# Angriff und Verteidigung

## Die technischen Möglichkeiten der virtuellen Täter und die Gegenmassnahmen in den Unternehmen.

***Die heutigen Formen von Wirtschaftskriminalität über den Weg Internet erfordern zunächst eine Risikoanalyse und dann strategische Gegenschritte. Unser Autor beleuchtet einige technische Aspekte.***

von Jochen Kellner

Im Internet existieren zwei grundsätzlich verschiedene Typen von Angriffen oder Delikten. Beim ersten Fall handelt es sich um einen ungezielten Angriff (zum Beispiel durch Phishing oder Abklopfen von zufälligen Adressbereichen). Ob und wer Opfer des Angriffes wird, ist dem Täter zunächst egal - solange die Erfolgswahrscheinlichkeit eines einzelnen Angriffes gross genug ist.

Der zweite Prototyp ist genauer. Im Mittelpunkt steht ein gezielter Angriff auf ein bestimmtes Opfer, zum Beispiel die Entwicklungsabteilung, eines Unternehmens.

Gegen den ersten Angriffstyp hilft grundsätzliche Wachsamkeit und Vorsicht bei Angeboten, die zu gut klingen, als dass sie wahr sein können. Ausserdem sollten die beteiligten Systeme mit aktuellen Sicherheitspatches versehen sein und keine grundsätzlich unsicheren Programme wie Outlook oder Internet Explorer verwendet werden. Zusammen mit Firewall und Virenscanner kann zumindest ein Grundschutz gewährleistet werden.

**Phasen der Angriffe**

Viel gefährlicher ist der zweite Typ der Angriffe - da hier gezielt der Besitz einer Person oder eines Unternehmens angegriffen wird. Die Erfahrung zeigt, dass IT-Systeme früher oder später Sicherheitsprobleme aufweisen – auch wenn damit ein Angreifer sich in Geduld üben muss.

Ein typischer Angriff dieser Art besteht dabei aus den folgenden Phasen:

- Definition des Angriffsziels (Wer soll angegriffen werden und was soll der Angriff erreichen?)
- Auskundschaften (die ist beim ersten Angriffstyp nicht notwendig)
- Eindringen in die betreffenden IT-Systeme
- Auslesen oder Verändern der gespeicherten Daten

**Definition des Angriffsziels**

Erst mit Festlegung eines Angriffsziels ist eine Planung notwendig. Wenn sich im Laufe des Angriffes zeigt, dass das Ziel auf dem angepeilten Weg nicht erreichbar ist, dann kann es sinnvoll sein, zum Beispiel zunächst ein Tochterunternehmen oder einen Partner anzugreifen und von dort aus den Angriff fortzusetzen.

Wenn das Ziel nicht das Ausspähen von Daten, sondern das Verhindern des Zugriffes auf Dienste ist (Denial-of-Service), dann ist kein Eindringen in das Zielsystem notwendig. Stattdessen setzt man häufig fremde, durch Trojanische Pferde übernommene Rechner für eine «Distributed Denial- Of-Service»-Attacke ein.

**Auskundschaften**

Je mehr Informationen der Angreifer über das Zielobjekt hat, desto einfacher werden die nachfolgenden Schritte. Informationsquellen sind das Internet (Firmenwebseite, Stellenangebote, Foren/Newsgroups, in denen Administratoren technische Fragen stellen etc.). Mit Hilfe von Suchmaschinen und dem Internet-Archiv (http://www.archive.org) kann die Recherche praktisch ohne jeden Kontakt zur Firmen-Präsenz stattfinden.

Als zweiter Weg kommt «Social Engeneering» zum Einsatz, zum Beispiel durch Anrufe bei der Telefonzentrale oder DV-Verantwortlichen für eine fingierte Umfrage. Auch das Durchwühlen des Abfalles oder Umsehen an den Arbeitsplätzen fördert oft interessantes zu Tage. Zutritt kann man sich als Lieferant (Pizza, Blumen oder Berater) oder Besucher getarnt verschaffen.

Wichtige Informationen für den Angreifer sind die eingesetzte Software und die Versionen (um eventuell bekannte Sicherheitslücken ausnutzen zu können), So weist die Zeichenkette «wgate» in der URL möglicherweise auf den Einsatz des Internet Transaction Servers der SAP hin, oder man kann nach spezifischen URLs eines bestimmten Content Management System suchen.

Ebenfalls eine Quelle für die verwendeten Programme und Versionen ist Netcraft (http://toolbar.netcraft.com/site_report?url=http://www.jochen.org). Verfolgt man die Ziel-Domain längere Zeit, so kann man hier auch die Installation neuerer Versionen erkennen oder den Wechsel des Betriebssystems.

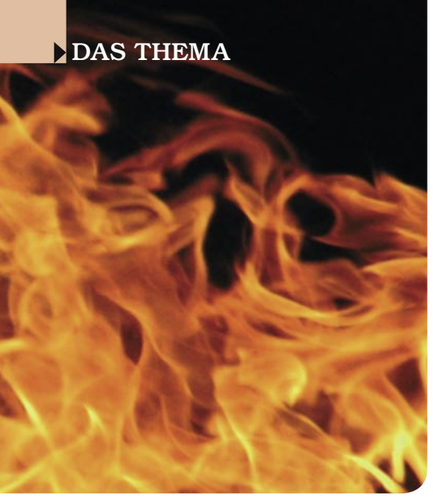
Zugangsdaten und Informationen über die Netzwerk-Infrastruktur sind ebenso hilfreich. Diese Informationen können möglicherweise über das Netzwerk ausgelesen werden (z.B. mit Hilfe von Analyse-Tools wie ethereal, oder diese Daten sind fälschlicherweise in öffentlich zugänglichen Verzeichnissen gespeichert), oder sind zum Beispiel auf ausgedruckten und dann entsorgten Listen enthalten.

**Gegenstrategien**

Gegen das Auskundschaften hat man praktisch keine rechtliche Handhabe. Der Aufruf der Internet-Seite oder diverser Suchmaschinen ist mit Sicherheit nicht strafbar (und in vielen Fällen auch nicht nachvollziehbar).

Eine Massnahme gegen das «Social-Engeneering» ist die Sensibilisierung der betroffenen Mitarbeiter, dass bei Anrufen von Fremden möglichst keine Informationen preisgegeben werden sollen. Auch sollten Mitarbeiter einen Ansprechpartner haben, dem sie (ohne Furcht vor Konsequenzen) Verdachtsmomente oder Vorkommnisse mitteilen können. Damit darf es aber nicht enden - eine Untersuchung und eventuelle Maßnahmen sollten folgen können.

Im Internet sollten Daten über das Unterneh-



**Zwei Möglichkeiten:** Überwinden der Firewall oder physisches Eindringen

men nur sparsam veröffentlicht werden. Das betrifft zum Beispiel Organigramme, Namen und Telefonnummern von Administratoren oder gar vollständige Telefonverzeichnisse.

Verwenden die Administratoren in öffentlichen Foren nicht eine Mail-Adresse der Firmen-Domain, sondern zum Beispiel einen Mail-Provider wie web.de, sind die Fragen nicht mehr dem Unternehmen zuzuordnen.

Das physische Eindringen kann man erschweren, indem Besucher sich nur in Begleitung im Hause bewegen dürfen. Das lässt sich aber bei externen Mitarbeitern (wie z.B. Beratern) nicht durchhalten.

**Türöffner**

Auch hier kann man grundsätzlich zwei Varianten unterscheiden: Beim ersten Fall geht es um das Überwinden der Firewall (Angriff über das Internet) und beim zweiten Fall um physisches Eindringen.

Das physische Eindringen wird durch die bekannten strafrechtlichen Sanktionen bestraft. Dabei ist oft das Eindringen einfach zu entdecken, insbesondere wenn Türen oder Schlösser beschädigt werden oder Computer, Festplatten oder Sicherungsbänder entwendet werden. Werden nur Daten auf mitgebrachte Datenträger kopiert, ist der Einbruch sehr viel schwerer nachzuweisen.

Auch kann ein Einbruch dazu verwendet werden, Keylogger oder Trojanische Pferde zu implementieren. Damit können Zugangsdaten ausgespäht werden, die für einen weiteren Angriff nützlich oder notwendig sein können. Heutzutage sind auch Rechner so klein, dass man beispielsweise eine Lauschstation an einen Druckerport anschließen kann, um den Netzwerk-Verkehr abzuhören (offene WLAN-Netze machen solch einen Angriff oft überflüssig).

Mit dem physischen Zugang zum Netz und ausgespähten Informationen kann es im nächsten Schritt wiederum einfacher sein, weitere Informationen mittels Social Engeneering zu erlangen. Je nach angestrebtem Ziel, kann und muss man in mehreren Schritten vorgehen und auf das bereits erlangte Wissen aufbauen.

Das Überwinden einer Firewall setzt Kenntnisse über die Zugriffsregeln und die angebotenen Dienste voraus. Diese können im Vorfeld mit einem Netzwerk-Scan (zum Beispiel mit nmap) erlangt werden - wobei Intrusion Detection Systeme diese Scans oft erkennen können. Hier zahlen sich Geduld und Ausdauer dadurch aus, dass der Scan möglicherweise unentdeckt bleibt.

In der Regel wird als Einfallstor nicht eine Fehlkonfiguration der Firewall dienen, sondern ein Angreifer wird Sicherheitslöcher in den verwendeten Applikationen ausnützen. Insbesondere sind dabei Methoden wie Cross-Site-Scripting und SQL-Injection (oder Abwandlungen davon)verbreitet und führen mit einer recht hohen Erfolgswahrscheinlichkeit zum Erfolg.

Auch hier kann sich Geduld auszahlen, damit nicht eine Vielzahl fehlgeschlagener Angriffe das Opfer alarmieren. Zudem kann es durch geänderte Konfiguration oder neuere Programmversionen zu neuen Sicherheitslücken kommen.

**Ausbeuten**

Nachdem ein Angreifer sich Zugang verschafft hat, kann er diesen für seine Ziele ausnutzen. Motivation kann sein, dass interne Daten entwendet werden sollen, zum Beispiel Angebote oder neue Entwicklungen. Diese Informationen können für ein Konkurrenz-Unternehmen interessant sein, um ein besseres Angebot abgeben zu können oder Entwicklungsergebnisse in eigenen Produkten zu verwenden.

Ein weiteres denkbares Ziel ist die Manipulation von Daten, entweder zu Gunsten des Angreifers oder mit der Absicht, dem Angriffsziel zu schaden (wie durch Gewinnausfälle oder zusätzlich entstehende Kosten). Auch kann das Stören eines Dienstes von innen einfacher und dauerhafter sein, als das als externe Denial-Of-Service-Attacke durchzuführen.

**Fazit**

Angriffe mit Computer-Mitteln sind ein Risiko für jedes Unternehmen, das wichtige, unternehmenskritische Daten mittels EDV verarbeitet. Ein Schutz ist niemals vollständig, aber grundsätzlich notwendig - alleine durch die Verantwortung des Managements gegenüber den Eigentümern.

Je nach wahrgenommener Bedrohung und erwartetem Ziel eines Angreifers, kann es verschiedene Massnahmen geben, entweder den Schaden zu begrenzen oder die Eintrittswahrscheinlichkeit zu verkleinern. Erfahrene Systemadministratoren kennen in der Regel die Schwachstellen ihrer Systeme - es ist notwendig diesen Mitarbeitern die Zeit und Möglichkeit zu geben, diese Schwachstellen zu schliessen.

Aussagen wie «wir sind sicher» oder «dafür habe ich keine Zeit» sind Alarmsignale, denn ein Administrator, der seine Handlungen nicht unter Sicherheitsgesichtspunkten reflektiert, ist auf Dauer Teil des damit entstehenden Sicherheitsproblems. In vielen Fällen ist nicht ein grosses Projekt, wie z. B. ein «Sicherheitsaudit» eine sinnvolle Lösung, sondern eine begrenzte Bestandsaufnahme und die Abarbeitung der offensichtlichen Schwachstellen ein riesiger Schritt in die richtige Richtung.

Neben der strafrechtlichen Relevanz muss man hier auch zivilrechtliche Ansprüche berücksichtigen, zum Beispiel durch Vernachlässigung der Sorgfaltspflicht der Administratoren oder des Managements. Neuere Richtlinien zur Unternehmensführung nehmen hier das Management immer mehr in die Pflicht - und ein Administrator kann in den meisten Fällen weder das Risiko tragen noch die Verantwortung übernehmen. Hier ist ein intensiver Austausch zwischen Technikern und Management notwendig, in dem zunächst eine gemeinsame Sprache und Sichtweise auf die Probleme gefunden werden muss.

Grundsätzlich kann aber das Internet niemals sicherer als das «Echte Leben» sein. Und die neuen Möglichkeiten, Geschäfte zu betreiben, wiegen die Risiken in vielen Fällen auf. Und letzten Endes fallen viele dieser Risiken unter das «Unternehmerische Risiko», das unmittelbar mit dem Geschäft verbunden ist. Daher ist Panik und Aktionismus dem Thema nicht angemessen.


## Jochen Kellner

Jochen Kellner ist Senior-Architekt bei der SerCon Service & Consulting, einer Tochtergesellschaft der IBM Business Consulting Services. Neben der Installation und Betreuung von SAP R/3 Systemen sind seine Schwerpunkte Unix und IT-Security.