

Was bringt 2009?

Voraussagen für die IT-Sicherheit

Elmar Török, bits und bites

Das einzig Beständige ist der Wandel. Das gilt umso mehr für einen schnelllebigen Bereich wie die IT-Sicherheit. Trotzdem versuchen wir mit Hilfe von Analysten und Herstellern einen Ausblick auf 2009 zu geben.

Das ausgehende Jahr 2008 war von einem bestimmenden Thema geprägt: der globalen Finanzkrise, die mittlerweile in zahlreiche andere Bereiche des täglichen Lebens hineinwirkt. Als wäre das nicht schon schlimm genug, liefert die Nachrichtenlage Spammern und Phishing-Betrüger massenhaft neue Munition. So wird die Wirtschaftskrise auch in Zukunft eine vielseitige Grundlage für zahlreiche neue Angriffe bieten. Dazu gehören Phishing-Attacken rund um das Thema insolvente oder scheinbar insolvente Banken genauso wie E-Mails mit falschen finanziellen Versprechungen oder gefälschte Scam-Sites von Jobvermittlern. Und auch das kann man schon jetzt mit Sicherheit sagen: im Jahr 2009 bleibt Spam ein Thema. Bill Gates scheint mit seinen Prognosen wenig Glück zu haben. Nach seinem (vermutlich) legendären Arbeitsspeicherzitat (640 kByte sind genug...) hatte er 2004 prognostiziert, dass sich das Spamproblem in zwei Jahren erledigt haben wird.

Datenschutz bleibt im Fokus

Das Jahr 2008 war geprägt durch eine Rekordzahl von Datenschutzlücken. Allein von T-Mobile tauchten 17 Millionen Kundendaten bei Adresshändlern auf. Dies war kein Einzelfall. Experten sind davon überzeugt, dass heute die Adressen fast aller Bundesbürger im Umlauf sind und auch Millionen von Kontendaten illegal kursieren.

Die öffentlich bekannt gewordenen Sicherheitslecks sind dabei nur die Spitze des Eisbergs. Die Öffentlichkeit nimmt diesen Schlendrian mit ihren persönlichen Informationen zunehmend wahr. In der Security-Index Studie auf Seite 9 haben die Befragten, verglichen mit vergangenen Untersuchungen, deutlich mehr Befürchtungen, dass ihre Daten missbraucht werden. Und laut einer aktuellen Umfrage von Utimaco im Oktober 2008 waren 61 Prozent von 1.043 Befragten der Meinung, Unternehmen würden den Schutz ihrer persönlichen Daten eher vernachlässigen. Eine überwältigende Mehrheit von 82 Prozent plädierte sogar für eine Bestrafung von Unternehmen und Behörden, wenn sie ihre Sorgfaltspflicht beim Datenschutz verletzen. Jedes Mal, wenn sensible Kundendaten verloren gehen, gerät die Kundenloyalität in Gefahr. Sie ist direkt abhängig von der Fähigkeit von Unternehmen, Kundendaten wirksam zu schützen. Im kommenden Jahr werden Unternehmen dafür noch mehr als bislang investieren, um zu verhindern, dass Kundendaten gestohlen oder unabsichtlich publiziert werden. Wenn wir schon bei der bösen Absicht angekommen sind: verärgerte oder enttäuschte Ex-Mitarbeiter sind deutlich eher dazu geneigt, Informationen zu entwenden. Und davon dürfte es in diesem Jahr eine ganze Menge geben, jetzt, wo die Finanz- zu einer Wirtschaftskrise geworden ist. Wo in diesem Jahr aufgrund der verschärften Rezession Jobs verloren gehen und Mitar-

beiter entlassen werden, sind sensible Unternehmensdaten einem erhöhten Risiko ausgesetzt. Allerdings muss man noch nicht einmal Böses im Sinn haben, um Schlechtes zu tun. Die wachsende Mobilität von Mitarbeitern und Tools trägt ebenfalls zum potenziellen Verlustrisiko bei. Die aktuell so beliebten Netbooks kann man überall hin mitnehmen, man kann sie allerdings auch überall vergessen und liegenlassen. An Verschlüsselung denkt bei den Geräten bislang so gut wie niemand.

Mehr und strengere Vorgaben

Als Konsequenz aus einer Reihe von Datenschutzverstößen im Bereich der Privatwirtschaft hat die Bundesregierung das Bundesdatenschutzgesetz überarbeitet und in verschiedenen Punkten verschärft. Hier kommen 2009 zusätzliche Anforderungen auf die Unternehmen zu. Einzelne Vorschläge aus dem Gesetzgebungsverfahren greifen aber zu kurz und verfehlen das Ziel, den Missbrauch von Kundendaten wirksam zu unterbinden. Eine Lösung könnte das Vorgehen der US-Bundesstaaten Kalifornien und Nevada sein. Dort gibt es seit 1. Oktober ein „Verschlüsselungsgesetz“: Unternehmen müssen sensible Daten verschlüsseln und sie müssen protokollieren, welcher Mitarbeiter zu welchem Zeitpunkt auf Kundendaten zugreift. Damit lässt sich recht einfach die berechtigte Nutzung der Kundeninformationen

vom absichtlichen Missbrauch trennen. Gehen Daten verloren und sie sind nicht verschlüsselt, sind Firmen und Organisationen darüber hinaus verpflichtet, Datenverluste den Betroffenen und der Öffentlichkeit sofort mitzuteilen.

von Trojanern steigen. Diese Entwicklung wird sich 2009 fortsetzen, die Angreifer, denen IT-Sicherheitsbeauftragte gegenüber stehen, sind nicht zu unterschätzen. Auswertungen von Symantec zeigten, dass heute täglich insgesamt mehr böserartige als legale Programme entwickelt werden.

Attacken abgelöst. Darum dürfte sich trotz angespannter wirtschaftlicher Lage an den Ausgaben für die IT-Sicherheit wenig ändern, wie die Analysten von IDC glauben. Auch wenn die Budgets insgesamt knapp sind, die meisten Firmen wissen mittlerweile, dass sie ein geglückter Hackerangriff noch teurer kommt und verheerende Auswirkungen auf ihr Image haben kann.

Dauertrend Virtualisierung

Virtualisierung ist schon seit mindestens drei Jahren ein Dauerbrenner in den Firmen, dabei wird es auch 2009 bleiben. Die Kostenvorteile durch bessere Auslastung der Hardware und – im Idealfall – vereinfachtes Management sind einfach zu verlockend. Mittlerweile steht die nächste Generation von Virtualisierungslösungen vor der Tür, die den Desktop der Mitarbeiter als Stream bereitstellen und so noch stärker von der physischen Hardware entkoppeln. Darum muss die Virtualisierungstechnologie aufbreiter Front in Sicherheitslösungen integriert werden – mit dem Effekt, dass der so geschaffene Schutzraum vom Chaos einer allgemeinen Betriebssystem-Umgebung unberührt bleibt. Diese Technologie sorgt für eine sichere Umgebung für sensible Transaktionen, wie z.B. Bankgeschäfte, und schützt die kritische Infrastruktur, wie Sicherheitskomponenten, die ihrerseits die Sicherheit der allgemeinen Betriebssystem-Umgebung gewährleisten. Damit dürfte 2009 das Jahr der Virtualisierungssicherheit werden. Und noch etwas ist in 2009 wahrscheinlich: verschiedene Produktbundles speziell für den Mittelstand werden die aktuellen Sicherheitsanforderungen aus Information Protection, Verschlüsselung und Umsetzung einheitlicher unternehmensweiter Sicherheitsrichtlinien adressieren. Damit sind auch kleine und mittlere Unternehmen deutlich einfacher als heute in der Lage, ihre sensiblen Firmendaten umfassend zu schützen.



Darf's ein bisschen mehr sein?
Online aktive Kriminelle professionalisieren ihre Aktivitäten zunehmen (Quelle: Symantec).

Die Firmen hingegen werden durch zunehmende Wirtschaftsspionage geplagt. Den Schaden, der deutschen Firmen dadurch entsteht, beziffern Experten auf bis zu 50 Milliarden Euro jährlich - Tendenz steigend. China und Russland gelten als besonders aktiv in diesem Bereich. Ob die Angriffe nun von einer Regierung kommen oder von „freien Unternehmern“, fest steht, dass sich die Malware-Szene in den letzten 12 Monaten extrem professionalisiert und kommerzialisiert hat. Mit Erfolg, denn die Nutzungsgebühren für Bot-Netze und die Kosten für das Maßschneidern

Aber nicht nur Unternehmen stehen im Fokus der Angriffe. Im Jahr 2008 war ein deutlicher Anstieg von Bedrohungen auszumachen, die sich gegen Social Network-Seiten richteten. Dazu gehörten Phishing-Attacken, um an die Nutzeraccounts zu kommen, als auch der Missbrauch des sozialen Kontextes, um die Erfolgsquote eines Angriffs zu steigern. Spammer haben vermehrt Social Network-Seiten aufs Korn genommen – ein Vorfall bei Facebook führte zu einer Rekordstrafe von 873 Millionen US Dollar gegen den Spammer. Solche Bedrohungen werden zunehmend auch für Unternehmen relevant, da insbesondere junge Mitarbeiter „ihre“ Social Network-Seite oft von ihrem Arbeitsplatz aus frequentieren. In dem Fall stellt weniger Spam als Phishing die Gefahr dar. Denn nach wie vor bieten Browser-Schwachstellen Angreifern einen idealen Ansatzpunkt für Attacken, dagegen helfen auch Firewalls nur bedingt. In dem Maß, in dem die angebotenen Web Services zunehmen und Browser einen einheitlichen Interpretationsstandard für Scripting Sprachen nutzen, werden webbasierte Bedrohungen wahrscheinlicher und gefährlicher werden. Schon heute hat das Web die E-Mail als Haupteinfallstor für