Andreas Rieke, Martin Hühne

Angriffe von innen (II): Wirtschaftsspionage

Im ersten Teil dieser Artikelreihe (s. Ausgabe 6/2005) haben wir gezeigt, wie sich Eindringlinge durch die Manipulation von Netzwerk-Adressen (sog. ARP-Spoofing) Zugriff auf vertrauliche Unternehmensinformationen verschaffen können. Im zweiten Teil wollen wir das Umfeld näher betrachten, in dem sich solche Attacken ereignen, und davon ausgehend mögliche Konsequenzen erörtern.

„Die Konkurrenz hat uns schon wieder um einen Bagatellbetrag unterboten. Als ob die genau wüssten, was unter unserem Angebot stand!" Besonders in Technologie-orientierten Unternehmen häufen sich in jüngster Zeit solche und ähnliche Klagen. Die erschütternde Regelmäßigkeit, mit der solche Klagen auftauchen, lässt vermuten, dass einige Wettbewerber zum Teil ganz bewusst illegale Methoden einsetzen, um sich im Markt zu behaupten.

In der Tat belegen entsprechende Studien der Unternehmensberatungen KPMG und PricewaterhouseCoopers (PwC) aus den beiden zurückliegenden Jahren (vgl. [1] und [2]), dass über 70 Prozent der Unternehmen Wirtschaftsspionage als Bedrohung empfinden und mehr als vier Fünftel der Befragten damit rechnen, dass die Zahl einschlägiger Delikte in Zukunft steigen wird. Das liegt sicher auch daran, dass die internationalen Geheimdienste hier mittlerweile ein lohnendes Betätigungsfeld entdeckt haben.

Unternehmensspezifische Gegenwehr

Eine wachsende Zahl von Wirtschaftsspionage-Delikten zählt zur Kategorie CyberCrime: Einer KPMG-Studie zufolge sind in 84 Prozent der Fälle Mitarbeiter der angegriffenen Unternehmen beteiligt

Dabei fallen mehr und mehr der genannten Straftaten in die Kategorie CyberCrime. Diese Entwicklung wird vielfach deshalb unterschätzt, weil die meisten Betriebe inzwischen erhebliche Anstrengungen unternehmen, um sich gegen Angriffe von außen zu schützen. Doch tatsächlich wird die überwiegende Anzahl der Übergriffe aus den attackierten Unternehmen heraus begangen, die Täter sitzen also „hinter der Firewall": Den Ergebnissen der KPMG-Studie zufolge sind in 84 Prozent aller Fälle eigene Mitarbeiter beteiligt (s. Grafik), und bei der Hälfte der fraglichen Straftaten stellten die Opfer im Nachhinein ein Zusammenspiel mit externen Angreifern fest. Ein verantwortliches IT-Management wird diese Gefahr also in Rechnung stellen und bei der Entwicklung neuer Sicherheitsstrategien vor allem Vorkehrungen gegen die Spionage im eigenen Netz treffen.



Wirtschaftskriminalität in Deutschland 2003/2004

Voraussetzungen

Die meisten Angreifer agieren so geschickt, dass das Opfer ihre Aktionen – wenn überhaupt – erst im Nachhinein bemerkt

Eine der wichtigsten Voraussetzungen für erfolgreiche Wirtschaftsspionage ist, dass die Opfer Angriffe nicht als solche erkennen bzw. im Idealfall nicht einmal bemerken. Nur so lässt sich verhindern, dass sie Abwehrmaßnahmen ergreifen und Anzeige erstatten, was unmittelbare juristische Konsequenzen für die Angreifer und illoyalen Beschäftigten hätte. Schon deshalb müssen sich Datendiebe immer bemühen, nicht entdeckt zu werden – was am besten funktioniert, wenn sie sich mit Hilfe von Mitarbeitern auf einem der drei folgenden Wege Zugriff auf Unternehmensnetze verschaffen:

- **Physikalischer/physischer Zugang:** Ein Mitarbeiter könnte dem Angreifer Zugang zum Unternehmen und damit auch zum Serverraum oder Rechenzentrum verschaffen. Diese Variante ist sehr gefährlich, da viele Betriebe Zugangs- und Zutrittskontrollen vornehmen und die entsprechenden Einrichtungen per Video überwachen.
- **Virtueller Zugang mittels legitimer Kommunikation:** Ebenso gut können sich Angreifer per Modem, ISDN oder über ein VPN in das Unternehmensnetz einwählen und Daten ausspionieren. Damit sinkt zwar das Risiko, in flagranti erwischt zu werden, aber dafür lassen die Täter jede Menge Spuren zurück, da im Normalfall die gesamte Netzwerkkommunikation protokolliert wird. Anhand von Informationen wie Benutzername und IP-Adresse lässt sich ein Angriff meist relativ leicht zurückverfolgen, Staatsanwaltschaft und Polizei können die Ermittlungen ohne großen Zeitverlust aufnehmen.
- **Virtueller Zugang mittels nicht autorisierter Kommunikation:** Diese Variante setzt i. d. R. einen bewussten Verstoß gegen die Sicherheitsrichtlinien des Hauses und damit eine nicht unerhebliche kriminelle Energie des Mitarbeiters voraus: Seine Aufgabe besteht hier darin, präparierte Hardware wie beispielsweise externe Modems, ISDN-Karten oder WLAN Access Points ins Unternehmensnetz einzuschleusen, über die der Spion je-

derzeit auf das interne Netz zugreifen kann. Solange keine Augenzeugen oder Videoaufnahmen existieren, ist es nahezu unmöglich, derartige Angriffe nachzuweisen – selbst wenn das Gerät später gefunden wird, sind die verräterischen Informationen darauf meist längst gelöscht.

Ist der Zugang erst einmal hergestellt, hindert den Täter praktisch nichts mehr am Datenraubzug im Unternehmensnetz: In den im Folgenden dargestellten Szenarien benötigt er nicht einmal Kenntnisse der angegriffenen IT-Infrastruktur, um erfolgreich Konstruktionspläne, Forschungsergebnisse oder auch die eingangs erwähnten Vertragsangebote „abzugreifen".

Angriffsmöglichkeiten

Für Angriffe auf die Unternehmens-IT existieren drei Hauptvarianten

Nach dem illegalen Einloggen kann der Spion zwischen drei Vorgehensweisen wählen, um an die gewünschten Informationen zu gelangen. In der Praxis kommt jedoch üblicherweise nur ein Weg wirklich in Frage, wie wir schnell sehen werden:

- **Angriffe auf Serversysteme:** Bevorzugtes Ziel sind hier in der Regel die File- (also Datei-)Server des angegriffenen Unternehmens. Das hat zum einen den Grund, dass selbst ansonsten sicherheitsbewusste Organisationen hier noch immer eine Vielzahl unverschlüsselter Informationen aufbewahren. Zum anderen bieten die in letzter Zeit bekannt gewordenen Schwachstellen im Windows-Betriebssystem und im Linux-Fileserver *Samba* lohnende Ziele, deren Nutzung einen deutlich umfangreicheren Zugriff auf die angegriffenen Netze gewährt. Ein Hauptnachteil dieser Attacken ist, dass sie umfangreiches Betriebssystem- und Applikations-Know-how voraussetzen und somit schwierig auszuführen sind; zudem muss der Angreifer hoffen, dass der Administrator Sicherheitsupdates nachlässig einspielt. Last not least besteht die Gefahr, entdeckt zu werden: Denn obwohl Angriffe dieser Art im Normalfall unbemerkt bleiben, können sie durch forensische Untersuchungen nachgewiesen werden.
- **Angriffe auf PC-Arbeitsplätze:** Client-Systeme sind i. d. R. weniger gut geschützt als die Server, auf die sie zugreifen. Daher werden sie oft zum Ziel weniger ausgefeilter Attacken etwa mit Hilfe von Keyloggern, die alle Tastatureingaben aufzeichnen, um so beispielsweise Passwörter auszuforschen. Daneben lagern auf dem einzelnen Desktop jedoch meist nicht genügend wichtige Informationen, so dass Angriffe normalerweise nur dazu dienen, sich Zugriff auf die Server zu verschaffen. Eine Ausnahme bildet das „Hijacken" von Maschinen im Rahmen von DoS- und DDoS-Attacken.
- **Angriffe auf das Netz:** Hierzu zählen neben Angriffen auf Netzwerkhardware vor allem die im ersten Beitrag beschriebenen Layer-2- und Layer-3-Angriffe wie MAC-Flooding, ARP- oder

IP-Spoofing, die Schwachstellen in den Übertragungsprotokollen nutzen, um den Angreifer in eine günstige Position zu bringen. Auf diese Weise kann er als Man-in-the-Middle die gesamte Kommunikation mithören und alle Daten manipulieren - sogar in nachlässig aufgesetzten verschlüsselten Verbindungen.

Selbstverständlich existiert in den meisten Unternehmen ein Sicherheitskonzept, das geeignete Maßnahmen vorsieht, um sowohl externe als auch interne Angriffe zu erkennen und abzuwehren. Das ist allein schon wegen seiner abschreckenden Wirkung sinnvoll, denn die meisten professionellen Angreifer unterstellen die Existenz eines solchen Konzepts und verzichten von vornherein auf eine Reihe von Übergriffen.

Abwehrmaßnahmen

Die meisten Sicherheitskonzepte und punktuellen Maßnahmen helfen bei der Abwehr, bieten aber keinen durchgängigen Schutz

Zu den gängigen Schutzmaßnahmen gehört beispielsweise die Absicherung der Server durch Intrusion-Detection- bzw. Intrusion-Prevention-Systeme (IDS, IPS), die jeden nicht autorisierten Zugriff protokollieren und ggf. Alarm auslösen. Selbst wenn ein System im Einzelfall nicht geschützt ist, verfügt der Spion über genau diese Information in der Regel nicht und wird einen Angriff schon aus Vorsicht unterlassen.

Schwieriger gestaltet sich dagegen die Erkennung bzw. Abwehr von Angriffen auf das Netzwerk. Zwar lassen sich manche Übergriffe wie etwa das MAC-Flooding durchaus wirkungsvoll unterbinden (z.B. durch das Auslösen von Traps beim CAM table overflow), in der Praxis werden diese Möglichkeiten jedoch nicht ausreichend genutzt. Für andere Varianten, insbesondere das sehr gefährliche ARP-Spoofing, existieren bisher nur wenige Gegenmaßnahmen.

Wie Erfolg versprechende Abwehrstrategien aussehen und zu implementieren sind, erörtert Teil 3 dieser Serie im nächsten Heft.

[1] KPMG: Wirtschaftskriminalität in Deutschland 2003/04: Ergebnisse einer Umfrage bei 1.000 Unternehmen
[2] PwC Deutsche Revision: Wirtschaftskriminalität 2003: Internationale und deutsche Ergebnisse

Zu den Autoren:
Dr.-Ing. Andreas Rieke ist Geschäftsführer der ISL Internet Sicherheitslösungen GmbH mit Sitz in Hagen. Die ISL befasst sich schwerpunktmäßig mit der Erkennung, Lokalisierung und Abwehr von internen Angriffen.
E-Mail-Kontakt: andreas.rieke@isl.de.

Prof. Dr. rer. nat. Martin Hühne ist Professor im Fachbereich Informatik und Naturwissenschaften an der Fachhochschule Südwestfalen in Iserlohn und forscht in den Bereichen Rechnernetze und IT-Sicherheit.
E-Mail-Kontakt: huehne@elon07.fh-swf.de.