Datenschutz als Wettbewerbsvorteil

Erich Moechel , futurezone.ORF.at

Während die Welle primitiven Phishings abebbt, ohne dass in Europa nennenswerte Schäden entstanden wären, hat sich eine neue, “höhere” Form der Netzkriminalität gebildet. Zur Abwehr von “gezielten Attacken” auf ausgewählte Mitarbeiter und damit auf die Firmendaten zum Zwecke von Betrug, Erpressung und Wirtschaftsspionage gibt es im Zeitalter von Web 2.0 keine rein technische Lösung.

Datenschutz gegen Identitätsbetrug

Von Spam und ebenso lästigen wie letztlich harmlosen Wurm-Ausbrüchen abgesehen, sind die neueren Wellen von "Cybercrime" an Kontinentaleuropa ohne wirkliche Schäden vorbeigegangen.

Während die Kombination von organisiertem Datendiebstahl und Identitätsbetrug in den USA seit 2002 jährlich Schäden um die 50 Milliarden US-Dollar anrichtet, ist das Delikt außer in Großbritannien kaum Thema für Europas Kriminalisten.

Zurückzuführen ist das auf mehrere Faktoren. Während überall in Europa Mitte der 80er Jahre mehr oder weniger starke Datenschutzgesetze entstanden, wurden persönliche Daten in den USA damals zur Handelsware. Daraus resultiert einerseits eine unterschiedliche Mentalität im Umgang mit personenbezogenen Daten.

Vor allem aber hat die Kombination von Melderegistern, Ausweispflicht sowie die stärkere Haftung der Banken im hochregulierten Europa dafür gesorgt, dass der Teufelskreis aus Datendiebstahl samt zugehörigem Schwarzmarkt und dem eigentlichen Delikt "Identitätsbetrug" gar nicht erst in Gang kam. Diese Masche lohnt sich für Kriminelle in Europa einfach nicht. Können wir uns daher zurücklehnen? Leider nicht.

"Qualitätssprung" der Netzkriminialität

Die Evolution der Netzkriminalität ist bereits in der nächsten Phase angelangt. Wie es Evolutionen nun einmal an sich haben, geht damit ein "Qualitätssprung" einher, gegen den staatliche Regulierungen nichts ausrichten können.

Anstatt mit "gemeinem Phishing" auf's Geratewohl die Unbedarften und Unvorsichtigen abzuzocken - in Österreich gab es 2007 fast keine Schadensfälle mehr – benutzen fortgeschrittene Kriminelle und “halbstaatliche” Organisationen spätestes seit 2003 andere, höherwertige Methoden. Mit gezielten Attacken ["Targeted Attacks" oder auch “Spear-Phishing”] werden größere Fische angegriffen, nämlich Behörden, Institutionen und Unternehmen, weil hier in jeder Beziehung mehr zu holen ist. Die Angriffe laufen in der Regel nicht auf einfachen Betrug hinaus, sondern auf "höhere Formen" der Kriminalität wie etwa Wirtschaftsspionage und Erpressung.

Fremde Datensätze

Der zunehmende elektronische Datenaustausch zwischen Unternehmen führt dazu, dass immer mehr geschäftskritische Datensätze in immer mehr verschiedenen Unternehmensdatenbanken landen.

Von ausgelagerten Buchhaltungen angefangen über Dienstleister bis zu Projekten, an denen mehrere Firmen, Consultants, Zulieferer usw. beteiligt sind, werden große Mengen von Datensätzen ausgetauscht. Diese landen in firmeneigenen EDVs, aber auch auf Laptops und sogar Privat-PCs der Mitarbeiter. Den meisten Unternehmen ist dieses Mehr an Risiko in puncto Haftung durch die exorbitant gewachsene Zahl "fremder", zu verwaltender Datensätze nicht wirklich bewusst.

Das Vordringen des Internets in den Lebensalltag eröffnet zudem ganz neue, gezielte Angriffsmöglichkeiten auf Mitarbeiter von Firmen. Stichworte: "Soziale Netzwerke" und "Social Engineering".

Aus den Statistiken der Anti-Virenhäuser läßt sich nur der allgemeine Trend absehen. Ende 2007 dominierten immer neue Varianten teils altbekannter Würmer [z.B. Netsky] neben Trojanern. Im Dezember 2007 war etwa die bekannte Trojaner-Familie Backdoor.Win32.Rbot gleich um 673 verschiedene, neue Versionen gewachsen. Diese Statistiken bilden im Wesentlichen nur die Tools der "Infrastruktur-Betreiber" ab, die ihr Netzwerk aus gekaperten Rechnern an das Gros der gemeinen Spammer bzw. gewöhnlichen Phisher vermieten.

"Social Engineering"

Die wirklich gefährlichen - und lukrativen - Attacken aber spielen sich abseits der Viren-Hitparade ab. Für gezielte Attacken verwenden die professionellen Angreifer eben nicht mehr Varianten bekannter Schadprogramme, sondern so genannte "Zero-Day-Exploits". Hier werden ganz aktuelle Sicherheitslücken ausgenützt, von Virenscannern bleibt diese Art von Angriffen daher meist unentdeckt.

Statt Würmern transportiert "Social Engineering" einen Trojaner auf den Rechner eines bestimmten Mitarbeiters und damit ins Netz des angegriffenen Unternehmens. Der Angreifer ist nämlich über sein Opfer sehr gut informiert, da im Zeitalter von Web 2.0 vom Beruf bis zum Verhalten in der Freizeit immer mehr personenbezogene Daten öffentlich zur Verfügung stehen.

"Zero-Day-Exploits"

Die gängigste Angriffsform sind momentan Word- und Excel-Dateianhänge an eine E-Mail, die wiederum ist vom Absender über Betreff, Anrede und Text bis hin zum Anhang individuell auf eine Zielperson oder eine Gruppe zugeschnitten. Allein bei Excel fanden sich im Lauf des Jahres 2007 17 neue Sicherheitslücken, von denen einige nachweislich für derartige Angriffe mit "Zero-Day-Exploits" genutzt wurden. Diese fortgeschrittene Form der Kriminalität ist relativ schlecht dokumentiert, denn anders als die gemeinen Phisher/Spammer fallen diese Angreifer in den Antivirus-Statistiken eben nicht auf.

Da die betroffenen Unternehmen in der Regel wenig Interesse haben, den Tatbestand öffentlich zu machen, ist eine hohe Dunkelziffer anzunehmen. Angegriffen wurden in den USA seit Jahren neben Behörden und großen Unternehmen auch innovative KMUs.

Am Beispiel China

Eine im Februar 2008 bekannt gewordene Untersuchung, der eine kritische Masse von Fällen zugrunde liegt illustriert diese Entwicklung. Seit 2003 sind die chinesische Glaubensgruppe "Falun Gong" einer ganzen Serie von "Targeted Attacks" mit E-Mails und Office-Dokumenten, die zumeist "Zero-Day-Exploit"-Trojaner enthalten, ausgesetzt.

Vom "Social Engineering" her, also in puncto Überzeugungskraft, sind die E-Mails professionell

gestaltet, denn die Texte sind genau im Stil der jeweiligen Gruppe gehalten, die Inhalte der angehängten Dokumente ebenfalls. Bis auf ein kurzes Ruckeln der Office-Applikation beim Öffnen des Dokuments ist nichts davon zu bemerken, dass sich gerade ein Trojaner eingenistet hat.

Der "halbstaatliche Sektor"...

Hier sind wir im "halbstaatlichen" Sektor angelangt, wo "targeted attacks" vor allem aus dem Osten an der Tagesordnung sind. Vor ihrem Besuch in der Volksrepublik China 2007 hatte sich die deutsche Bundeskanzlerin Angela Merkel gar öffentlich über gezielte Trojaner-Attacken aus China auf bundesdeutsche Ministerien beschwert. In allen Fällen ging es weniger um politische Spionage, die Angreifer suchten vielmehr nach Informationen, die wirtschaftlich verwertbar waren.

Für österreichische KMUs, die typischerweise eine relativ kleine, dafür hochspezialiserte Produktpalette haben, kann eine einzige, erfolgreiche Datenattacke auf das Firmen-Know-How daher fatale Folgen haben. Der Schutz der eigenen Daten vor gezielten Angriffen kann nur über die Mitarbeiter selbst erfolgen, weil die – neben Sicherheitslücken in Web-Applikationen und Firmennetzen – die einzigen wirklichen Angriffspunkte sind.

... und der staatliche

Die Liechtensteinische Justiz sucht nach dem Informanten, der Konto-Daten deutscher "Steuersparer" aus der Bank LGT entwendet und um fünf Millionen Euro an den deutschen Bundesnachrichtendienst verkauft hat. Davor war die Liechtensteinische Landesbank mehrfach auf dieselbe Weise erpresst worden – man drohte mit Übermittlung der gestohlenen Daten an die deutsche Finanz - hier sollen neun Millionen geflossen sein. In allen Fällen handelt es sich um "Targeted Attacks" auf ganz bestimmte Datensätze, allerdings ganz ohne "Social Engineering" und eingeschmuggelte Schadsoftware. In allen Fällen waren die "Trojaner" nämlich Angestellte der betroffenen Bank.

Und: Der so genannte "Bundestrojaner", den die Innenminister Deutschlands und Österreichs als neues Ermittlungsinstrument der Polizei durchsetzen wollen, ist – strukturell gesehen – geradezu ein Musterbeispiel für eine "Targeted Attack."