ANGST IM UNTERNEHMEN

Fast täglich erfahren wir von Hacker-Angriffen und von millionenfach gestohlenen Passwörtern. Schwachstellen in Computerprogrammen erhöhen die Wahrscheinlichkeit eines Angriffs, auch auf das eigene Unternehmen; und werden Updates nicht genügend schnell eingespielt, nimmt man unnötiges Risiko in Kauf.

Von *Andreas Wisler**

Ransomware

Vielleicht können Sie sich noch an die vielen Ransomware-Vorfälle vor zwei Jahren erinnern: Auf Bahnsteigen in ganz Deutschland blieben ein ganzes Wochenende lang die Abfahrtsanzeigen leer und die Ticketautomaten aus. Seither wurde es wieder ruhig, doch in Wellen schwappen neue Versionen von Schadsoftware durch das Internet. Das Ziel ist immer das gleiche: Nach einem unbedarften Klick wird der Schädling installiert und alle Daten verschlüsselt. Während – oder noch fieser: nach – der Installation erscheint eine Anzeige mit der «Bitte», eine bestimmte Anzahl Bitcoins an eine Adresse zu senden. Erst dann kann das Kennwort heruntergeladen und die eigenen Daten wieder entschlüsselt werden. Die Verschlüsselungstechnik ist so gut, dass ohne Backup alle Daten für immer verloren sind.

Phishing

Phishing hat immer Hoch-Konjunktur: Auf verschiedene Arten werden Empfänger einer Mail verführt, auf einen Link zu klicken oder anderweitig aktiv zu werden. Verschickten die Betrüger früher plumpe E-Mails ohne persönliche Anrede, in schlechtem Deutsch und schlechter Gestaltung, sind diese heute viel raffinierter: Persönliche Anrede und perfektes Deutsch, ja sogar teilweise auf Schweizerdeutsch, verleiten dazu, doch darauf zu klicken. Auch die vorgeschobenen Beweggründe der Absender verleihen den Phishing-Mails zunehmend Echtheit: Der Schädling kann z.B. in einer schön gestalteten Bewerbung im PDF- oder Word-Format versteckt sein; auch Rechnungen sind bei Phishern beliebt. Doch lassen Sie sich nicht in die Irre führen: Durch ein gesundes Mass an Zweifel können solche E-Mails erkannt werden, um sie gleich zu löschen.

Cloud

Ohne Cloud geht es heute nicht mehr. Viele Dienste sind gar nicht mehr als lokale Software-Lösung verfügbar, sondern nutzen auf die eine oder andere Art die Cloud.

Doch sind die Daten auch geschützt? Das ist schwierig zu beurteilen, denn auch in der Cloud entdecken Angreifer immer wieder Schwachstellen, um sie auszunutzen; daher gilt es, die Daten zusätzlich zu verschlüsseln. Eine Möglichkeit ist die Software «BoxCryptor», die alle Daten verschlüsselt, bevor sie sie in die Cloud überträgt. Sollte der eigene Zugang zu den Daten dann «gestohlen» werden, kann der Hacker damit doch nichts anfangen.

Spuren im Netz

Jede Aktivität im Internet wird aufgezeichnet und ausgewertet. Allein das Aufrufen von vier verschiedenen Schweizer Tageszeitungen zeigt, dass über 200 weitere Webseiten im Hintergrund geladen wurden. Auch wenn Sie kein Profil bei einem sozialen Dienst haben, sind Sie dort bekannt – zwar noch nicht als identifizierte Person, aber als «Nummer». Mit jeder Webseite, die Sie anklicken, geben Sie mehr Daten über sich Preis. Auch die Zeit, die Sie auf einer Seite verbringen, kann heute gemessen und ausgewertet werden. «Aber ist es denn so gefährlich, wenn ich anschliessend Werbung erhalte, die zu mir passt?» fragen Sie sich vielleicht. Vermutlich nicht. Aber was wird sonst noch alles über uns gespeichert? Hier liegt die grosse Gefahr: Gemäss verschiedener Studien wurden durch das Sammeln von Daten im grossen Stil sogar schon Wahlen beeinflusst.

Aktualität von Systemen

Das stetige Aktualisieren des Betriebssystems und der verwendeten Applikationen ist eine wichtige Aufgabe; dabei spielt es gar keine Rolle, ob es ein Windows- oder Mac-Computer ist, denn auf beide haben Hacker es abgesehen. Hacker greifen Systeme mit bekannten Schwachstellen an.
Der Aufwand, neue Schwachstellen aufzudecken, ist sehr gross; es ist also für einen Angreifer einfacher, die Nachlässigkeit der Benutzer auszunutzen: Fehlt diesem eine Software-Aktualisierung, ein sogenannter Patch, kann schon der einmalige Besuch einer Webseite genügen, sich einen Schädling einzufangen. Diese Angriffsmethode nennt sich Drive-by – es benötigt noch nicht einmal einen Klick dazu. Und auch wenn es manchmal nervt, wenn eine Software schon wieder meldet, dass ein Update zur Verfügung steht – installieren Sie es, verschieben Sie es nicht auf morgen!

Passwörter

Praktisch alle Systeme verlangen ein Passwort. Doch wie sieht ein gutes Passwort aus? Mindestens zehn Stellen sollten es heute sein, denn die Rechenleistung zum «Knacken» von Passwörtern wird immer besser und schneller; so stehen z.B. für Windows im Internet kostenlose Dateien für Passwörter fixfertig zum Download bereit (so genannte Rainbow-Tables). Damit kann ein Passwort von bis zu acht Stellen in weniger als 15 Minuten geknackt werden.

Ausserdem sollte man dringend für jeden Dienst bzw. Webseite ein eigenes Passwort verwenden:

Wird dann die eine Webseite gehackt – und das waren in den vergangenen Wochen viele, auch namhafte – kann der Hacker nicht gleichzeitig auf die anderen Dienste zugreifen. Und es kommen doch einige Passwörter zusammen – zwischen 50 und 100 sind es beim normalen Benutzer schnell. Viele Experten empfehlen zudem, das Passwort komplex zusammenzustellen, d.h. mit Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen. So viele und solch komplizierte Passwörter im Kopf zu haben, ist schlicht nicht möglich. Zwei Lösungen dafür, die den Alltag vereinfachen, sind KeePass und LastPass: Bei KeePass wird eine verschlüsselte Datei angelegt; beim Aufruf einer Webseite kann das Passwort dann mit einem Klick übernommen werden. Bei LastPass wird die verschlüsselte Passwortdatei via Internet synchronisiert – doch das birgt einige Risiken, die vor der Nutzung abgeklärt werden müssen.

Ein Vorteil ist aber die Möglichkeit, Passwörter in der Familie (Private Version) oder mit den Geschäftskollegen (Business Version) zu teilen.

Zertifizierungen

Die nötige Datensicherheit stellt viele Unternehmen vor grosse Herausforderungen: Gesetze wie die DSGVO (Datenschutz-Grundverordnung der Europäischen Union – die Schweizer Version folgt noch in diesem Jahr) müssen eingehalten werden. Die ISO-27001-Norm hilft, eine solide Basis dafür zu schaffen: Der erste Teil dieser Norm umfasst Aufbau, Unterhalt und Pflege eines ISMS (Informations-Sicherheits-Management-System), der zweite umfasst 114 Massnahmen. In der ISO 27002 werden diese Massnahmen ausführlich erläutert; sie umfassen aber nicht nur technische Elemente wie Zugriffskontrolle, Verschlüsselung, den Betrieb der IT, (sichere) Datenübertragung oder die Entwicklung von Software, sondern auch Anforderungen an Inventar, das Führen der Dokumentation, physische Anforderungen (Zutritt, Arbeiten in Sicherheitsbereichen usw.) sowie die Sicherheitsanforderungen gegenüber Lieferanten und Partnern.

FAZIT

Die Informationssicherheit hat viele Facetten:

Es ist nicht mit einer einmaligen Schulung oder einer Umsetzung einer einzelnen Massnahme getan; es gehört dazu, dass viele Zahnräder ineinandergreifen. Wenn die verschiedenen Aspekte, die hier behandelt wurden, regelmässig neu betrachtet werden, kann die Sicherheit auf einem hohen Niveau gehalten werden, um Angriffe ins Leere laufen zu lassen.

Autor

** Andreas Wisler ist Senior IT-Security Auditor und Inhaber der goSecurity GmbH (https://goSecurity.ch). Er berät unter anderem Unternehmen bei der erfolgreichen Einführung eines ISMS nach ISO 27001. Zudem unterrichtet er an der Fachhochschule Nordwestschweiz verschiedene IT-Security-Themen. Unter https://andreaswisler.com kann sein Blog verfolgt werden.*