber nur 39 Prozent der Unternehmen sind überzeugt, einen Angriff rechtzeitig zu entdecken.

Die gelegentliche Aussage «Wer noch nie angegriffen wurde, hat es einfach nicht gemerkt» dürfte wahrer sein als erwünscht. Die Tatbestände, welche unter die Rubrik Cybersecurity fallen, sind schliesslich vielfältig: Daten kopieren oder verändern, Daten zerstören oder Erpressung durch Verschlüsselung, Diebstahl von Authentifizierungen, Mithören oder Mitsehen über Kameras und Mikrofonen und noch Unbekanntes. Hinzu kommen die Gefahren von innen, wo möglicherweise unzufriedene Mitarbeitende Daten mitnehmen und extern verwerten. Der Bankenplatz Schweiz kann dies bestätigen. Wenn man den ganzen Gefahrenbereich betrachtet, dürfte jedes Unternehmen, welches mehr als einen Mitarbeitenden umfasst, bisher tatsächlich schon einmal irgendwie betroffen gewesen sein.

KRIMINELLE BEREICHERUNG

Das Gute an der kriminellen Bereicherung ist, dass man sie relativ schnell bemerkt. Die Daten müssen «taufrisch» auftauchen, um dafür möglichst viel Geld zu lösen. Im Falle von Erpressung durch Verschlüsselung wird man sofort mit den Tatsachen konfrontiert. Der Schutz vor diesen klassischen Viren, Trojanern etc. ist eigentlich einfach, genügen hier aktuelle Virensoftware und eine intensive und laufende Sensibilisierung der Mitarbeitenden.

WIRTSCHAFTSSPIONAGE

Diese Art des Cyberangriffes will im Stillen wirken und nicht auffallen. Hier dürfte eine signifikante Dunkelziffer liegen. Um diese Angriffe zu bemerken, braucht es eine Cyberabwehr-Strategie, welche immer auf den neusten Erkenntnissen und Tools aufsetzt. Und nie stehen bleibt. Es ist ein Kampf gegen professionelle und sehr clevere Organisationen, geheime Dienste, welche per definitionem immer einen Schritt voraus sind. Selbst bei besten Vorkehrungen bleibt die Gefahr, über ein bisher unbekanntes Leck gehackt zu werden.

SCHUTZ NACH AUSSEN

Bei 74 Prozent der Antwortenden ist das Thema Cybersecurity ein Traktandum auf Ebene Verwaltungsrat. Also auf der wichtigsten Stufe angesiedelt, um diesbezüglich über Strategie zu entscheiden und Ressourcen bereitzustellen. Alle grossen Firmen dürften über eigene spezialisierte Teams verfügen, die mittelständischen Unternehmen haben es an externe Partner delegiert. Als KMU ist es praktisch unmöglich, mit der schnellen Entwicklung der sehr vielfältigen Bedrohungen und kreativen Täterschaften mithalten zu können. Wer nicht in eigene oder externe Spezialisten investiert, lebt gefährlich.

SCHUTZ NACH INNEN

Der Schutz nach inneren Gefahren geht über die Kontrolle von Mitarbeitenden. Ein heikles Thema. Der am 12. Feb. 2019 veröffentlichte «KPMG Forensic Fraud Barometer» von KPMG lässt aufhorchen. Der Bericht ermittelte das Management als Haupttäter und stellte fest, dass mit einer hohen Dunkelziffer zu rechnen sei. Diese Aussage müsste dem Verwaltungsrat die grösste Sorge bereiten, bedeutet dies doch, gegenüber dem selbst ausgewählten Management auch etwas misstrauisch zu sein.

LOHNT ES SICH?

Besitzt das Unternehmen überhaupt wertvolle und schützenswerte Daten? Das ist die Grundsatzfrage. Rund ein Drittel der Antwortenden in der erwähnten Umfrage glauben, dass es bei ihnen nichts auszuspionieren gibt. Das dürfte für sehr kleine Firmen im Dienstleistungsbereich sicher zutreffen, wo der grösste Schaden wohl der Diebstahl von Bankzugangsdaten wäre. Bei Datenverlust genügt eine Datensicherung, um im Geschäft zu bleiben. Für KMUs und grössere Firmen hätte ein Angriff möglicherweise existentielle Konsequenzen. In der Schweiz als Spitzenreiter auf dem weltweiten Innovationsindex dürfte es sich für geheime Dienste lohnen, ein paar Unternehmen mehr als weniger auszuspionieren.

Von wahrem Luxus in diesem Zusammenhang dürfte für einmal nur profitieren, wer nichts Interessantes und Wissenswertes besitzt.

* Umfrage von P-CONNECT im Januar 2019 unter https://www.p-connect.ch/cybersecurity

DER AUTOR

Christoph Hilber ist Betriebswirtschafter und seit über zehn Jahren Personalberater mit seiner eigenen Firma P-CONNECT – Executive Search & Outplacement, fokussiert auf Positionen Verwaltungsräte, Geschäftsleitungen/Kader und Spezialisten in Industrie (MEM), Informatik, Telekom. Vorgängig war er in leitenden Linienfunktionen bei NCR/AT&T, diAx und Siemens.

www.p-connect.ch