Empfehlungen

Datensicherheit – Angriffe im Netz nehmen zu

28. März 2018, von Irène Wilson

Die Panzerknacker von heute sind Schreibtischtäter – Hackerangriffe sind ein lukratives Geschäft. Wie sich Unternehmen davor schützen können, erklärt unser Partner und IT-Forensik Experte, Rogier Teo, im Interview der aktuellen Ausgabe des ZKB Kundenmagazins.

Steuererklärung, E-Banking, Ferienbuchung: Was erledigen Sie online?

Ich nutze alle Möglichkeiten. Zum Beispiel wickle ich meine Bankgeschäfte übers Internet ab, seit vor 20 Jahren die ersten Onlinebanken entstanden sind.

Dürfen wir uns also darauf verlassen, dass unsere Daten sicher sind?

Wir müssen zwischen unserem Bequemlichkeits- und unserem Sicherheitsbedürfnis abwägen. Absolute Sicherheit gibt es weder in der virtuellen noch in der physischen Welt. Banken und Versicherungen stehen relativ gut da, denn Sicherheit gehört seit jeher zu ihrem Kerngeschäft. Bei anderen Anbietern, etwa bei Onlineshops und Social Media, setze ich mehr

Fragezeichen.

Laut Bundesamt für Polizei fedpol nimmt die Kriminalität im Internet zu. Warum?

Die Digitalisierung durchdringt unseren Alltag immer stärker; Online-Dienstleistungen nehmen rasant zu. Das vergrössert die Angriffsfläche. Es lohnt sich, Geld in Angriffe zu investieren. Hinzu kommt, dass man kein IT-Crack mehr sein muss, um sich in ein System einzuhacken. Mit einigen Online-Tools können sich Interessierte rasch über Sicherheitslücken informieren. Und mit einer Portscanner-Software lassen sich Eintrittskanäle in ein fremdes IT-System identifizieren.

Wer steht hinter den Angriffen?

Das Problem im Cyberbereich ist, dass der Angreifer unsichtbar bleibt. Das Bild vom Hacker als schrulligem Nerd trifft in immer weniger Fällen zu. Die Akteure sind in der Regel kriminelle Organisationen. Sie verfügen über eine „Geschäftsleitung“ und beschäftigen Spezialisten. Manchmal verkaufen sie ihre Dienstleistungen sogar über eine „Marketingabteilung“. Wo sie effektiv sitzen, lässt sich kaum ermitteln. Doch wer sie sucht, der findet sie.

Worauf sind die Hacker aus?

Die Motive reichen von Neugier über persönliche Rache bis zu rein finanziellen Interessen. Umweltaktivisten attackieren Konzerne, um brisante Akten an die Öffentlichkeit zu bringen. Andere wollen geistiges Eigentum ausspionieren oder an Kreditkartendaten gelangen. Manche Diebe ergattern Daten, um ein Lösegeld zu erpressen oder die Daten weiterzuverkaufen. Oder sie nehmen Online-Bestellungen in unserem Namen vor.

Wie viele Angriffe werden pro Tag auf Unternehmen ausgeübt?

Gemäss einer Untersuchung von 2017 finden in den USA jährlich über 130 gross angelegte, digitale Einbrüche statt; Tendenz steigend. Die effektive Zahl liegt, je nach Definition von „Angriff“, wohl im Millionenbereich.

Findet ein Wettrüsten zwischen „Gut“ und „Böse“ statt?

Es ist ein Katz-und-Maus-Spiel. Die Unternehmen versuchen, ihre IT so sicher wie möglich zu

gestalten. Hacker nutzen Sicherheitslücken aus.

Schützen sich Unternehmen denn ausreichend vor virtuellen Gefahren?

Schweizweit hat die Sensibilisierung zugenommen, auch dank der Melde- und Analysestelle Informationssicherung MELANI des Bundes. Die Budgets für Cybersecurity steigen.

In welchen Bereichen orten Sie Nachholbedarf?

Die grösste Schwachstelle ist der Mensch. Am wirksamsten ist es, die Mitarbeitenden zu schulen: keine sensiblen Daten offen herumliegen lassen, Passwörter nicht an die Tastatur des Laptops kleben, eine Passwort-Policy ein-führen. Brandgefährlich sind zudem Phishing-Mails-Mails, die vorgeben, von seriösen Absendern zu sein, und einen auffordern, bestimmte Angaben zu machen.

Mit welchen Massnahmen können Unternehmen die Daten von Kunden schützen?

Jedes Unternehmen braucht ein Sicherheitskonzept. Es geht darum, darüber nachzudenken, welche Daten man besitzt, wie man sie anhand ihrer Vertraulichkeit klassifiziert und entsprechend schützt. Dann dürfte es sinnvoll sein, dass Mitarbeitende nur Zugriff auf Daten haben, die sie für ihre Arbeit benötigen. Hinter vielen Datendiebstählen stecken Interne, nicht Externe. Bei Kundendaten empfiehlt es sich, sie zusätzlich zu verschlüsseln. Auch sichere Netzwerkzonen sind wirksame Schutzmassnahmen. Darüber hinaus gilt es, regelmässig Sicherheitsprüfungen durchzuführen und die Systeme aktuell zu halten.

Ist das mit kleinem Budget überhaupt möglich?

Die meisten Massnahmen sind nicht kostspielig. Viele einfache Sicherheitsmassnahmen lassen sich im Internet recherchieren. Nehmen wir an, ein kleiner Handwerksbetrieb pflegt eine Kundendatei auf einem PC. Trennt man den PC vom Internet, ist er relativ sicher.

Etwas lässt sich noch nicht online erledigen: Abstimmen und Wählen. Woran liegt das?

Um das Vertrauen in das demokratische System nicht zu gefährden, müsste ein digitales Wahlsystem gefeit sein gegen Manipulation und Personen zweifelsfrei identifizieren. Der Prozess würde ziemlich kompliziert – und kostspielig.

Das komplette Interview inkl. wichtigen Tipps betreffend Does and Don’ts finden Sie hier.

Zum ganzen Artikel

Irène Wilson

Irene Wilson ist auf digitale Forensik und eDiscovery spezialisiert und hat im Laufe ihrer langjährigen Erfahrung für Kunden aus einer Vielzahl von Branchen in ganz Europa gearbeitet. Zu ihren Qualifikationen gehören die renommierten Master-Titel für Nuix Workstation und Nuix Discover.

Swiss FTS AG | www.swiss-fts.com | +41 43 266 78 50 | info@swiss-fts.com

https://swiss-fts.com/blog/datensicherheit-angriffe-im-netz-nehmen-zu-1