Das Sicherheitsjahr 2012

Blick in die Glaskugel

Elmar Török, bits+bites

Zu Anfang des Jahres wagen Hersteller und Branchenkenner gern einen Blick in die Glaskugel: Was wird in den nächsten 12 Monaten in puncto Sicherheit passieren? Wir fassen aus den zahllosen Prognosen einige der wahrscheinlichsten Trends zusammen.

Achtung Hacktivisten: Hackergruppen wie Lulzsec oder Anonymous greifen weiterhin staatliche Stellen und Unternehmen an

„Prognosen sind äußerst schwierig, vor allem, wenn sie die Zukunft betreffen". Auch wenn nicht ganz klar ist, wer für dieses schöne Bonmot nun letztendlich verantwortlich ist – Mark Twain, Karl Valentin und Winston Churchill gelten als Kandidaten – bleibt die Aussage im Kern richtig. Doch unsere Jahresvorschau für 2011 lag in vielen Punkten durchaus richtig, die IT-Security-Szene ist, bei aller Aktualität und Schnelllebigkeit, eben doch in gewissem Maß einschätzbar. Basierend auf den zahlreichen Herstellerprognosen für 2012 haben wir einige Trends ausgewählt, die unserer Ansicht nach große Chancen haben, das Jahr in Sachen Sicherheit zu dominieren.

Mobil ist Trumpf

2011 kann man getrost als das Jahr des Tablet-PCs bezeichnen. Die tragbaren Internet-Zugangsgeräte erlebten einen Boom sondergleichen, vor allem das iPad, aber auch die diversen Ableger, die meistens Android-Betriebssysteme nutzen. Schon Anfang 2011 zeichnete sich ab, dass diese mobilen Endgeräte verstärkt im Fokus der Angreifer stehen würden. Unübersichtliche Softwareangebote in AppStores und die große Verbreitung zogen Angreifer unwiderstehlich an. Nachdem sich die Tablets immer weniger aus Firmen und deren Netzen heraushalten lassen, oft weil Vorstand oder Geschäftsführer die größten Fans davon sind, werden die Geräte immer mehr zum Problem für die IT-Abteilungen werden. Einer Ponemon-Studie aus dem Sommer 2011 zufolge griffen in diesem Jahr in 78 Prozent der befragten Unternehmen mehr als doppelt so viele, persönlich genutzte Endgeräte auf das Unternehmensnetzwerk zu, als noch vor zwei Jahren. 63 Prozent der Studienteilnehmer glauben, dass ein Zusammenhang zwischen diesem Trend und der zunehmenden Häufigkeit von Sicherheitsvorfällen besteht.

Die Problemfälle sind mögliche Schadsoftware und die Frage, wie man mit vertraulichen beruflichen Daten auf den Tablets umgehen soll. Bislang unterstützen noch sehr wenige Device Management Lösungen alle Aspekte der Tablets in ausreichendem Umfang. 2012 werden mit Sicherheit mehr Hersteller dieses Thema adressieren, sodass im Laufe des Jahres für IT-Administratoren genügend Werkzeuge zur Verfügung stehen dürften, damit Bring Your Own Device (BYOD) an Problempotenzial verliert.

Die meisten Sorgen hatten Regierungen und Großunternehmen 2011 Stuxnet bereitet. Angriffe auf kritische Infrastrukturen abseits der IT rückten plötzlich Schadsoftware in ein neues, viel bedrohlicheres Licht. Bislang sind Ausfälle auf breiter Ebene ausgeblieben, auch wenn mit Duqu bald ein Nachfolger mit ähnlich destruktiver Wirkung auf der Bildfläche erschien. Die Ruhe auf dem Gebiet trügt aber, wie Alexander Gostev, Chief Security Expert bei Kaspersky Lab warnt: „Waren bis dato vor allem Unternehmen und staatliche Organisationen im Fokus, die mit Waffenfertigung, Finanztransaktionen oder High-Tech- sowie wissenschaftlicher Forschung im Zusammenhang stehen, erwarten wir im nächsten Jahr eine Ausweitung der Angriffsziele auf Unternehmen aus der Rohstoffgewinnung, Energie-, Verkehrs-,

Lebensmittel- und Pharmaindustrie sowie Internet-Services und IT-Sicherheitsunternehmen“. Immerhin hatten Stuxnet und Duqu die Wirkung eines heilsamen Schocks auf viele Unternehmen und Kunden der Automatisierungsbranche. IT-Sicherheit – traditionell ein sehr vernachlässigtes Anhängsel in diesem Bereich – erfährt gerade eine enorme Bedeutungssteigerung. Besser spät als nie.

Für die gute Sache hacken

Wikileaks war als Konzept eine gute Sache, wie die Veröffentlichungen gehandhabt wurden, ist eine komplett andere Geschichte. Aber zumindest konnte man bei den Aktivisten davon ausgehen, dass sie lediglich als Plattform für vorhandene Daten agierten. Mittlerweile sieht man jedoch eine ganze Reihe an sehr aktiven Hackergruppen wie Lulzsec und Anonymous, die politisch motivierte Angriffe auf Institutionen starteten, um deren tatsächliche oder angenommene Verfehlungen zu ahnden. Deren Angriffspalette reicht von einfach gestrickten Hack-Szenarien bis hin zu beträchtlichen Datenschutzverletzungen. Weil die Angriffe in der Regel sehr medienwirksame Ziele und manchmal auch genauso attraktive Ergebnisse haben, können die „Hacktivisten“ mit viel öffentlicher Aufmerksamkeit rechnen. Robin Hood meets Matrix, so könnte man das nennen. Gegen Attacken auf die mexikanische Drogenmafia ist auch nichts einzuwenden, außer der hohen Gefahr, in die sich die Hacktivisten damit bringen. Wer allerdings das Adressbuch von Tony Blair veröffentlicht, Online-Spieleserver lahmlegt und in die Server des US-Parlaments eindringt, muss mit einer gehörigen Portion Skepsis hinsichtlich seiner Ziele rechnen.

Nicht alles ist neu und unbekannt, was die IT-Sicherheitswelt angeht. Der mittlerweile fest etablierte Ansatz, Hacken als Mittel zur finanziellen Bereicherung einzusetzen, wird weiterhin konsequent umgesetzt. So prognostiziert Imperva, dass DDoS in den kommenden Monaten neue Ausprägungen finden und noch effektiver sein wird. Die Hakker werden nicht nur die Netzwerk-, sondern verstärkt die Anwendungs- und sogar die Geschäftslogikebene angreifen. Hauptziel werden unsichere Webanwendungen sein. Das Problem dürfte jetzt schon unangenehm große Ausmaße haben, nur scheuen die meisten betroffenen Firmen den Weg an die Öffentlichkeit. Kurz vor Weihnachten wurde eine zumindest teilweise erfolgreiche, mehrtägige DDoS-Attacke auf den Elektronik-Versandhändler Conrad bekannt. Wenn ein derartig großes Unternehmen mit einer seit vielen Jahren etablierten und erprobten eCommerce-Website Probleme bekommt, bedeutet das nichts Gutes für kleinere Unternehmen.

SSL im Kreuzfeuer

Immer mehr Webanwendungen werden über das HTTPS-Protokoll übertragen. Daher fokussieren Angreifer ihre Attacken zunehmend auf die verschiedensten SSL-Komponenten. Nach den spektakulären Angriffen auf Zertifizierungsstellen wie DigiNotar haben viele Unternehmen erkannt, wie gefährdet die Basis der Zertifikatsstruktur eigentlich ist. In Zukunft müssen sie auch den Inhalt ihres SSL-Verkehrs überprüfen – und zwar ohne Einbußen bei der Leistungsfähigkeit des Netzwerks. Zudem werden auch die Hersteller von Webbrowsern neue Wege finden müssen, um sichere und vertrauenswürdige Verbindungen anzuzeigen. Denn das bekannte Schloss-Symbol und eine grüne Adresszeile werden zukünftig kein großes Vertrauen mehr beim Anwender erwecken.

Überhaupt entwickelt sich der Browser zum absoluten Dreh- und Angelpunkt aller Angriffsvektoren. Die Weiterentwicklungen innerhalb der IT-Sicherheitsbranche hinsichtlich der Abwehr gezielter Angriffe sowie das gewachsene Bewusstsein der Öffentlichkeit zwingt die Cyberkriminellen, neue Instrumente zu entwickeln. Die herkömmliche Methode der Angriffe via E-Mail und das damit verbundene Ausnutzen von Sicherheitslücken wird zunehmend weniger effektiv werden, Attacken beim Einsatz von Browsern werden hingegen an Popularität gewinnen. Und auch wenn das Thema 2011 relativ wenig Beachtung fand, dürfte sich in 2012 IPv6 erheblich stärker bemerkbar machen. Die Architektur von IPv6 bringt jedoch besondere Security-Anforderungen mit sich. In einigen Organisationen könnte IPv6 bereits ohne Wissen des Netzwerkadministrators in den Unternehmensnetzen im Einsatz sein und von Hackern oder Botnets als verdeckter Kanal genutzt werden. Weil dieses Jahr zahlreiche Unternehmen zu IPv6 migrieren werden, sollten die Organisationen mit Bedacht überlegen, was für einen sicheren Übergang zu IPv6 erforderlich ist. Auch die beiden anderen fundamentalen Eckpfeiler des Internet - Border Gateway Protocol und Domain Name System - stehen in einer Next-Generation-Version zur Verfügung. 2012 werden viele zu diesen neueren Versionen wechseln und eine neue Runde an Schwachstellen und Exploits eröffnen.

Fehlen darf natürlich auch das Lieblingsthema der Firmen und Medien in 2011 nicht: Cloud Computing. Mittlerweile gibt es ausreichend Anbieter und Anwendungen, die Cloud Computing in allen seinen Ausprägungen umsetzbar machen. Und wie jede populäre Technologie wird auch die Cloud vermehrt ins Visier der Angreifer geraten. Der Skaleneffekt ist einfach zu verlockend, als das Hacker nicht versuchen würden, über Attacken auf Cloud-Provider an Daten und Rechnerkapazität zu kommen. Vielleicht wird es 2012 noch keinen großen geglückten Angriff geben. Erste ernsthafte Versuche sind aber auf alle Fälle zu erwarten.