

NWSI

Autor: Michael Raith

Inhaltliches Lektorat: Roland Fischer

7. überarbeitete Ausgabe, 2009

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder einem anderen Verfahren) ohne schriftliche Genehmigung des Herausgebers reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Dieses Buch wurde mit großer Sorgfalt erstellt und geprüft. Trotzdem können Fehler nicht vollkommen ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Sollte es uns trotz intensiver Recherchen nicht gelingen sein, alle Rechteinhaber der verwendeten Quellen und Abbildungen zu finden, bitten wir um kurze Nachricht an die Redaktion.

Die in diesem Buch und in den abgebildeten bzw. zum Download angebotenen Dateien genannten Personen und Organisationen, Adress- und Telekommunikationsangaben, Bankverbindungen etc. sind frei erfunden. Übereinstimmungen oder Ähnlichkeiten mit lebenden oder toten Personen sowie tatsächlich existierenden Organisationen oder Informationen sind unbeabsichtigt und rein zufällig.

Die Bildungsmedien des HERDT-Verlags enthalten Links bzw. Verweise auf Internetseiten anderer Anbieter. Auf Inhalt und Gestaltung dieser Angebote hat der HERDT-Verlag keinerlei Einfluss. Hierfür sind alleine die jeweiligen Anbieter verantwortlich.

## Netzwerke

Sicherheit

NWSI

|  |           |  |            |
|--|-----------|--|------------|
| <b>1 Informationen zu diesem Buch .....</b>      | <b>4</b>  | <b>9 Standalone-Virenschutz.....</b>           | <b>70</b>  |
| 1.1 Voraussetzungen und Ziele .....              | 4         | 9.1 Einfache Virenprävention .....             | 70         |
| 1.2 Aufbau und Konventionen .....                | 5         | 9.2 Gängige Antivirussoftware.....             | 77         |
| <b>2 Was ist Sicherheit?.....</b>                | <b>6</b>  | 9.3 Computer scannen .....                     | 79         |
| 2.1 Vertraulichkeit.....                         | 6         | 9.4 Viren entfernen.....                       | 81         |
| 2.2 Integrität .....                             | 6         | <b>10 Unternehmensweiter Virenschutz .....</b> | <b>84</b>  |
| 2.3 Verfügbarkeit .....                          | 7         | 10.1 Client/Server-Konzept von Norton          |            |
| <b>3 Risikolage für Unternehmen .....</b>        | <b>8</b>  | Antivirus .....                                | 84         |
| 3.1 Warum ist das Internet nicht "sicher"? ..... | 8         | 10.2 Installation.....                         | 85         |
| 3.2 Schadensmöglichkeiten .....                  | 9         | 10.3 Konfiguration.....                        | 89         |
| 3.3 Überlebenschancen .....                      | 10        | 10.4 Überwachen eines Firmennetzwerkes .....   | 91         |
| <b>4 Angriffsvorbereitung .....</b>              | <b>12</b> | <b>11 IT-Sicherheitsstandards.....</b>         | <b>92</b>  |
| 4.1 Hacker, Cracker und Script-Kids.....         | 12        | 11.1 Standards im Bereich                      |            |
| 4.2 Netzwerkscans.....                           | 13        | Informationssicherheit.....                    | 92         |
| 4.3 Wardialing.....                              | 17        | 11.2 IT-Grundschutzhandbuch.....               | 95         |
| 4.4 Wardriving.....                              | 18        | 11.3 Security Policy.....                      | 95         |
| 4.5 Social Engineering.....                      | 19        | <b>12 Symmetrische Kryptografie .....</b>      | <b>98</b>  |
| <b>5 Angriffe auf Server.....</b>                | <b>22</b> | 12.1 Das Problem von Alice und Bob .....       | 98         |
| 5.1 Exploits .....                               | 22        | 12.2 Einfache Verschlüsselungsmethoden .....   | 100        |
| 5.2 Rootkits.....                                | 28        | 12.3 Symmetrische Verfahren.....               | 106        |
| 5.3 DoS/DDoS.....                                | 29        | <b>13 Asymmetrische Kryptografie .....</b>     | <b>114</b> |
| 5.4 Sniffer .....                                | 30        | 13.1 Nachteile von symmetrischen Verfahren ... | 114        |
| 5.5 Replay-Attacken .....                        | 31        | 13.2 Einwegfunktion .....                      | 115        |
| 5.6 Hijacking .....                              | 31        | 13.3 Diffie-Hellman-Schlüsseltausch.....       | 119        |
| <b>6 Sicherheitsprobleme durch</b>               |           | 13.4 El-Gamal .....                            | 120        |
| <b>Mitarbeiter .....</b>                         | <b>34</b> | 13.5 RSA.....                                  | 120        |
| 6.1 Ausfall/Krankheit .....                      | 34        | 13.6 Digitale Signatur .....                   | 122        |
| 6.2 Hintertürchen .....                          | 35        | 13.7 Hashfunktionen .....                      | 123        |
| 6.3 Spionage.....                                | 35        | 13.8 Schwachstellen in RSA .....               | 124        |
| 6.4 Mangelnde Kompetenz .....                    | 36        | 13.9 Public Key Infrastructure .....           | 126        |
| <b>7 Virenarten und ihre Verbreitung .....</b>   | <b>38</b> | <b>14 Kryptografische Protokolle und ihre</b>  |            |
| 7.1 Grundkonzepte von Viren .....                | 38        | <b>Anwendung.....</b>                          | <b>128</b> |
| 7.2 Virenarten.....                              | 39        | 14.1 SSL/TLS .....                             | 128        |
| 7.3 Tarnmechanismen von Viren .....              | 46        | 14.2 SSH .....                                 | 130        |
| 7.4 Würmer.....                                  | 51        | 14.3 IPSec .....                               | 130        |
| 7.5 Trojanische Pferde.....                      | 52        | 14.4 SET/HBCI .....                            | 131        |
| 7.6 Hoaxes .....                                 | 53        | <b>15 Sichere E-Mail mit GnuPG.....</b>        | <b>134</b> |
| 7.7 Tendenzen und Ausblick.....                  | 54        | 15.1 Installation.....                         | 134        |
| <b>8 Spyware, Phishing und Browser</b>           |           | 15.2 Schlüssel generieren.....                 | 135        |
| <b>Hijacking .....</b>                           | <b>56</b> | 15.3 Schlüsselexport und -import.....          | 137        |
| 8.1 Geld verdienen im Internet.....              | 56        | 15.4 Signieren von Schlüsseln.....             | 139        |
| 8.2 Spyware .....                                | 57        | 15.5 Revocation Certificates .....             | 141        |
| 8.3 Browser Hijacking.....                       | 60        | 15.6 E-Mail signieren und verschlüsseln.....   | 143        |
| 8.4 Was ist Phishing?.....                       | 62        |  |            |
| 8.5 Anti-Spyware einsetzen .....                 | 64        |  |            |

|   |            |  |            |
|---|------------|--|------------|
| <b>16 Firewalls .....</b>                                     | <b>146</b> | 19.3 WEP .....   | 176        |
| 16.1 Wie Firewalls arbeiten .....                             | 146        | 19.4 WPA, WPA2 und 802.11i .....                       | 177        |
| 16.2 Paketfilter-Firewall .....                               | 148        | 19.5 Funkausleuchtung .....                            | 178        |
| 16.3 Stateful Inspection .....                                | 149        |  |            |
| 16.4 Proxy Level/Application Level .....                      | 150        | <b>20 Alternative Software .....</b>                   | <b>180</b> |
| 16.5 NAT-Firewall .....                                       | 151        | 20.1 Warum andere Software sinnvoll sein<br>kann ..... | 180        |
| 16.6 Personal Firewall .....                                  | 152        | 20.2 Alternative Webbrowser .....                      | 181        |
|   |            | 20.3 Alternative E-Mail-Clients .....                  | 182        |
| <b>17 Intrusion-Detection-Systeme .....</b>                   | <b>156</b> |  |            |
| 17.1 Notwendigkeit von Intrusion-Detection-<br>Systemen ..... | 156        | <b>21 Zugangskontrollsysteme .....</b>                 | <b>184</b> |
| 17.2 Arbeitsweise eines IDS .....                             | 157        | 21.1 NT-LM und Kerberos .....                          | 184        |
| 17.3 Intrusion-Reaction-System .....                          | 158        | 21.2 PAP, CHAP, EAP und RADIUS .....                   | 188        |
| 17.4 Snort .....  | 159        | 21.3 Smartcards und Tokensysteme .....                 | 188        |
| 17.5 Honeypot-Netzwerke .....                                 | 163        | 21.4 Biometrie .....                                   | 189        |
|   |            |  |            |
| <b>18 Virtual Private Network .....</b>                       | <b>166</b> | <b>22 Proaktive Sicherheit .....</b>                   | <b>192</b> |
| 18.1 Zielsetzung .....  | 166        | 22.1 Defensive Programmierung .....                    | 192        |
| 18.2 PPTP .....   | 167        | 22.2 Gehärtete Betriebssysteme .....                   | 193        |
| 18.3 L2TP/IPSEC .....   | 168        | 22.3 Patches .....                                     | 193        |
|   |            | 22.4 Vulnerability Assessment .....                    | 194        |
| <b>19 WLAN und Sicherheit .....</b>                           | <b>172</b> |  |            |
| 19.1 WLAN-Arbeitsweise .....                                  | 172        | <b>Stichwortverzeichnis .....</b>                      | <b>198</b> |
| 19.2 Access-Points .....                                      | 175        |  |            |

## 3 Risikolage für Unternehmen

### In diesem Kapitel erfahren Sie

- ▶ warum das Internet entwickelt wurde
- ▶ warum das Internet nicht "sicher" ist
- ▶ welchen Risiken sich ein vernetztes Unternehmen aussetzt

### 3.1 Warum ist das Internet nicht "sicher"?

#### Die Entstehung des Internets

Um verstehen zu können, warum das Internet heute gewisse Eigenschaften im positiven sowie im negativen Sinne aufweist, ist es nützlich, zu wissen, unter welchen Umständen das Netzwerk und die dazugehörigen Protokolle entwickelt wurden.

In den 60er-Jahren, auf dem Höhepunkt des kalten Krieges, standen sich die Supermächte USA und die Sowjetunion mit einem riesigen Arsenal an Atomwaffen gegenüber. In den Planungsstäben waren die Befürchtungen groß, dass man einen sowjetischen Erstschatz nicht überstehen würde - im zivilen sowie im militärischen Bereich.

Die Computersysteme der damaligen Zeit waren, wenn sie vernetzt waren, grundsätzlich zentral gesteuert. Ein Angriff auf einen derartigen zentralen Knotenpunkt würde also zwangsläufig das gesamte daran angeschlossene Netz außer Betrieb setzen. Paul Baran, der für die Rand Corporation arbeitete, wurde mit der Konzeption eines Netzwerkes beauftragt, das selbst einen Atomangriff überstehen würde.

Barans revolutionäres Konzept sah ein Netzwerk vor, bei dem prinzipiell jeder Rechner mit jedem anderen kommunizieren konnte - ein vollständig dezentrales Netz. In Barans Konzept sollten sich die Datenpakete "selbstständig" einen Weg von der Quelle zum Ziel suchen und, wenn notwendig, einen anderen Weg einschlagen, falls ein bestimmter Netzknoten ausgefallen war.

Sein elfbändiger Bericht, den er im Jahre 1962 einreichte, wurde aber vom Pentagon vorerst ignoriert, weil man dieses Netzwerk für nicht realisierbar hielt. Jedoch wurde kurz darauf eine Projektgruppe erneut mit der Entwicklung eines derartigen Netzes beauftragt: die Advanced Research Project Agency. Diese nahm gegen Ende der 60er-Jahre das nach ihr benannte ARPANET in Betrieb.

In den 70er-Jahren wurde das derzeit am häufigsten eingesetzte Übertragungsprotokoll TCP entwickelt. TCP war dafür konzipiert, Datenströme in Pakete aufzuteilen und diese über das Netzwerk zu versenden. Auf der Empfängerseite konnte TCP die Datenpakete wieder korrekt zu einem Datenstrom zusammensetzen. Auch E-Mail und andere Dienste wurden nach und nach entwickelt. Bis Ende der 80er-Jahre war das ARPANET (später dann schon Internet genannt) fest in der Hand der amerikanischen Regierung und vernetzte Militär- und Forschungseinrichtungen. Anfang der 90er-Jahre begann die amerikanische Regierung allerdings, sich aus dem Internet zurückzuziehen und es für kommerzielle Firmen zu öffnen.

#### Der Internet-Boom

Der eigentliche Boom des Internets begann schließlich mit der Entwicklung des HTTP-Protokolls und der ersten Internet-Browser, die es auch technisch nicht versierten Benutzern erlaubten, über eine grafische Bedienoberfläche vernetzte Inhalte abzurufen.

Heutzutage ist das Internet eine Plattform für jedermann, in der viele Informationen und Dienstleistungen angeboten werden. Für die Frage nach der Sicherheit des Internets sind folgende Fakten wichtig:

Die Internet-Protokolle wurden im Hinblick darauf entwickelt, eine Datenübertragung auch nach einem Ausfall eines oder mehrerer Netzknoten zu gewährleisten. Die automatische Wegfindung im Netzwerk (auch Routing genannt) war hier das Hauptziel.

Übertragungsprotokolle wie TCP wurden dafür entwickelt, Datenströme versenden zu können. TCP sollte sicherstellen, dass einzelne Pakete auf der Empfängerseite wieder zum ursprünglichen Datenstrom zusammengesetzt würden, und dabei die richtige Reihenfolge berücksichtigen sowie eine automatische Neuübertragung bei fehlenden oder falsch übertragenen Paketen garantieren.

### **Vernetzung: jeder mit jedem**

Da die Entwickler nicht absehen konnten, dass dieses Netzwerk später nicht nur die Rechenanlagen des amerikanischen Militärs, sondern fast alle Computer auf dem Erdball vernetzen würde, wurde auch kein Mechanismus eingebaut, der die Korrektheit der Angaben in den Protokollen sicherstellt. Es ist also möglich, Datenpakete mit gefälschten Daten oder gezielt manipulierte Pakete in das Netz zu senden - mit unzähligen nicht berücksichtigten Seiteneffekten, die sich durchaus auch für betrügerische Zwecke ausnutzen lassen.

Dadurch, dass die am Internet teilnehmende Personenzahl schier unüberschaubar ist und die Internet-Protokolle mit dem Ziel entwickelt wurden, dass jeder Rechner mit jedem kommunizieren konnte, ist ein an das Internet angeschlossener Computer buchstäblich an "den Rest der Welt" angeschlossen - dazu gehören auch Kriminelle.

## **3.2 Schadensmöglichkeiten**

### **Was passieren kann**

Wenn ein oder mehrere Rechner eines Unternehmens an das Internet angeschlossen sind, gibt es zahlreiche Möglichkeiten, wie der Einsatz der IT vom Sollzustand abweichen kann. Aus dem Internet kann bösartige Software wie Viren in das Unternehmensnetzwerk gelangen und dort Datenverluste sowie Ausfallzeiten verursachen. Spam und E-Mail-Virenwellen können E-Mail-Server überlasten und Netzwerk-Bandbreiten belegen.

Vertrauliche und geheime Informationen könnten unkontrolliert das Unternehmen verlassen, wenn Cracker in die Netzwerke eindringen, um Informationen auszuspähen und zu stehlen, oder wenn Mitarbeiter unvorsichtig Dokumente versenden. Erlangen unautorisierte Personen Schreibzugriff auf Dateien und Systeme, können Daten manipuliert und Netzwerke neu konfiguriert werden.

Der entstandene Schaden lässt sich meist nur schwer beziffern. Bei einem Serverausfall oder einem Datenverlust ist es relativ leicht, die zur Behebung des Schadens angefallenen Arbeitsstunden aufzuaddieren und zusammen mit dem Ausfall an produktiver Arbeitszeit eine Zahl zu nennen, aber Imageschäden lassen sich nur äußerst schwer beziffern.

Eine Online-Bank, deren Webseite von einem Cracker verändert wurde, oder eine Firma, deren Kundendaten inklusive Kreditkartendaten veröffentlicht werden, dürften wohl das Vertrauen ihrer Kunden verloren haben. Ebenso ist dem Aussickern von Informationen schwer ein genau bestimmbarer finanzieller Schaden zuzuschreiben. Gelangt der Schriftverkehr einer Firma mit ihrem Versicherungsunternehmen in unbefugte Hände, ist zwar klar, dass dies eine unerwünschte Situation ist -, die Forderung nach Vertraulichkeit wurde verletzt - der finanzielle Schaden ist dennoch nicht genau errechenbar.

### **Folgen einer Datenpanne**

Problematisch bei Datenunfällen ist die Wiederherstellung des Betriebszustandes deswegen, weil verlorene Daten rekonstruiert werden müssen und die inzwischen angefallene Arbeit auch erledigt werden muss. Untersuchungen zeigen, dass die benötigte Zeit zur Rückkehr in den Normalzustand nach einer geplanten Betriebsunterbrechung ohne weiteres die Ausfallzeit circa um den Faktor fünf übersteigt. Nach einem ungeplanten Zwischenfall oder einer Computerkatastrophe beträgt dieser Faktor leicht das 10-Fache.

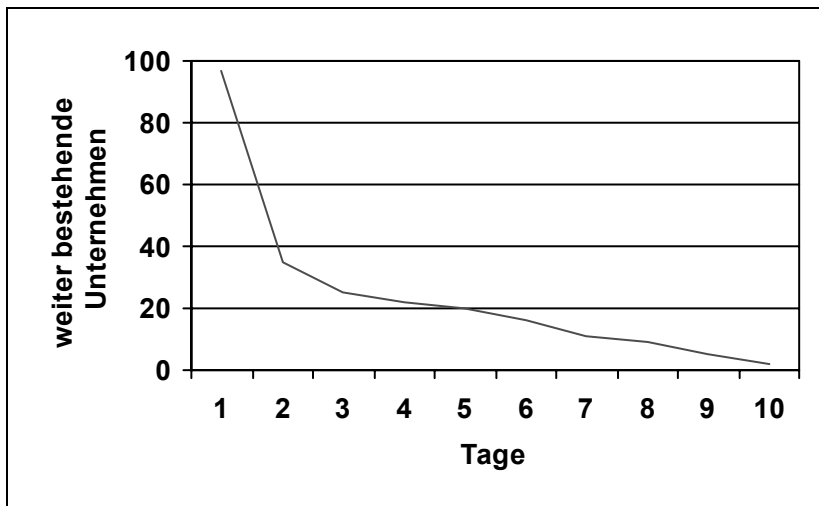
Dies kann in eine Art Teufelskreis führen, wenn man annehmen darf, dass die verlorene Zeit meist mithilfe von Mehrarbeit und Überstunden hereingeholt werden muss. Die Wahrscheinlichkeit, dass in dieser Zeit neue Fehler begangen werden, die andere Sicherheitslücken öffnen und neue Ausfälle verursachen können, steigt somit sehr wahrscheinlich.

### 3.3 Überlebenschancen

#### Wie abhängig sind Firmen vom IT-Einsatz?

Eine Untersuchung der Universität von Minnesota schätzte die durchschnittlichen Zeiten für das Weiterbestehen von Unternehmen nach einer Katastrophe im Rechenzentrum auf folgende Werte:

- ✓ Banken                    2 Tage
- ✓ Handelsunternehmen    3 Tage
- ✓ Industrie                5 Tage
- ✓ Versicherungen        6 Tage



Umfrage: *Wie viele Tage könnten Sie den Ausfall Ihrer IT überleben?*

Weiterhin zeigte eine Studie über amerikanische Unternehmen, die von einer Katastrophe betroffen waren, dass 25 % kurz nach der Katastrophe und 40 % innerhalb von zwei Jahren Konkurs anmelden mussten. Nach 5 Jahren waren weniger als 7 % der betroffenen Firmen noch auf dem Markt tätig.

Diese Studie definierte eine Computerkatastrophe als Totalausfall der EDV in einem Unternehmen. Extremfälle dieser Art sind erfreulicherweise relativ selten. Dennoch zeigen diese Zahlen, dass bei Problemen im EDV-Bereich die Achillesferse einer Firma getroffen wird - zu viele Daten von der einfachen E-Mail bis zur Auftragsverarbeitung und Produktionsplanung und Steuerung laufen über Computersysteme.

Um eine Computerkatastrophe zu verhindern, aber auch um kleinere Ausfälle zu vermeiden, sollte sich nicht nur die IT-Abteilung eines Unternehmens Gedanken machen, sondern auch das Management. Es gilt, schützenswerte Elemente der Firma zu identifizieren, deren Risiko zu analysieren und gegen denkbare Bedrohungen geeignete Maßnahmen zu ergreifen und deren Wirksamkeit zu prüfen.

