Cyber-Spionage-Angriffe reissen auch 2015 nicht ab

Im zurückliegenden Jahr gab es zahlreiche Security-Zwischenfälle im Cyberspace – von Spionage und Sabotage bis hin zu folgeschweren Hackerangriffen. Doch welche Lehren wurden aus diesen Attacken gezogen, und welche Gefahren lauern im Jahr 2015? Autor: Candid Wüest

Obwohl das Internet der Dinge bereits bei den Nutzern Einzug gehalten hat, werden TVs oder Kühlschränke in diesem Jahr nicht das Hauptangriffsziel von Hackern sein. Staatliche Schadprogramme, der Missbrauch von elektronischen Zahlungsmitteln, die Verwundbarkeit von Open-Source-Plattformen sowie das überholte Passwortsystem werden die Sicherheitsexperten im Jahr 2015 dafür aber umso mehr beschäftigen.

Staatlich finanzierte Cyberangriffe sind Realität

Im Jahr 2014 haben staatlich finanzierte Spionage- und Sabotageangriffe wie DragonFly, Turla oder Regin die Öffentlichkeit aufgeschreckt. Auch 2015 werden solche Angriffe nicht abreissen. Dabei wird versucht, Staats- und Industriegeheimnisse auszuspionieren und Organisationen zu sabotieren. Sowohl der private wie auch der öffentliche Sektor müssen daher ihre aktuelle Cyber-Sicherheitslage überdenken und die eigene Sicherheit bei Investitionen priorisieren, um gegen solche Angriffe gewappnet zu sein.

Elektronische Zahlungsmethoden werden ins Visier genommen

Der Verkauf von gestohlenen Kredit- oder Debitkartendaten auf dem Schwarzmarkt ist ein lukratives Geschäft für Cyberkriminelle. Es ist aber eher unwahrscheinlich, dass es in Europa zu Grossangriffen auf Point-of-Sale-Systeme wie in den USA kommen wird, da die meisten europäischen Karten dank des Chip- und PIN-Systems eine höhere Sicherheit bieten als die magnetstreifenbasierten Karten in den USA. Trotzdem besteht weiterhin das Risiko, dass elektronische Zahlungsmittel auch in unseren Breitengraden für betrügerische Onlineeinkäufe verwendet werden.

Da immer mehr Smartphones Near Field Communication (NFC) unterstützen, werden sich solche kontaktlosen Zahlungsmittel auch bei uns immer grösserer Beliebtheit erfreuen. In London und anderen Grossstädten wird diese Technologie bereits rege genutzt, etwa beim Bezahlen von Tickets im öffentlichen Verkehr. Die zunehmende Popularität ruft aber Hacker auf den Plan, die einzelne NFC-Transaktionen in einmaligen Angriffen ausspähen könnten.

Open-Source-Plattformen bleiben anfällig

Es ist davon auszugehen, dass auch 2015 neue Schwachstellen in Open-Source-Datenbanken und auf Webservice-Plattformen entdeckt und von Hackern ausgenutzt werden. Wie im Fall von Heartbleed und Shellshock stellen diese Schwachstellen ein attraktives Ziel für Angreifer dar. Das grösste Risiko geht aber nach wie vor von Schwachstellen aus, die zwar bekannt sind, aber von Unternehmen und Konsumenten noch nicht gepatched wurden.

Dass Open-Source-Plattformen im Fokus von Hackern stehen, zeigt zum Beispiel auch die erst kürzlich entdeckte Schwachstelle mit dem Übernamen Ghost im Linux-Betriebssystem. Ghost ermöglicht es Angreifern, unter bestimmten Bedingungen die Kontrolle über ein anfälliges System zu übernehmen.

Heutiges Log-in-/Passwortsystem hat bald ausgedient

Unternehmen versuchen, Wege zu finden, um Schwachstellen zu verhindern und ihre Endnutzer zu schützen. Es zeichnet sich ab, dass aufgrund dieser Bemühungen allmählich Alternativen zum alten Log-in-System eingesetzt werden. Dazu gehört zum Beispiel die Zwei-Faktor-Authentifizierung (2FA): Diese benötigt etwas, das nur der rechtmässige Besitzer weiss – etwa ein Passwort – sowie etwas, dass nur er besitzt – etwa ein Smartphone. Da Serviceanbieter immer häufiger auf dieses Verfahren zurückgreifen, werden auch die Anwender verstärkt auf verschiedene Apps, Telefonnummern und Sicherheitsfragen angewiesen sein – und dies über verschiedene Plattformen hinweg. Sich dabei zurechtzufinden, kann für die Nutzer am Anfang vielleicht zur Herausforderung werden, führt aber letztlich zu mehr Sicherheit.

Engere Zusammenarbeit zwischen Unternehmen und Strafverfolgungsbehörden absehbar

Die jüngsten internationalen Verhaftungen im Jahr 2014 sind Beweis dafür, dass internationale Strafverfolgungsbehörden aktiver und bestimmter mit Cyberverbrechen umgehen und mit der digitalen Sicherheitsbranche zusammenarbeiten. Dieses gemeinsame Vorgehen ist ein Versprechen für die Zukunft, da Cyberkriminalität auf diese Weise noch effektiver bekämpft werden kann.

DER AUTOR

Candid Wüest
Virenforscher und Principal Threat Researcher bei Symantec