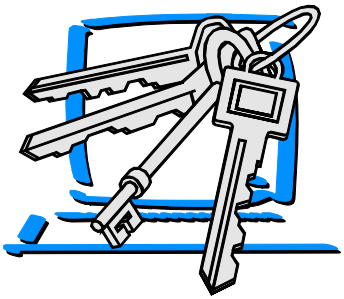


2.3

Computer - Sicherheit gestern, heute und morgen

Was Sie wissen sollten

und

wie Sie sich schützen können

Erlenaustraße 27
83022 Rosenheim
Tel. 08031 / 66005
Fax 08031 / 65375

RÜNAGEL computer-systeming

www.Ruenagel.de H@Ruenagel.de

Kurzbeschreibung

Gestern, heute und morgen ...

In keinem Bereich ändern sich die Umstände so schnell wie in der EDV. Die Geschwindigkeit erhöht sich ständig, so dass sich eine EDV-Anlage zu einem hoch-dynamischen System entwickelt hat.
Laufende Aktualisierung der Hard- und Software ist notwendig geworden. Damit verbundene Risiken müssen beachtet und konsequent gelöst werden.

Gestern
lag die Bedrohung bei einigen zerstörenden Viren. Datensicherung und ein klassischer Virenscanner war ausreichend.

Heute
gibt es raffinierte Methoden, um volle Kontrolle, perfekte Spionage und Manipulation auf PC´s und Netzwerken auszuüben. Komplexe Schutzmechanismen sind notwendig, um die Vorteile der modernen Kommunikation gefahrlos zu nutzen.

Morgen
gibt es mit Sicherheit viele neue Varianten der Angriffstechniken.
Bereits heute ist der Schutz dagegen wichtig.

... mit Sicherheit

Die Verfügbarkeit und Sicherheit der EDV kann durch moderne und wirkungsvolle Sicherheitsmassnahmen gewährleistet werden.

Von den grundlegenden Hard- u. Softwareeigenschaften

wie Notstromversorgung, Festplattenspiegelung, Betriebssysteme

über Datensicherung, physikalischer Entkopplung des Netzwerkes, Firewall

bis hin zur Immunisierung der Arbeitsplätze gegen Viren und Trojaner

sind alle Möglichkeiten zum Schutz des Netzwerkes und der Arbeitsplätze auch für die Zukunft berücksichtigt.

Die inzwischen als selbstverständlich zu bezeichnenden Massnahmen sind hier nicht weiter beschrieben.

Lediglich die durch die Kommunikation per Email und Internet zusätzlich notwendig gewordenen Abwehrtechniken und -massnahmen sollen hier genauer erläutert werden.

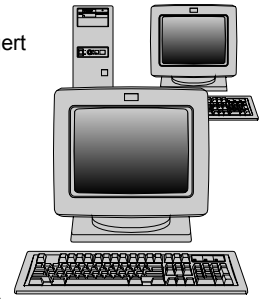
Überblick Beispiel

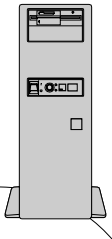
CSR-Sicherungs-Server

Daten werden laufend aktualisiert zB15Min., und stehen absolut sicher aktuell zur Verfügung.

Server

Festplattenspiegelung, Sicherung u. Archivierung mit DAT-Band-Laufwerk, Bänder mit komplett-Sicherung sollen regelmässig ausgelagert werden.

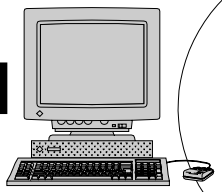




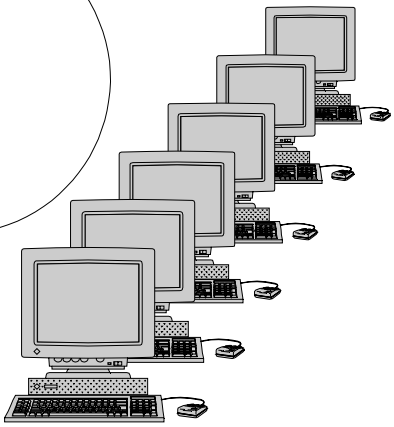
Internet-Gateway

physikalische Entkopplung, Firewall, Portfilter, Proxy, Viren- und Angriff-Überwachung... Selbständige Regenerierung und Reinigung.

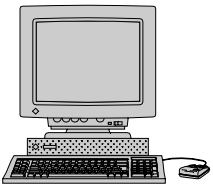
Internet



LAN



ISDN



Gesonderter Internetzugang evtl. RAS u. DATA

Passwort nach Zeit wechseln, wenn möglich Rückruf einrichten, Zugriffsrechte auf Server möglichst einschränken.

Arbeitsplätze

Absicherung durch CSR-Si - unzerstörbar, auch neue Viren und Trojaner werden entfernt,
Virenscanner, wo Disketten oder anderer Datenaustausch stattfindet

Chef-Info nach Analyse Beispiel

- EDV-Sicherheitsbeauftragter u. Stellvertreter definieren, nur diesen neue Passwörter mitteilen.

- Server-Datenstruktur / Rechte überprüfen, genau definieren

- Server soll anderes Passwort bekommen, als Administrator auf WS

- Jeder Benutzer muss ein Passwort bekommen

- Alle Daten müssen auf dem Server abgelegt werden (Sicherung)

- Zugang zu DAT-Bändern nicht ermöglichen, Bänder mit Komplettsicherung regelmässig auslagern, Sicherungspasswort vergeben / ändern

- FIBU-PC (homebanking) - anderes Protokoll, kein Internet u. Email

- auf Clients alle Script-Interpreter entfernen bzw. ausschalten

- möglichst wenig Microsoft-Produkte einsetzen, da die meisten Viren

- Emails sollen laufend abgeholt werden (kurze Verweildauer beim Provider)

(- Externen Zugang (RAS) anderes Protokoll, regelmässig PW ändern und Rückruf einrichten)

...

Nötige Arbeiten, Neuanschaffungen:

- Browser-, Programm-, Scripteinstellungen wegen Sicherheit prüfen bzw. einstellen

- getrennte Netzwerkprotokolle für FIBU, RAS u. Server verwenden

- Kommunikationsserver mit Firewall, Portfilter, Proxy ... einrichten

- CSR-Sicherungs-Server installieren

- Virenscanner auf PC´s mit intensivem Datenaustausch (Disketten) bzw. Administrator-PC zur Prüfung der Server-Festplatten

...

Gefahr ?

Ist Schutz wirklich notwendig und woher droht die meiste Gefahr ?

Bevor die PC´s mit den sehr offenen Kommunikationsleitungen verbunden wurden, lag die Gefahr anders gelagert. Die Verbreitung von Viren dauerte sehr viel länger, da sie auf die beschreibbaren Datenträger angewiesen waren. Spionage auf diesem Weg war nicht möglich und deshalb handelte es sich um reine Zerstörer-Viren.
Trotz der relativ langen Zeit die für die Herstellung von Gegenmassnahmen (Virenscanner) zu Verfügung stand, verbreiteten sich schon damals manche Viren sehr weit. Was uns zu denken geben sollte, ist die Tatsache, dass viele dieser Viren immer wieder auftauchen und aktiv werden.

Nachdem jetzt Leitungen mit hohem Durchsatz praktisch weltweit verbunden sind, kann jeder Mensch über seinen PC jeden anderen erreichen.
Diese Möglichkeit eröffnet natürlich auch für die negative Nutzung grenzenlose Möglichkeiten.

Was kann auf meinem PC oder Netzwerk geschehen ?

- Viren
  Programme - Zerstörung von Programmen und Daten
- Trojaner und Hintertüren
  Programme - unberechtigter Zugang zu Ihrem Rechner (Netzwerk) mit allen Möglichkeiten
- Cracker, Hacker
  Personen - unerlaubtes Eindringen in PC´s und Netzwerke über Kommunikationsleitungen

Diese Begriffe sind inzwischen bekannt und kommen natürlich in jeder denk- oder undenkbaren Form vor. So kann z.B. ein Cracker über einen Trojaner Ihren gesamten Rechner fernsteuern, die Tastatur abfragen usw. Welche Gefahr das bedeutet dürfte klar sein.
Von willkürlicher Zerstörung bis zur perfekten Spionage ist alles möglich.
Beispielsweise kann ein Cracker ein Passwort herausfinden, auch wenn es noch so genial verschlüsselt ist. Und was das für Ihr Bankkonto bedeuten kann...?

Virenangriffe können weitaus grösseren betriebswirtschaftlichen Schaden anrichten, als allgemein angenommen wird.

So reichen die Kosten, die alleine der bekannte Loveletter verursachte weit über die bisher geschätzten zwei Milliarden Mark hinaus. Bei Attacken dieser Art dürfen nicht einfach die Arbeitsstunden zur Beseitigung des Virus addiert werden. Vielmehr müssen auch die Vermögensschäden berücksichtigt werden, die den Kunden der Betroffenen durch die Verzögerung entstehen.
Diese Schäden können nicht versichert werden und selbst wenn der Urheber ausfindig gemacht werden kann, ist Schadenersatz nicht zu erwarten.

Viren wie der Loveletter sind eher in den Bereich Scherz bis harmlos einzuordnen. Dieser Virus (Wurm) zerstörte nur unwichtigere Dateien und überlastete so manchen Email-Server kurzzeitig.
Ein Virus, der gezielt auf Zerstörung programmiert ist, erreicht ein Vielfaches des angerichteten Schadens. Man stelle sich vor, eine Verteilungstechnik wie die des Loveletters mit zeitversetzten Sende-Aktivitäten, Muttation nach Aufruf und in Wartezustand bis zu einem Datum in ca. 6 Monaten. Bei Eintreffen des Datums, gezielte (auch anfangs unmerkliche, langsame) Zerstörung der Daten, danach Zerstörung der Programme und des Bootbereiches.
Dieser Virus würde die Daten und Installationen von garantiert 50% der PC´s und Netzwerke weltweit auf einen Schlag zerstören. Alleine die Ausfallzeit und der Wiederherstellungsaufwand würde ungeahnten Schaden bedeuten. Die Datenwiederherstellung könnte durch eine langsame Zersetzung sogar unmöglich werden. Dies würde in sehr vielen Fällen den Ruin eines Unternehmens bedeuten, da inzwischen fast völlige Abhängigkeit von der EDV besteht.

Die Verbreitung von solchen Programmen war bisher fast ausschließlich durch Leichtsinn der Anwender möglich.
Beispielsweise hat auch die rasend schnelle Verbreitung des Computer-Virus Melissa im März 1999 gezeigt, dass Word-Dateien immer noch arglos geöffnet werden, selbst wenn sie unverhofft als Email-Anhang eintrudeln.

Die Krönung der Anwenderverhaltens dürfte ein harmloses Email (Juli 2000) sein, in dem der Autor beschreibt, dass er nicht fähig sei, einen Virus zu programmieren und bittet deshalb um Mithilfe der Empfänger. Diese sollen das Mail an 50 weitere Personen versenden, Dateien in ihrem System-Verzeichnis

löschen und an bestimmten Tagen die Festplatte formatieren.
Unglaublich aber wahr, dieser Scherz hat erheblichen Schaden angerichtet, weil sich viele Benutzer zumindest an die erste Aufforderung hielten.

2002 erhielten die neu erkannten Exemplare bereits eine Qualität, die erahnen lässt, was auf uns zukommt. Die autom. Verbreitung über sämtliche Verbindungsmöglichkeiten, Mutationen, Ausserbetriebsetzung von Firewalls und Virenscannern, Öffnen von IP-Ports, Auslesen von Passwörtern, Pins und anderen geheimen Informationen und unerkannte Übermittlung per Internet.

Täglich werden neue, ausgefeiltere Viren (Tendenz weiter steigend) hergestellt und in Umlauf gebracht. Weil die klassischen Methoden diese Muster natürlich nicht erkennen können, stellen die unbekannten Varianten nach wie vor ein mit bisherigen Methoden ungelöstes Problem dar.

Schadensumfang bei Zerstörung eines ungesicherten Arbeitsplatzes
ohne Datenverlust und ohne Folgeschäden durch Zeitverzögerung:
Ausfallzeit von Mitarbeitern
Feststellung der Ursache - Schutz bzw. Warnung anderer Mitarbeiter
Wiederherstellung Betriebssystem und Anwendersoftware
Rekonstruktion anwenderspezifische Einstellungen
mind. 1500,-- Eur

Folge- und Spionageschäden sind nicht zu beziffern. Spionage wird meistens nicht entdeckt ! Die eingeschleusten Programme produzieren keine für den Anwender sichtbarn Effekte und werden deshalb auch den Virenschutz-programmierern nicht gemeldet.
Entwicklungen, Vorhaben und Daten (Passwörter, Geheimnummern, Kundenstamm) jeder Art werden ausspioniert. Der Verwendungszweck ist unterschiedlich.
Vom Mitbewerber bis zu Einrichtungen, die die Weltherrschaft zum Ziel haben, gibt es genügend Interessenten.
Auch wer glaubt, er könne ruhig ausspioniert werden hat mit weiteren Gefahren und u.U. erheblichen Kosten zu rechnen. "Wer denkt an sowas ?"
Der PC ruft selbstständig teure 0190er Nummer an, oder Andere benutzen den Account zum Provider ...
Die hier angesprochenen Bedrohungen betreffen nur die lokalen Installationen (LAN). Internet- und externe Email-Server werden durch andere Methoden attakiert. Die Gegenmassnahmen sind hier nicht relevant und negative Auswirkungen können durch die Wahl des richtigen Providers praktisch vermieden werden.

Schutz ?

Ist es möglich, sich vor diesen vielfältigen Angriffsmöglichkeiten zu schützen ?

Es sind verschiedenen Schutzmechanismen erforderlich.
Neben den zu beachtenden Strukturen und Softwareeinstellungen sind einige Massnahmen unabdingbar, spätestens seit 1999 verfügbar und erfolgreich im Einsatz.

- Virenscanner
  erkennen zigtausend bekannte Muster und können die meisten entfernen. Sollte auf allen PC´s vorhanden sein, die direkt per Diskette oder Dfü ... kommunizieren.
- Firewall
  verhindert erkannte, nichtautorisierte Zugriffe über die Kommunikationsleitungen.
- Rechte / Protokolle / physikalische Trennung / Adressumsetzung ...
  die üblichen Sicherheitsmassnahmen erschweren es Hackern erheblich, in ein System einzudringen bzw. Schaden anzurichten.
- CSR-Sicherheits-System
  entfernt jede Art von Viren und Trojaner aus Betriebssystem und Programmen - auch unbekannte und tagesaktuelle, die von Virenscannern nicht erkannt werden.
- CSR-Wiederherstellungs-System
  stellt autom. den Urzustand der System- und Programminstallation her und verhindert die Zerstörung.
- CSR-Sicherungs-System
  autom. Sicherungssystem, das im Notfall eine sofortige Wiederherstellung von möglichst aktuellen (15Min.)Daten erlaubt. Der Zugriff von Cracker, Viren und Anwendern auf diese Sicherungs-Daten ist unmöglich.

- Sicherung der lokalen Installation
  bootfähige CD oder HD, die im Notfall zB.
  bei Hardware-Ausfall (Festplattendefekt)
  die sehr schnelle Wiederherstellung gewährleistet.

Die Kombination der klassischen und neuen Methoden ergänzen sich zu einem "dichten" System, das auch in Zukunft evtl. auftretende Schäden auf ein Minimum beschränkt.

Ein Firewall alleine ist kein ausreichender Schutz, da ein Trojaner die Identität des Anwenders nutzten kann, um so scheinbar legitime Verbindungen aufzubauen. Der Firewall kann dies nicht erkennen und verhindern, ist aber ein wichtiger Bestandteil, um Standardangriffe abzublocken.

Viren und Trojaner (auch unbekannte) können in diesem System nur temporär aktiv werden. Sie werden autom. entfernt, auch wenn sie der Virenscanner nicht erkennt.
Somit werden auch Cracker, die evtl. durch einen Trojaner ein System ausspionieren oder steuern wollen, daran gehindert.

Evtl. Schäden an den lokalen System- und Programminstallationen werden autom. erkannt und repariert. Sie sind somit, einmal richtig eingerichtet und angewendet, softwaretechnisch unzerstörbar.

Der letzte Stand der Daten kann bei evtl.(auch versehentlich) Zerstörung in kürzester Zeit wieder hergestellt werden.

Bei Befall von Dateien durch unbekannte Macroviren (Excel / Word) wird vom CSR-System Erste Hilfe geleistet und durch einen Virenscanner bei Bekanntwerden des Virus die Entfernung aus den Daten vorgenommen.

Somit sind alle Möglichkeiten berücksichtigt, um Angriffe zu verhindern bzw. vereiteln und eine Zerstörung nicht zuzulassen.

Anwender benötigen dafür kein Spezialwissen. Verantwortungsbewusstes Verhalten ist jedoch Voraussetzung.

Mehrjährige Untersuchungen von unabhängigen Einrichtungen ergaben immer wieder die gleiche Reihenfolge für die Gefahren Im Unternehmen, die wir bestätigen:

1. Nachlässigkeit der Mitarbeiter
2. Viren und Trojaner (Tendenz stark steigend / 88% der Unternehmen)
3. Softwaremängel
4. externe Fehler, bekannt gewordene Spionage, Sabotage ...

Was kann ich tun ?

Das Benutzerverhalten ist eine wichtige Grundlage, um die Funktionsfähigkeit und den Datenbestand zu erhalten.
Jeder Mitarbeiter trägt hier eine grosse Verantwortung.

- Alle Daten auf dem File-Server speichern,
- möglichst keine .DOC oder .XLS-Dateien von Geschäftspartnern annehmen, statt .DOC .RTF-Dateien anfordern,
- niemals "Objekte", die mit Dateien verknüpft sein können anklicken (auch hier sind in erster Linie MS-Office-Dateien betroffen),
- Word-Dateien immer "öffnen ohne Macro",
- niemals Dateien öffnen bzw. ausführen, deren Herkunft oder Zweck Sie nicht kennen,
- grundsätzlich aus dem Internet nichts auf einen Arbeits-PC laden,
- keine Demonstrations- bzw. Test-Software auf Ihren PC installieren,
- auf keinen Fall fremde Bildschirmschoner verwenden,
- Disketten CD´s und DVD´s nur auf einem virengeschützten PC verwenden,
- Bei auftretenden Phänomenen und Verdacht auf Manipulation, sofort EDV-Verantwortlichen bzw. Sicherheitsbeauftragten mit möglichst genauen Angaben benachrichtigen.

- Passwörter geheimhalten,
- Passwort auf dem (Standard-) Bildschirmschoner verwenden,
- Virenscanner laufend aktualisieren,
- als Administrator nie längere Zeit angemeldet bleiben und möglichst keine Anwenderprogramme ausführen,
- niemals als Administrator im Internet serven oder Dateien öffnen,
- niemals auf einem Server Anwenderprogramme ausführen,
- Stillschweigen bzgl. Massnahmen, Passwörter und Mitarbeiter- u. EDV-Struktur usw. gegenüber Nichtbetriebsangehörigen (Spione sind freundlich !),
- niemals aufgrund einer Aufforderung (tel. oder Email...) einen Benutzernamen oder Passwort bekanntgeben, egal von wem und unter welchem Vorwand es angefordert wird. Derartige Vorkommnisse, sofort einem Sicherheitsbeauftragten mitteilen.

Begriffe

ActiveX

Technik von Microsoft, Anwendungen autom. um bestimmte Fähigkeiten zu erweitern und ein Interagieren zwischen Anwendungen zu ermöglichen.
Aufgrund der Sicherheitsprobleme von Avtice Content bei Web-Browsern hat es nur sehr geringe Bedeutung erlangt.

Attachment

Anhang, eine an eine Email angehängte Datei.

Backdoor

Server, der versteckt auf einem Computer läuft und einem Angreifer mehr oder weniger vollständigen Zugriff ermöglicht.

Back Orifice 2000.

Dieses Programm ermöglicht dem Hacker, als sogenanntes Trojanisches Pferd in einer anderen Datei versteckt, beliebige Windows 95-, Windows 98-, Windows NT- sowie z. T. Windows 2000-PCs zu manipulieren. So kann dieser unautorisierte Benutzer beispielsweise Maus und Tastatureingaben lenken, protokollieren und auch sperren, Passwörter ablesen, Dateien kopieren oder löschen, Programme öffnen und sogar die Hardware steuern, während er selbst verborgen bleibt. Installiert er ein Zusatzprogramm mit Videomodus, kann er sowohl einen Live-Mitschnitt des Bildschirminhalts anfertigen als auch den Ausspionierten selbst über eine angeschlossene Internetkamera beobachten.

Bouncer

Diese Art von Software läuft meist auf einer Shell und ermöglicht dem Benutzer eine Verbindung ins IRC-Netz. Der Vorteil dabei ist, dass nicht die eigene IP-Adresse zum IRC-Server übermittel wird, sondern die der entsprechenden Shell.

Buffer Overflow

Stapelüberlauf, dieser Angriff führt zu einem Fehler, der unter Umständen dazu ausgenutzt werden kann, beliebigen Code auf einem Fremdrechner auszuführen.

CHAP

Challance Handshake Protocol, Authentifizierungsmethode für PPP mit verschlüsselten Passwörtern.

Chat

Zwei oder mehrere Teilnehmer kommunizieren, indem sie online per Tastatur Nachrichten austauschen. Chat-Foren sind themengebundene Anlaufstellen in denen sich viele Anwender an einer Diskussion beteiligen.

Cheater

Software, die andere Programme täuscht. ZB. Funktionen abfängt und das Ergebnis verfälscht oder durch andere Funktionen ersetzt.

Client

Ein Programm, das Daten von einem Server empfängt. Ein PC wird zum Client, wenn entsprechende Software darauf läuft. Darunter fallen alle Programme, die Zugang zu Internetdiensten erlauben, wie etwa Web-

Browser.

Cracker

Einerseits Personen, die Software "knacken", um Kopierschutz zu entfernen, in der Sicherheitsthematik aber auch Leute, die sich Zugriff auf fremde Rechner verschaffen und diese ausspionieren oder ernsthaften Schaden anrichten.
Im Gegensatz zu einem Hacker zeichnet sich der Cracker durch kriminelle Energie aus und verschafft sich in der Regel persönliche Vorteile.

CSR-Sicherheits-System

Einzigartiger Schutz gegen ungewollte PC-Manipulationen.
Vernichtet nicht nur alle der heute bekannten ca. 40.000 Viren und Trojaner, sondern erkennt auch bislang unbekannte Exemplare und entfernt sie von der Festplatte.
Die Schutz-Software gegen Angriffe und Computer-Viren wie z. B. das gefährliche Ausspäh-Programm Back Orifice 2000.

CSR-Sicherungs-System

autom. Sicherungssystem, das im Notfall eine sofortige Wiederherstellung von möglichst aktuellen Daten erlaubt. Der Zugriff von Cracker, Viren und Anwendern auf diese Sicherungs-Daten ist unmöglich.

Denial of Service (Dos)

Eine Attacke mit dem Ziel, die Verbindung eines Rechners zum Internet zu kappen. Es existieren zahlreiche Varianten, die zu einem Denial of Service führen: Das kann ein einfaches Flooding sein, aber auch trickreiche Methoden, die den Zielrechner dazu bringen, sich durch exzessive Kommunikation lahm zu legen.

DHCP

Dynamic Host Configuration Protocol, Methode, zur autom. Vergabe von festen und dynamischen IP-Adressen an Clients. Neben der IP-Adresse überträgt der DHCP-Server auch Angaben zu Gateway- und DNS-Adressen.

Distributed DoS

Ein Denial-of-Service-Angriff, an dem sich mehrere Rechner beteiligen. Je nach Intensität (Bandbreite) können solche verteilten Angriffe Netzwerkknoten lahmlegen.

DNS

Domain Name System, Protokoll zur Auflösung von Host-Namen in IP-Adressen. Die Datenbank für diese Umsetzung verwaltet ein DNS-

Server. Statt dieser dynamischen Namensauflösung lässt sich in kleinen Netzen auch die statische Umsetzung über die Datei hosts erreichen, in der alle am LAN beteiligten Rechner mit IP-Adresse festgehalten sind.

E-Mail-Bombing

Das Problem des E-Mail-Bombing gewinnt in letzter Zeit zunehmend an Bedeutung. Es kommt immer öfter vor, daß E-Mail-Adressen nichtsahnender Privatanwender von vermeintlichen Freunden oder Rivalen mißbraucht werden. Hierbei werden Tausende von E-Mails an den Anwender geschickt, bis dessen E-Mail-Adresse blockiert oder das System auf Grund von Überlastung lahmgelegt wird.

Exploit

Ein Programm, das eine bestehende Sicherheitslücke im Zielrechner ausnutzt, etwa um dem Angreifer Zugang zu verschaffen.

Firewall, Personal Firewall

Im Unterschied zum Personal Firewall arbeitet ein "richtiger" Firewall auf einem speziell dafür eingerichteten Rechner. Es dient dem Zweck, ein- und ausgehenden Verkehr zu anderen Rechnern (meistens im Internet) zu überwachen und unerwünschte Verbindungen zu unterbinden. Arbeitsplatzrechner befinden sich hinter dem der Firewall: Eine Verbindung ins Internet muss also zunächst den Rechner passieren, auf dem der Firewall läuft.
Ein Personal Firewall hingegen ist ein Programm, das auf dem Rechner aktiv ist, mit dem gearbeitet wird.

Flood, Flooding

Oberbegriff für einen Angriff auf die Verbindung eines Rechners zu einem bestimmten Service im Internet. Es gibt verschiedene Arten von Foods; zu der harmlosen Variante gehören Text-Floods, die beispielsweise im IRC häufig geschehen: Hier werden grosse Mengen von Textzeilen schnell hintereinander an den Client des Opfers geschickt. Eine bösartige Variante ist das Packeting, das direkt auf die IP-Adresse des Opfers zielt.

ftp

File Transfer Protocol, ein Client/Server-Protokoll, das zur Übermittlung von Dateien über TCP/IP dient.

Hacker

Computerspezialisten, die teilweise auch in fremden Systemen nach Sicherheitslücken suchen, diese aber nicht nutzen, um sich selbst zu bereichern.

HTML

Hyper Text Markup Language, Formatierungssprache für Dokumente im WWW.

HTTP, HTTPS
: Hyper Text Transfer Protocol (Secure), ein Client/Server-Protokoll, das im WWW zum Austausch von HTML-Dokumenten dient. Die (Secure-) Variante verschlüsselt die Daten vor der Übertragung.

ICMP
: Internet Control Message Protocol, erlaubt das versenden von Fehlermeldungen sowie Test- und andere Informationspaketen. Es wird häufig zum Packeting missbraucht.

IP-Adresse
: Numerische Adresse zur Identifizierung von Rechnern in einem TCP/IP-Netz. Die 32-Bit grosse IP-(V4)-Adresse wird in vier Oktetten dargestellt (etwa 192.168.0.0). Sie besteht grundsätzlich aus zwei Teilen, netid (Adresse der logischen Netzwerks) und der hostid (Adresse einer Hosts innerhalb des logischen Netzwerks, siehe Netzklassen).

IP-Masquerading
: Sondeform von NAT, dei der mehrere private IP-Adressen auf eine einzige öffentliche Adresse umgesetzt werden.

Java
: Programmiersprache, die von Sun mit Blick auf die Unterstützung von Netzwerken entwickelt wurde. Durch Plattformunabhängigkeit gewährleistet sie die Ausführung der in ihr entwickelten Anwendungen aud den unterschiedlichsten Systemen.
Durch die Netzwerkuntersstützung hat sie vor allem bei der Entwicklung von Anwendungen für das Internet und Applets (Software-Module für Web-Browser) Bedeutung erlangt.

Java Script
: Von Netscape entwickeltem nicht mit Java verwandte Script-Sprache zur Erweiterung der hauseigenen Browsers.

Love-Letter
: Schlagartig hat sich am Donnerstag, den 4. Mai, in Deutschland und der ganzen Welt ein per E-Mail verschickter Wurm (Computervirus) in Deutschland verbreitet.
Die E-Mail hat die Betreffzeile "I love you" und beinhaltet einen Anhang mit dem Namen "Love-Letter-for-you.txt.vbs".
Schon beim Öffnen dieser E-Mail können zahlreiche Dateien auf der Festplatte infiziert und unbrauchbar gemacht werden. Sämtliche E-Mail-Adressen aus dem Verzeichnis bei Microsoft Outlook werden

ausgelesen und der Virus wird an diese Adressen automatisch weiterverschickt. In Deutschland wurden zahlreiche große Unternehmen von dem Virus befallen - auch Privat-User waren betroffen. Experten sprechen von einer neuen Dimension, weil sich der Virus in Windeseile verbreitet hat.
Betroffen sind ausschließlich Computer, auf denen das Betriebssystem "Windows" installiert ist. Eigentlich ist der Wurm für Betriebssysteme Windows 98 /2000 gedacht, allerdings infiziert er auch Windows 95 und NT wenn WSH (Windows Scripting Host) installiert ist.
Inzwischen sind mehrere Kopien des Virusprogramms auch unter anderen Namen im Umlauf.

Version B ist eine "billige" Modifizierung der ursprünglichen Version. Die einzigen Unterschiede liegen darin, dass eingehenden Emails andere Betreffs und Attachments haben. Hier ist der Betreff: "fwd: Joke" anstatt "I-LOVE-YOU", der Name des Attachment ist: "Very Funny.vbs" anstatt "LOVE-LETTER-FOR-YOU.TXT.vbs.", das HTML file, das über IRC gesendet wird, heißt "Very Funny.HTM".
Version C beinhaltet Routinen der CIH Familie (Cernobyl Virus) und ist in der Lage, Festplattenpartitionen zu zerstören. Das Subject der Email ist hier "Subject line: Long time i did not hear from you "attachment" i was missing you. exe".
Version D beinhaltet einen sehr primitiven Trojaner, der eine telnet session ermöglicht (Fernsteuerung des Computers). Das Subject und das Attachment sind wie in Version C beschrieben...

MAC-Adresse

Hardware-Adresse einer Netzwerkkarte. Sie ist für jeden Adapter fest auf der Karte gespeichert und weltweit eindeutig. Alle logischen Adressierungsarten im Netz müssen immer auf die MAC-Adresse umgesetzt werden.

NAT

Network Address Translation, Umsetzung der in der Regel privaten IP-Adressen eines LANs auf anders, meist öffentliche IP-Adressen- Neben der Möglichkeit, mehrere Rechner über eine einzige vom Provider gelieferte IP-Adresse ins Internet zu bringen, verschafft NAT schon einen gewissen Schutz gegen Angriffe aus dem Internet auf Rechner im LAN.

Nuken

Einen fremden PC "abschiessen". Es werden offene Kommunikationsschnittstellen benutzt um den Rechner zum Stillstand zu bringen.

Packeting
: Eine spezielle Form des Flooding: Es werden massenhaft ICMP-Pakete an die IP-Adresse der Opfers geschickt.

Pager
: Ein Chat-Programm, das eine Kontaktliste führt und somit immer anzeigt, welche Bekannten sich gerade online oder offline befinden.

PAP
: Point Autorisation Protocol, Authentifizierungsmethode für PPP. Im Unterschied zu CHAP, das mit Host-Namen arbeitet, beruht PAP auf Benutzernamen und überträgt Passwörter unverschlüsselt.

Phreaker
: Cracker, die sich auf Telefon- und Kommunikationsanlagen spezialisiert haben, um diese für Ihre Zwecke (kostenlos telefonieren...) zu benutzen.

Port
: TCP/IP-Anwendungenkommunizieren mit Partnern auf anderen Rechnern über eine Kombination aus IP-Adresse und Port-Nummer. Diese spezifiziert den Dienst auf dem Ziel-Rechner, der angesprochen werden soll (HTTP/FTP...)

PPP
: Point-to-Point-Protocol, Kommunikationsmethode für TCP/IP zwischen zwei Partnern, die meist über eine Dfü-Verbindung zum Einsatz kommt. In der Regel benutzen Internet-Provider PPP für die Einwahlzugänge.

Private IP-Adressen
: Innerhalb der Netzklassen sind Bereiche für die so genannte private internets vorgesehen. Sie sind im Internet nicht gültig und können daher mehrmals in verschiedenen, nicht verbundenen Netzen eingesetzt werden.

Proxy
: Ein Proxy übernimmt als Stellvertreter für Clients die Kommunikation mit Servern in einem anderen Netz (auch Internet). Es ändert die Datenpakete (Ports) und leitet die Antwort an die entsprechenden Clients weiter.

Routing
: Vermittlung von Datenpaketen zwischen zwei unterschiedlichen IP-Teilnetzen. Router können über spezielle Protokolle die besten Wege zur Weiterleitung der Daten selbstständig miteinander aushandeln.

Scannen
: Systematische Durch- / Untersuchung oder Abfrage. Hacker können mit

Hilfe eines Trojaners einen fremden PC nach gewünschten Daten durchsuchen oder mit einem (Port-) Scanner offene Stellen zum Angriff über das TCPIP-Protokoll suchen.

Server

Ein Rechner, der einem Client Daten zur Verfügung stellt. Jeder Rechner wird zum Server, sofern entsprechende Programme darauf laufen, wie beispielsweise ein ftp-Server.

Shell

Für gewöhnlich ist eine Shell im Zusammenhang mit dem Internet ein Rechner, der ständig mit dem Internet verbunden ist und über den andere Rechner ihre Identität verbergen können.

Sniffer

Programm, das es ermöglicht, die Datenübertragung in Netzwerken (auch Internet) mitzulesen und auszuwertet.

Social Engineering

Dabei wird ein Opfer durch eine vorgebliche Autorität überrumpelt oder trickreich überredet Informationen herauszugeben oder "ungesunde" Kommandos in seinen Rechner einzugeben. Typische Beispiele sind Passwörter oder Kreditkartendaten.

Socket

Ein Mechanismus für virtuelle Verbindungen zwischen einzelnen Prozessen, ursprünglich auf UNIX-Systemen.

Spam

Unaufgefordert versendete Massenwerbung, oft per Email.

Spoofing

Eine Täuschung, bei der man seine Identität hinter einer anderen versteckt. Auch bei Fax oder Email einfach möglich, indem des Absender gefälscht wird.

TCP/IP

Transmission Control Programm / Internet Protocol,
Standard-Protokoll im Internet. IP ist für die Adressierung und Weiterleitung der Daten zuständig. TCP sorgt beim Empfänger für die Sortierung der Pakete in der richtigen Reihenfolge und sichert die Kommunikation durch Bestätigung des Paket-Empfängers ab.

Telnet

Das Internet-Standard-Protokoll für das Einloggen auf entfernten Rechnern. Telnet benutzt TCP/IP mit erweiterten Optionen.

Trojanisches Pferd (Trojaner)

Programme, die meist versteckt in anderen Programmen oder durch irreführende Namen den Rechner eines Opfers ausser Betrieb setzen oder unberechtigten Zugang zum Rechner verschaffen. Durch die Benutzung der lokalen Identität können diese Programme sogar unerkannt durch einen Firewall kommunizieren. Trojanische Pferde vermehren sich im Gegensatz zu Viren weniger selbstständig. Gerade aus diesem Grund sind sie aber schwerer aufzuspüren. Speziell angefertigte Varianten sind nicht zu erkennen.

UDP

User Data Protocol, auf IP basierendes Protokoll, das im Unterschied zu TCP keine direkte Verbindungsaufnahme des Senders mit dem Empfänger notwendig macht (verbindungsloses Protokoll).

URL

Uniform Resource Locator, eindeutige Adresse eines Dokumentes oder einer Datei im WWW.

Verschlüsselung

Ein handelsüblicher PIII braucht im Durchschnitt etwa 15 Min, um einen 40Bit-Schlüssel zu knacken. Standard-Verschlüsselungs-Verfahren bieten also wenig bis keinen Schutz. Ist der Schlüssel einmal bekannt, ist jede Übertragung sofort zu lesen.
Das einzig sichere, ist das dynamische, mehrschichtige Verfahren. Jede Übertragung ist in Anzahl und Verfahren der Schichten unterschiedlich. Nur der Sender und Empfänger kann die Nachricht lesen. Eindeutige Identifizierung des Absenders, Manipulation wird sofort erkannt und ist somit ausgeschlossen. Abgefangenen bzw. vernichtete Nachrichten werden als fehlend erkannt und beim Absender erneut abgefragt. Eine Entschlüsselung ist nicht möglich.

Virus

Selbstreproduzierendes bösartiges Programm, das sich in Bootsektoren oder Dateien einnistet und verändert bzw. zerstört Daten.

Würmer

Eigenständige Programme, die sich über Netzwerkverbindungen vermehren, aber keine anderen Dateien befallen.

WWW

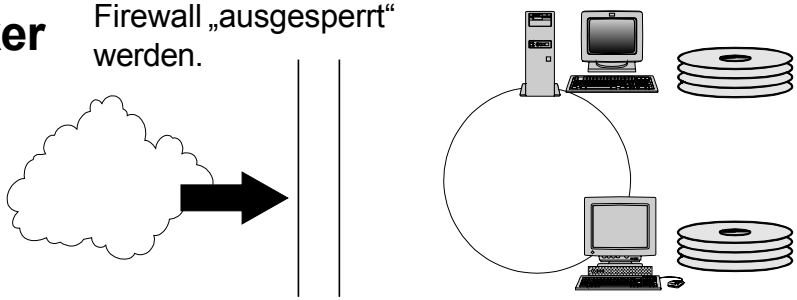
World Wide Web, ein Internetdienst zur plattformunabhängigen Bereitstellungen von miteinander verlinkten Hypertextdokumenten (HTML) und anderen Daten (ftp...). Ursprünglich vom CERN-Institut in Genf.

Hannes Rünagel
Erlenaustr. 27
83022 Rosenheim

Zugriffsmöglichkeiten - Gefahren

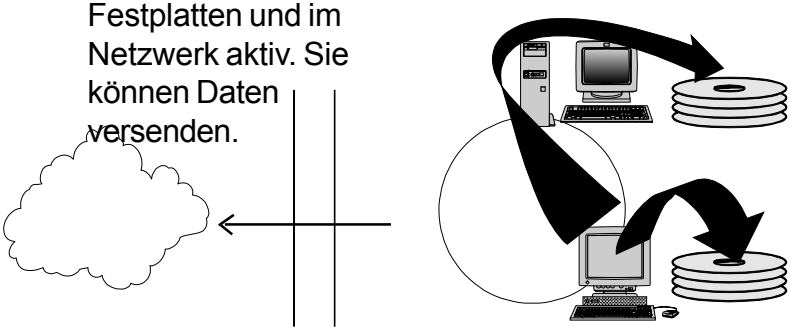
Cracker

können durch einen Firewall „ausgesperrt“ werden.



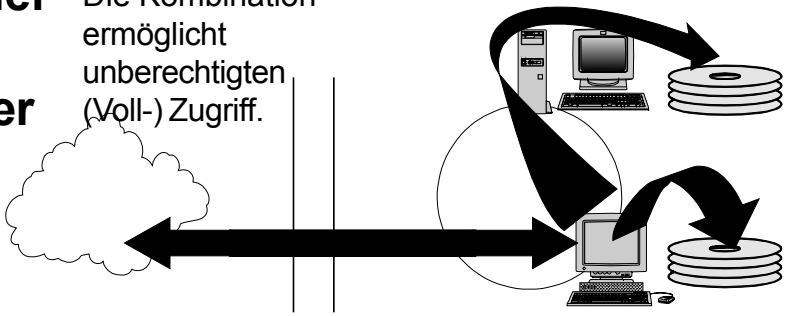
Viren

sind auf den lokalen Festplatten und im Netzwerk aktiv. Sie können Daten versenden.



Trojaner und Cracker

Die Kombination ermöglicht unberechtigten (Voll-) Zugriff.



Derzeitige Standardmethoden erkennen nur die bekannten Angriffe. Unsere Systeme entfernen auch Unbekannte.
Ein schlüssiges Gesamtkonzept vom Profi spart Zeit, Geld und Nerven.