FOTO: SHUTTERSTOCK

Kein einfaches Ziel sein

100 Prozent Sicherheit gibt es nicht

Mittlerweile ist wohl jedem Unternehmer klar, dass er seine IT vor Angriffen schützen muss. Viel schwieriger ist das Wie. Letztlich geht es darum, Hackern und Spionen das Eindringen so schwierig wie möglich zu machen und sie möglichst schnell zu entdecken.

VON ANDREA PRZYKLENK

In der US-amerikanischen Fernsehserie über eine Spezialeinheit des FBI, die Cyber-Verbrechen verfolgt, löst das Team natürlich jeden Fall. In der Realität sieht es wesentlich schlechter aus. Die Aufklärungsquote lag 2016 bei Fällen von Cyberkriminalität bei gerade einmal 38,7 Prozent. Insgesamt gab es 82.649 Fälle von Cyberkriminalität – gegenüber 2015 übrigens eine Zunahme um 80,5 Prozent. Dazu gehören Delikte wie Computerbetrug, das Ausspähen, Abfangen oder Verändern von Daten ebenso wie Computersabotage. Zum letztgenannten Delikt zählen auch die so genannten DDoS-Attacken, die ganze Systeme und Webseiten lahmlegen und dann den Betreiber erpressen. Und laut Lagebild des Bundeskriminalamts ist auch das organisierte Verbrechen inzwischen im Internet angekommen, kauft sich dort seine Hacker ein und nutzt das Deep beziehungsweise Dark Web für dunkle Geschäfte. Die Polizei und Experten verweisen im Übrigen darauf, dass die Zahlen des Lageberichts nur die Spitze des Eisbergs sind, denn nur ein Bruchteil aller Cyber Crimes kommt überhaupt zur Anzeige. Viele Unternehmen wenden sich an private Cyberwehren, die sie von Schadprogrammen befreien sollen.

Hohe Schäden

Unternehmen gehören zu den bevorzugten Zielen von Hackern und Spionen. Für eine Studie des Branchenverbands Bitkom wurden über 1.000 Geschäftsführer und Sicherheitsverantwortliche aus allen Branchen befragt. Das Ergebnis ist niederschmetternd: Mehr als die Hälfte der Unternehmen in Deutschland (53 Prozent) wurde in den vergangenen beiden Jahren Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl. Der dadurch entstandene Schaden wird auf rund 55 Milliarden Euro pro Jahr geschätzt. Wenn man bedenkt, dass diese Schadensumme die Folgekosten von Cyberangriffen beziffert, drängt sich der Gedanke auf, dass eine Investition in umfassende IT-Sicherheit vermutlich günstiger wäre. Erschreckend ist auch die Zufälligkeit, mit der Cyberkriminalität entdeckt wird. 30 Prozent der betroffenen Unternehmen entdeckten nur zufällig, dass es IT-Security-Vorfälle gegeben hatte. Auf die eigenen Sicherheitssysteme war kein Verlass – ob die Technik versagte oder falsch eingesetzt worden war, konnte nicht festgestellt werden. Lediglich ein Prozent der befragten Unternehmen gab an, durch eigene Sicherheitssysteme wie Virenscanner oder Firewall auf sicherheitsrelevante Vorgänge aufmerksam geworden zu sein.

Die Ergebnisse der Bitkom-Studie weisen darauf hin, dass deutsche Unternehmen die IT-Sicherheit noch nicht mit dem gebotenen Ernst betrachten. Kleinere Unternehmen werden sich manchmal überfordert fühlen oder nicht über das entsprechende Know-how verfügen. Doch langfristig betrachtet, führt kein Weg an der Aufrüstung der IT-Sicherheit vorbei. Gängige Lösungen wie Virenschutz und Firewalls waren laut einer Studie des Bundeswirtschaftsministeriums schon 2011 bei nahezu 100 Prozent der Unternehmen vorhanden und über 90 Prozent aller KMU ergriffen technische Maßnahmen wie Authentifizierung per Passwort, regelmäßige Backups, Spamfilter und Patches sowie Updates für Software. Komplexere Sicherheitslösungen werden aber deutlich seltener eingesetzt und daran hat sich nach Meinung von Experten bis heute nicht viel geändert.

Schnell handeln

Wenn das Unternehmen gehackt wurde, gilt es schnell zu sein, denn Hacker versuchen meistens, das ganze System zu infizieren. Nur durch Schnelligkeit können die Schäden gering gehalten werden. Am Anfang steht immer die Bestandsaufnahme: Welche Systeme sind von dem Angriff betroffen? Welche Daten wurden gestohlen? Im Falle von Erpressung sollte ebenfalls der Schaden analysiert werden. Falls der Hacker Daten zum Beweis vorlegt, muss überprüft werden, ob sie tatsächlich echt sind. Wer gehackt wurde, hat verständlicherweise den Drang, das Einfallstor, die Sicherheitslücke sofort zu schließen. Experten halten das nicht immer für ratsam, denn der Hacker könnte sich neue Wege suchen. Besser sei es, alle Stellen zu finden, an denen sich der Eindringling bereits eingenistet habe. Dann könne man alle Verbindungen kappen.
Es empfiehlt sich, Vorbereitungen für einen Cyber-Angriff zu treffen, bevor er tatsächlich geschieht. Unternehmen sollten frühzeitig festlegen, wer verantwortlich für die Schadenabwehr ist, wie intern und extern kommuniziert werden soll und wie man im Falle von Lösegeldforderungen verfährt. Zum Beispiel sollte die Frage geklärt werden, ob man reagiert und Kontakt zum Erpresser aufnimmt. Sind von einem Angriff viele Unternehmen betroffen, könnte es durchaus sein, dass der Hacker an denen, die sich nicht rühren, das Interesse verliert. Und nicht jeder Hacker gibt die Daten frei, nachdem er Geld erhalten hat.

Nach dem Angriff ist vor dem Angriff

Eine Cyber-Attacke bringt die Lücken im Sicherheitssystem zum Vorschein und hilft dabei, sie zu schließen. Die IT-Abteilung sollte möglichst schnell und systematisch die Sicherheitsvorkehrungen erhöhen. Alle wichtigen Ebenen und Beteiligten im Unternehmen sollten einbezogen und informiert werden. Neben der IT sind vor allem das Management und die Rechtsabteilung ins Boot zu holen. Experten empfehlen außerdem so genannte Penetrationstests. Sie helfen dabei, die eigenen Kontrollen zu bewerten, Schwachstellen zu identifizieren und zu beheben. Darüber hinaus ist es wichtig, herauszufinden, woran die Hacker Interesse hatten, welche Daten sie haben wollten. Mit jedem Detail, das über den Angriff und die Täter bekannt ist, lässt sich Sicherheit gezielter gestalten.
Nicht vergessen sollten Unternehmen, dass auch Mitarbeiter eine Schwachstelle sind. Irgendjemand wird immer einen E-Mail-Anhang öffnen oder auf einen Link klicken und schon ist es passiert – dem Angreifer steht die Unternehmenswelt offen.

Völlige Sicherheit wird es nicht geben. Ziel der IT-Sicherheit sollte es sein, Angreifern das Eindringen so schwer wie möglich zu machen. Wer etwas Wertvolles im Haus hat, verlässt sich nicht auf die Haustür, sondern installiert zusätzlich einbruchhemmende Fenster und ein Alarmsystem, lässt Hunde laufen und baut einen Tresor ein, den er hinter einem Gemälde versteckt. Mit Sicherheit gibt es einen Meisterdieb, der alle Hindernisse überwindet, aber die Masse der Diebe scheitert schon am Alarmsystem. ■

Ist der Feind im System, ist er nur schwer zu entdecken.