Was wirklich schützt

Über den richtigen Einsatz von Security

Wenn es um Security geht, höre ich oft: „Schaden kann es nicht“, „Besser als gar nichts“ oder gar „Je mehr Schutz, desto besser“. Nein, nein und noch mal nein!

Von Jürgen Schmidt

Security darf man nicht mit der Gießkanne verteilen, weil viele Sicherheitsmaßnahmen unerwünschte und äußerst sicherheitsrelevante Nebenwirkungen haben. Schlechte Security kann sehr wohl gefährlich und damit schlimmer sein als „gar nichts“. Und zu restriktive Security-Maßnahmen führen entweder dazu, dass man Dinge überhaupt nicht mehr sinnvoll benutzen kann – mit entsprechenden, negativen Konsequenzen. Oder die Menschen finden kreative Workarounds, um sich das Leben trotz Security wieder erträglich zu machen. Da sich die gefährlichen Mantras hartnäckig halten, sollen ein paar konkrete Beispiele die damit verbundene Gefahr illustrieren.

„Schaden kann es nicht?“

Die als Teil von Internet-Security-Suiten verkauften Personal Firewalls versuchten lange Zeit, nur ausgewählten Programmen wie dem Browser und dem Mailer Zugang zum Internet zu gestatten. Außerdem versprachen sie, Angriffe zu erkennen und die Netzwerkpakete der offenbar bösen Systeme zu blockieren. Das sollte etwa Trojaner daran hindern, Schadcode aus dem Internet nachzuladen und Angriffe von außen im Keim ersticken.

Trotzdem schafften es Trojaner, an diesen Sperren vorbeizukommen. Dafür funktionierten plötzlich viele andere Dinge nicht mehr, die auf eine Internet-Verbindung angewiesen waren. Das führte nicht nur zu einer unglaublichen Verschwendung von Zeit für die Fehlersuche, sondern auch zu echten Sicherheitsproblemen. So kappten Personal Firewalls etwa den Auto-Update-Mechanismus von Programmen. In der Folge infizierten sich Anwender durch die Nutzung veralteter, unsicherer Versionen ihrer Anwendungen. In c’t-Tests gelang es uns mehrfach, Personal Firewalls dazu zu bringen, die Update-Server für Viren-Signaturen auf die schwarze Liste böser Systeme zu setzen und damit die Updates von Antiviren-Software zu blockieren. Das angebliche Mehr an Security schadete also durchaus.

„Besser als gar nichts?“

Bei der Verschlüsselung von Verbindungen über ein unsicheres Netz (Transport Layer Security, TLS) aktivierten viele Administratoren als Fallback für veraltete Software auch Verschlüsselungsverfahren, von denen bereits bekannt war, dass sie sich knacken ließen. Dieses Knacken koste trotzdem Aufwand und der Fallback sei allemal besser als die Daten im Klartext zu versenden, war die auf den ersten Blick durchaus einleuchtende Begründung.

Dass das so trotzdem nicht stimmt, beweist etwa die 2016 demonstrierte DROWN-Attacke. Das Akronym steht für Decrypting RSA with Obsolete and Weakened eNcryption und beschreibt das Prinzip des Angriffs schon recht gut. Die Angreifer erzwingen dabei den Einsatz der veralteten Verschlüsselung gemäß SSLv2. Diese können sie mit überschaubarem Aufwand knacken.

Der Clou dabei ist, dass sie damit das zentrale Geheimnis des Servers errechnen können, das all seine Verbindungen schützt – auch die eigentlich sicheren. Mit diesem Pre-Master-Secret können die Angreifer dann nachträglich sogar Daten entschlüsseln, die mit dem aktuellen TLS 1.2 gesichert waren. Dieses Problem betraf damals rund ein Drittel aller HTTPS-Webserver. Die veraltete Verschlüsselung war eben nicht besser als gar keine Verschlüsselung, sondern eine akute Gefahr.

„Je mehr Schutz, desto besser?“

Gute Passwörter sind lang und enthalten eine Mischung aus Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen. Sicherheitsbewusste Administratoren setzen das dann etwa so um, dass man nur Passwörter mit mindestens 12 Zeichen eingeben kann, die dem beschriebenen Mix entsprechen. Außerdem müssen die Anwender jeden Monat ein neues Passwort wählen. Die können sich diese Passwörter natürlich nicht merken und greifen zu praktischen Notwehrmaßnahmen. Sie schreiben sie auf Zettel, die sie unter der Tastatur oder bestenfalls in Schreibtischschubladen deponieren.

In einem realen Fall fehlte eine wichtige Datei für eine Präsentation im Konferenzraum. Die Nutzung von USB-Sticks war – wegen der davon ausgehenden Gefahr – untersagt und durch versiegelte USB-Ports unterbunden. Ein gemeinsam genutztes Netz und Austauschordner für Arbeitsplatz-PCs und die im Konferenzraum gab es natürlich auch nicht. Die Präsentation drohte zu platzen, weil die wichtige Datei nicht herbeizuschaffen war.

Das wurde dann so gelöst, dass ein Kollege die Datei per E-Mail an den privaten Mail-Account des Präsentators schickte, auf den er via Web-Mail auch im Konferenzraum zugreifen konnte. Die hochsensiblen Daten wurden also unverschlüsselt übers Internet verschickt und lagen dann nahezu ungeschützt bei einem Mail-Provider. Auf Nachfragen bestätigte der Mitarbeiter, dass diese Vorgehensweise durchaus üblich sei, weil der Austausch von Dateien zwar immer wieder notwendig, aber „wegen der Security“ nicht anders möglich sei.

Weniger ist manchmal sogar mehr!

Das Problem sind in beiden Fällen nicht die Mitarbeiter. Die versuchen nur, irgendwie ihren Job zu machen – trotz Security. Das Problem sind Admins, die Security über die Bedürfnisse der Mitarbeiter stellen. Mehr Anwenderfreundlichkeit und weniger Pseudo-Schutz führt häufig zu mehr Sicherheit.

Lange Rede, kurzer Sinn: Wer sich richtig schützen will, setzt Security maßvoll und zielgerichtet ein: so viel wie nötig, aber auch so wenig wie möglich. Dazu muss man natürlich wissen, was wovor schützt, was es nicht gewährleisten kann und welche Nebenwirkungen die gewählten Maßnahmen haben. Die folgenden Artikel klären das für die Bereiche Malware, Internet, Dateien und Zugänge. *(ju@ct.de)* c't