



Cybercrime: Wie man sich davor schützt

Microsoft schätzt die Bedrohung durch Viren derzeit eher klein ein. Vielmehr sind DOS/DDOS und Malware-Attacken, Social Engineering und Wirtschaftsspionage Themen, welche die grossen Unternehmen beschäftigen. Und das wird auch in naher Zukunft so sein. **VON MARCO MARCHESI UND CHRISTOPH BAUMGARTNER**

Noch vor vier Jahren wurden Systeme hauptsächlich von Script-Kiddies, interessierten junge Menschen, angegriffen. Diese haben sich inzwischen zu versierten «Hobby-Hackern» und Auftrags-hackern weiterentwickelt. Während Script-Kiddies aus Neugier handelten, waren Hobby-Hackern Ruhm und Anerkennung ihrer Kollegen wichtig. Heute stehen wirtschaftliche und je nach Ausprägung nationale Interessen als Beweggrund für Spionageakte im Vordergrund. Wirtschaftsspionage klingt nach Grosskonzern, Militär oder CIA – aber längst sind auch Privatbanken und mittelständische Betriebe in der Schweiz davon betroffen.

Überall wo Geld im Spiel ist, wird organisiert, gut organisiert. Otto-Normalverbraucher kann sich heute Bot-Netze mieten oder eine DoS-Attacke als Dienstleistung im Internet kaufen. Das Angebot ist vielfältig.

Marc Henauer von der Fedpol weiss, dass solche Aktionen heute an der Tagesordnung

sind. Durch die Angebotsvielfalt kann sich heute ein Hobby-Hacker Zugang zu hochspezialisierten Werkzeugen verschaffen. Die Akteure sind Hobby-Hacker, Experten (-Organisationen) und Spezialisten mit ausgezeichnetem Wissen. Diese werden von Firmen oder in nationalem Interesse für entsprechende Aufgaben engagiert. Sie führen Angriffe aus und nutzen dabei noch nicht veröffentlichte Schwächen von Standardprodukten aus oder individualisieren Malware für gezielte Zwecke.

Finanzielle Motive

Die Tatsache, dass heute meist finanzielle, respektive gewinnbringende Absichten im Vordergrund stehen, führt dazu, dass Angriffe sehr leise geschehen. Script-Kiddies oder Hobby-Hackern schien es recht, wenn ein Angriff erkannt wurde und ihr Name in den News erschien. Moderne Angriffe sollen aus Sicht des Angreifers nicht mehr erkannt werden, der Daten- und Know-how-Verlust

möglichst unbemerkt bleiben. Damit ist High-Noise-Malware out.

Wirtschaftsspionage ist so alt wie die Wirtschaft selbst. Mit den technischen Möglichkeiten von heute kann sie aber äusserst effizient und kostengünstig betrieben werden. Die Methode «Phishing» und deren potenzielle Opfer sind aufgrund der Medien allgemein bekannt. Dies führte auch zu einer gesteigerten Security Awareness der Bevölkerung. Viel gefährlicher ist die Kombination von Social Engineering und gezielten technik-gestützten Attacken.

Es folgt ein auf Tatsachen basierendes Szenario: In einer Firma wird eine neue Raumpflegerkraft beschäftigt, die am frühen

Marco Marchesi ist CEO der ISPIN AG, President der ISSA Schweiz und im Vorstand von Infosurance und Datenschutzforum.ch www.ispin.ch
Christoph Baumgartner ist CEO der international tätigen Sicherheitsberaterin Oneconsult GmbH www.oneconsult.com

von seinem Chef – mit den korrekten Anhängen. Inzwischen hat die Spyware (die vermeintlichen Protokolle und Konzepte) un bemerkt und systematisch wertvolle Informationen gesammelt und rausgeschickt – über Umwege direkt zur Konkurrenz. Und das in der korrekten, gut abgesicherten Schweiz.

Mittel gegen Spionage

Wie begegnen wir solchen Bedrohungen? Einerseits werden wir lernen müssen, mit derartigen Bedrohungen und vereinzelt entsprechenden Schadensfällen zu leben. Andererseits können wir uns darauf vorbereiten. Die Erkennung solcher Angriffe ist der erste Schritt. Anti-Spyware-Programme, Intrusion-Detection-Systeme (IDS) sind technische Mittel zur Erkennung. Der Datenfluss muss genau bekannt sein. Beim Aufbau und Design einer Online-Banking Architektur ist dies zwingend, damit ein wirksamer Schutz gewährleistet werden kann. Ist ein IDS angedacht, muss überlegt werden, welcher Datenfluss wo erwartet wird und welcher nicht, damit die Alarmierungsschwelle exakt eruiert und justiert werden kann. Andernfalls liefert das IDS zwar viele Daten mit welchen nichts angefangen werden kann. In einem solchen Fall ist das IDS zwar physisch präsent, aber nutz-

Abend, wenn der eine oder andere Mitarbeiter noch im Büro ist, ihre Reinigungsarbeiten durchführt. Sie bekommt ein Gespräch mit, in welchem der Chef einem Mitarbeiter ein Mail mit Anhängen (Protokolle und Konzepte) ankündigt. Am nächsten und den darauf folgenden Tagen ist die Raumpflegerkraft nicht mehr im Hause. Sie ist zurückge reist an ihre eigentliche Wirkungsstätte und beschafft sich auf dem Markt geeignete Software-Tools und bereitet den Angriff vor. Sie verfasst eine E-Mail im Namen des Chefs, fügt die vermeintlich erwarteten Anhänge hinzu und sendet die E-Mail an den Mitarbeiter, der die E-Mail von seinem Chef erwartet. Hand aufs Herz – wer würde nicht auf die Anhänge klicken? Komischerweise startet dann aber das Textverarbeitungs- oder Tabellenkalkulationsprogramm nicht. Weil der Mitarbeiter noch mit einer anderen Aufgabe beschäftigt ist, hakt er nicht nach, sondern arbeitet an etwas anderem weiter. Am nächsten Tag erhält er die echte E-Mail

ILLUSTRATION: CWT/THU

WEITERE INFORMATIONEN

Management Summary

Die Gefahren kommen heute weniger von Viren und dergleichen, sondern vielmehr sind Wirtschaftsspionageakte an der Tagesordnung. Hobby-Hacker, Experten und Spionagespezialisten können heute wie Auftragshackings, Bot-Netze und DDoS-Attacken als Dienstleistungspaket engagiert beziehungsweise gekauft oder gemietet werden. Das Motiv hinter Spionageakten ist persönliche Bereicherung mittels Know-how oder Schädigung von Konkurrenten. Die Angriffe verlaufen daher sehr leise. Die wirklich kritischen Angriffe sind eine Kombination von Social Engineering und technischen Angriffen.

Wie begegnen wir diesen Gefahren?

Es ist heute unumgänglich ein umfassendes, ganzheitliches Sicherheitsdispositiv aufzubauen und zu betreiben:

- Auf technischer Seite gehört dazu eine State-of-the-Art-Sicherheitsarchitektur mit Perimeter-Schutz und Angriffserkennung, Applikationsschutz und Alarmierungsmechanismen.
- Auf organisatorischer Seite braucht es eine Alarmorganisation, Verantwortungen müssen klar definiert sein und die Mitarbeiter und Kunden müssen aufgeklärt werden, wie solche Angriffe stattfinden und was sie dagegen tun können.
- Technische Onlineplattformen müssen regelmässig durch Fachpersonen geprüft werden.

los. Die Alarmorganisation muss genau definiert sein. Wer ist wann für was verantwortlich? Es muss definiert sein, wer im Ernstfall entscheidet, ob die Onlineplattform ab dem Netz genommen werden soll und die Abkoppelung zeitnah durchsetzt.

Bei verteilten Systemen wie Online-Banking-Plattformen liegt die Achillesferse üblicherweise nicht beim Systembetreiber (in diesem Fall der Bank) sondern beim Benutzer. So werden die Applikationsserver mittels geeigneter Massnahmen vor unerlaubtem Zugriff geschützt und die Kommunikation mit dem Client-PC erfolgt verschlüsselt. Die prüfungswerten Aspekte sind insbesondere Authentisierung und Autorisierung. Nach neuestem Stand der Technik sollten (zertifikatsbasierte) 2-Weg-Authentisierungsmechanismen (SSL v3) und idealerweise 3-Komponenten-Authentisierung (User-ID, Passwort plus Smartcard/Secure-ID oder ähnliches) eingesetzt werden. Doch diese Massnahmen greifen nicht, wenn der Client von einem gezielt für diesen Zweck entwickelten Trojaner kontaminiert wurde – denn dann kann sich der Angreifer in die Kommunikation einklinken und beispielsweise gezielt Geld vom Konto des Opfers transferieren oder via Client in die Bankapplikation eindringen. Aus diesem Grund sollten sensible Applikationen mittels Application Security Audits inklusive Penetration-Tests auf System- und Applikationsebene überprüft werden.

Bewusstsein schärfen

Als Firma müssen Mitarbeiter lernen, mit Angriffsszenarien umzugehen. Diese permanente Security Awareness wird mittels Trainings- und Lernprogrammen gefördert. Am einfachsten geht dies, wenn das Interesse am Thema beim Benutzer so stark ist, dass er sich mit den Firmenwerten identifiziert und für die Sicherheit der Firma einsteht. Dann sprechen wir von Informationssicherheitskultur. Diese erreichen wir mit gezielten, auf die Firmenkultur abgestimmten Awareness-Massnahmen.

Um zu erreichen, dass Mitarbeiter eine Informationssicherheitskultur leben können, müssen ihnen entsprechende Werkzeuge mitgegeben werden. Das Tragen eines Sichtausweises sollte Pflicht sein. Inklusive der Verantwortung, einen Mitarbeiter ohne Sichtausweis zum Empfang zu begleiten. Wird dann zufälligerweise ein Verwaltungsratsmitglied zum Empfang begleitet, darf sich dieser glücklich schätzen über aktiv gelebte Sicherheit. Informationssicherheitskultur beginnt deshalb beim Management und muss vor- beziehungsweise mitgelebt werden. ■