

HEINIGER

Ein Unternehmen der Gruppe
Une entreprise du groupe



**KROMBERG
& SCHUBERT**

www.heiniger-ag.ch

Netzwerk-Lexikon

Heiniger Kabel AG

Bereich EDV-Netzwerke

Sägestrasse 65

3098 Köniz

Tel: 031 970 55 50

Fax: 031 970 55 59

E-Mail: cnet@heiniger-ag.ch



802.11g

Der weit verbreitete 802.11g-Standard arbeitet mit 54 Mbps und ist zu 802.11b abwärtskompatibel. Der gemischte Einsatz von 802.11g- und b-Komponenten reduziert die Performance. Dies kommt häufig vor, wenn ein Nachbar b-Komponenten einsetzt. In den meisten Access-Points ist deshalb die Funktion «G-only» verfügbar. Der Access-Point kann damit auf das 802.11g-Netz fixiert werden, und b-Netze stören die Performance nicht.

802.1Q VLAN

Die VLAN-Funktion vereint die Vorteile von Sicherheit und Performance, sei es Port-basierend oder dynamisch (mit GVRP). VLAN eignet sich zur Isolation des Datenverkehrs verschiedener Benutzergruppen (z. B. Abteilungen), was die Sicherheit erhöht.

ActiveX

Eine von Microsoft entwickelte Technologie, mit welcher es möglich ist, kleine Programme – so genannte ActiveX Controls – beim Anzeigen von Webseiten auf den Rechner des Besuchers zu laden, von wo sie ausgeführt werden. Sie ermöglichen es, unterschiedliche Effekte oder Funktionen umzusetzen. Leider wird diese Technologie häufig missbraucht und stellt ein Sicherheitsrisiko dar. Beispielsweise werden viele Dialer über ActiveX auf den Rechner geladen und ausgeführt. Die ActiveX-Problematik betrifft nur den Internet Explorer, da die anderen Browser diese Technologie nicht unterstützen.

ADSL₁ (Asymmetric Digital Subscriber Line)

Eine Technologie, die einen schnellen und permanenten Internet-Zugang über die Telefonleitung ermöglicht. (siehe DSL)

ADSL 2/2+ ready

Übertragungsgeschwindigkeiten von bis zu 12 Mbit/s (ADSL2) oder 24 Mbit/s (ADSL2+).

Adware

Der Begriff „Adware“ setzt sich aus den englischen Wörtern „Advertising“ (Werbung) und „Software“ zusammen. Eine klare Definitionsgrenze zwischen Spyware und Adware ist schwer zu erkennen. Adware wird vielfach für Werbezwecke verwendet, indem die Surfgewohnheiten des Benutzers aufgenommen und dazu benutzt werden, entsprechende Produkte (z.B. durch Links) zu offerieren. Adware gelangt meist über heruntergeladene Programme auf den Rechner.

Gefahren:

- Ausspähen von vertraulichen Daten (z.B. Passwörtern)
- Gefährdung der Privatsphäre
- Ungewollte Werbung

Massnahmen:

- kostenlose wie auch kommerzielle Tools (Werkzeuge) zum Entfernen von Adware.
- Installieren Sie eine Personall Firewall (dadurch kontrollieren Sie die Verbindungen vom und zum Internet)
- sorgsamer Umgang mit E-Mails und dem Herunterladen von Dateien aus dem Internet

Antennengewinn

Qualitativ gute Antennen haben die Eigenschaft die Sendeleistung zu verstärken. Dieser Gewinn wird in dBi angegeben.

Antennenkabel

Kabel zur Verlängerung zwischen WLAN-Komponente und Antenne. Sollte wenn möglich immer sehr kurz gehalten werden. Kabel bringen einen hohen Verlust der Leistung mit sich.

Antiviren-Software

Antiviren-Software schützt Ihre Daten vor Viren, Würmern oder Trojanischen Pferden. Eine aktuelle Antiviren-Software ist absolut unverzichtbar, wenn Sie Programme und Dateien vom Internet

herunterladen oder mit anderen Personen austauschen. Da allein pro Tag mehrere neue Viren, Würmer oder Trojanische Pferde auftauchen können, ist eine häufige Aktualisierung der Antiviren-Software zwingend erforderlich.

Massnahmen:

- Installation einer aktuellen Antiviren-Software
- Antiviren-Software regelmässig aktualisieren (mind. 3 Mal pro Woche)
- Gültigkeit der Lizenz überprüfen

Applet

Ein kleines Programm zur Verwendung innerhalb von Webbrowser-Umgebungen. Üblicherweise in der Programmiersprache Java geschrieben, die von Sun Microsystems entwickelt wurde. Applets versehen Webseiten im allgemeinen mit Grafiken, Animationen und Texteffekten. Sie sind aus sicherheitstechnischen Gründen relevant, weil Java ungehindert durch Firewalls dringen kann, wenn keine Vorkehrungen dagegen getroffen worden sind.

Applikation

Ein Computerprogramm, das eine bestimmte Aufgabe erfüllt. Textverarbeitungsprogramme und Internet Browser sind Beispiele für Applikationen.

Attacken

Als Attacken bezeichnet man Angriffe aller Art, auf ein System mit dem Ziel, in dieses einzudringen oder es lahmzulegen.

Authentifizierung

Generell: Überprüfen der Identität (und damit der Berechtigung) eines bestimmten Benutzers oder Hosts. Eine solche Authentifizierung kann einfach sein und auf der Anwendungsebene stattfinden (ein Passwort anfordernd). Sie kann jedoch auch sehr komplex sein (wie bei Challenge-Response-Dialogen zwischen Rechnern, die im Allgemeinen auf Algorithmen oder Verschlüsselung auf einer diskreten Ebene des Systems beruhen).

Auto-Cross-over (Auto-MDI/MDIX)

Auto-MDI/MDIX ermöglicht die automatische Anpassung der Sende- und Empfangsleitung eines Ports, d. h. das angeschlossene Ethernet-Kabel (gekreuzt oder nicht gekreuzt) sowie die Konfiguration der Gegenstelle. Alle Auto-MDI/MDIX-Ports können so als Uplink-Port genutzt werden.

Auto-Negotiation

Eine Signalisierungs-Methode, die einem Knoten ermöglicht, seine Arbeitsweise zu definieren: 10 Mbps, 100 Mbps oder 1 Gbps Half- oder Full-Duplex des angeschlossenen Knotens.

Backdoors

Backdoors sind Programme, welche auf Ihrem PC (meist ohne Ihr Wissen) installiert und von fremden Personen benutzt werden können, um Ihren PC zu kontrollieren. Dabei werden die normalen Sicherheitsfunktionen von diesem umgangen, um so quasi von hinten ins Haus zu gelangen. Um ein solches Backdoor unbemerkt zu installieren, werden in der Regel Trojaner (zum Beispiel ein harmlos wirkender Bildschirmschoner oder ein kleines Spiel) verwendet.

Bandbreiten-Management

Verschiedene Anwendungen wie Web, FTP, VPN, VoIP, etc. «kämpfen» um die verfügbare Bandbreite des Internetzugangs. Problematisch ist z.B. der Versand eines grossen E-Mails, wenn gleichzeitig über Internet telefoniert wird (VoIP). Aggressive Anwendungen (wie FTP) nehmen sich so viel Bandbreite wie möglich, zeitkritische Applikationen leiden darunter. Die Qualität eines Telefongesprächs über Internet oder die Stabilität einer VPN-Verbindung können durch den richtigen Einsatz von Bandbreiten-Management verbessert werden.

Black- / White-List,

Black-List (schwarze Liste): Liste von Instanzen wie zum Beispiel Webseiten, die im Vergleich zur Allgemeinheit benachteiligt werden sollen. Die Benachteiligung kann sich beispielsweise in einer Sperre der entsprechenden Webseite äussern.

White-List (weisse Liste): Liste von Instanzen, die nach der Meinung des Verfassers per se vertrauenswürdig sind.

Blackbox-Firewall (Hardware Firewall)

Eine Blackbox-Firewall ist auf einer eigenen Hardware aufgebaut. Eine Firewall als Blackbox ist mit zwei oder drei Ethernet-Interfaces ausgerüstet. Gegenüber einer Firewall als Software ist eine Blackbox einfacher zu installieren und auch kostengünstiger.

Bluetooth,

Eine Technologie, die eine drahtlose Kommunikation zwischen zwei Endgeräten ermöglicht und vor allem bei Mobiltelefonen, Laptops, PDAs und Eingabegeräten (z.B. Computermaus) zur Anwendung gelangt.

Die Zeiten, als Handys lediglich fürs Telefonieren benutzt wurden, gehören der Vergangenheit an. Umfassende Funktionen wie integrierte Kamera, Terminkalender, Spiele, SMS- und MMS-Funktionen, Infrarot- und Bluetooth-Unterstützung oder die Möglichkeit des Surfens im Internet, verwandeln Mobiltelefone in kleine multifunktionale Geräte. „Personal Digital Assistants“ (PDAs) verfügen zumeist ebenfalls über eine Bluetooth-Funktion.

Doch je grösser der Funktionsumfang eines Gerätes, desto höher die Wahrscheinlichkeit, dass Schwachstellen auftreten. Speziell die in Handys umgesetzte Bluetooth-Technologie hat in der Vergangenheit zu mehreren Schwachstellen bei gewissen Mobiltelefonen unterschiedlicher Hersteller geführt.

Gefahren

- Gewisse fehlerhafte Implementationen der Bluetooth-Technologie erlauben unbefugtes Auslesen des Terminkalenders, des Adressbuchs oder gar der gespeicherten SMS-Nachrichten. Weiter kann ein unbemerktes Tätigen von Anrufen oder Verschicken von SMS-Nachrichten sowie die Verbreitung von Handy-Würmern stattfinden.
- Ungewolltes Abschliessen von (teuren) Abonnementen beim Herunterladen von Klingeltönen oder Spielen. SMS-Nachrichten mit der Aufforderung, auf teure 0900 Telefonnummern zurückzurufen.

Massnahmen beim Einsatz von Bluetooth:

- Bluetooth nur bei Bedarf aktivieren (nach Gebrauch deaktivieren)
- Verwenden Sie Bluetooth nur in sicherer Umgebung (nicht an öffentlichen Plätzen)
- Sichtbarkeit des Gerätes für Bluetooth nur bei Bedarf aktivieren
- Sicherheitsoptionen nutzen (aktivieren Sie wenn möglich Authentifizierung und Verschlüsselung)

Massnahmen beim Einsatz von Handys:

- Lesen des Kleingedruckten. Achten Sie beim Herunterladen von Spielen oder Klingeltönen auf mögliche Bedingungen des Diensteanbieters.
- Vorsicht bei SMS-Nachrichten von Unbekannten

Bot / Malicious Bot,

Ursprung im slawischen Wort für Arbeit (Robota). Bezeichnet ein Programm, das bestimmte Aktionen nach dem Empfang eines Befehls selbstständig ausführt. Vor allem im Bereich des IRC werden Bots zur Administration (z.B. Benutzerverwaltung, automatische Sperrung von Benutzern usw.) eingesetzt. Dieses Prinzip wurde in der jüngeren Vergangenheit aber auch von Angreifern missbraucht. So genannte Malicious Bots können kompromittierte Systeme fernzusteuern und zur Durchführung beliebiger Aktionen veranlassen (Versenden von Spam, DoS-Angriffe, Installation zusätzlicher Programme wie beispielsweise Keylogger usw.).

Botnetz,

Eine Ansammlung von Computern, die mit Malicious Bots infiziert sind. Diese lassen sich durch einen Angreifer (den Botnetzbesitzer) komplett fernsteuern. Je nach Grösse kann ein Botnetz aus einigen Hundert bis Millionen kompromittierter Rechner bestehen.

Browser,

Computerprogramme, die vorwiegend dazu verwendet werden, verschiedene Inhalte im World Wide Web anzuzeigen. Die bekanntesten Browser sind Internet Explorer, Netscape, Opera, Firefox und Safari.

Browser-Plug-In,

Software, welche Webbrowsern zusätzliche Funktionalität gibt, beispielsweise um Multimedia Inhalte anzuzeigen.

Bug

Ein Bug ist ein Sicherheitsloch oder eine Schwachstelle eines Computerprogramms. Dieser Begriff bezieht sich auf jede Schwäche in einem System (entweder der Hard- oder Software), die es Eindringlingen ermöglicht, sich unautorisierten Zugang zu verschaffen oder das System lahmzulegen.

CERT (Computer Emergency Response Team)

Das CERT ist eine Sicherheitsorganisation, die sich zum Ziel gesetzt hat, den Betreibern von Computernetzwerken zu helfen, die von böswilligen Benutzern oder Crackern attackiert werden. Sie finden sie unter <http://www.cert.org/>

Chat / Instant Messaging,

Als Chat bezeichnet man eine Kommunikationsmöglichkeit im Internet, bei der man sich in Echtzeit mit anderen Leuten unterhalten kann. Im Gegensatz zum Telefon werden jedoch die Diskussionen nicht durch Sprechen, sondern durch Tippen der Nachrichten geführt. Je nach Themengebiet stehen dafür verschiedene, sogenannte Chat-Räume (auch Kanäle genannt) zur Verfügung. Ein Benutzer kann entweder gleichzeitig mit allen Teilnehmern des Chat-Raums diskutieren oder sich mit einem anderen Benutzer in einen privaten und von den Anderen nicht einsehbaren Raum „zurückziehen“. Im Internet sind verschiedene Chat-Plattformen kostenfrei zugänglich.

Eine ähnliche Kommunikationsmöglichkeit bieten die Instant Messaging-Dienste (z.B. AOL, MSN, ICQ, Yahoo und Skype), bei denen Millionen Benutzer auf der ganzen Welt registriert sind.

Gefahren:

- Durch die (scheinbare) Anonymität werden Chat- bzw. IM-Dienste auch für illegale Machenschaften genutzt, z.B. zur Kontaktsuche von Pädophilen mit Gleichgesinnten und Opfern.
- Einschleppen von Viren, Würmern und Trojanischen Pferden auf den eigenen Rechner.
- Chat- Teilnehmer werden immer wieder aufgefordert, auf Links zu klicken oder unbekannte Befehle einzutippen.

Massnahmen:

- Sorgsamer Umgang mit Chat. Das gilt vor allem für das Öffnen von Dateien und Links.
- Deaktivieren des automatischen Empfangs von Dateien.
- Software-Update. Chat-, respektive IM-Software auf dem neusten Stand halten.
- Keine vertraulichen Informationen im Chat (wie z.B. Passwörter)
- Keine Freigaben. Stellen Sie sicher, dass keine Freigaben (sogenannte Shares) auf Ihrem Rechner eingerichtet sind. Freigaben ermöglichen es, auf einem Windows-System, Dateien oder ganze Laufwerke über das Netzwerk anderen Benutzern zur Verfügung zu stellen. Freigaben sind nicht nur Angriffspunkt für Viren und Würmer, sondern können Ihre (vertraulichen) Daten einem grossen Benutzerkreis (im schlimmsten Fall allen Internet-Benutzern) zugänglich machen.

Citrix ICA

Ist eine kommerzielle Fernsteuerungs-Software für den PC. Siehe auch MS Terminal Service

Client,

Ein Rechner, der die von einem Server angebotenen Dienste beansprucht.

CNM (Centralized-Network-Management) von ZyXEL

Vantage CNM ist eine Software-Applikation, mit der verteilte ZyXEL-Netzwerkkomponenten effizient konfiguriert, analysiert und überwacht werden können.

VPN-Verbindungen

Eine benutzerfreundliche grafische Oberfläche ermöglicht, VPN-Verbindungen einfach per Mausclick zu erstellen. Start- und Endadressen müssen nicht mehr manuell eingegeben werden.

Device- und Account-Management

Vantage CNM ermöglicht, die Netzwerkkonfiguration mit Hierarchiestufen darzustellen, zum Beispiel Firmen-, Abteilungs- oder Device-Level. Für jede Hierarchiestufe lassen sich Benutzer mit unterschiedlichen Zugriffsrechten definieren.

Infrastruktur für Vantage CNM

Für Vantage CNM wird ein Server mit FTP-, Syslog- und Telnet-Dienst vorausgesetzt. Der FTP-Server ist für das Hosten der verschiedenen Firmware-Versionen erforderlich, während der Syslog-Server die Log-Einträge aller gemanagten Devices aufzeichnet. Für den Betrieb des Servers wird eine fixe, öffentliche IP Adresse benötigt. Die örtlich verteilten Devices kommunizieren über das sogenannte Service-Gateway-Management-Protocol (SGMP), wobei die Übertragung sicher mit DES oder 3DES verschlüsselt werden kann. Vantage CNM Administratoren können sich bequem über einen Webbrowser mit Internetzugang mit ihren persönlichen Account-Informationen einloggen. Damit kann der Administrator an einem beliebigen Rechner und Standort auf alle Devices zugreifen.

Code,

Programmanweisungen, die dem Computer die auszuführenden Befehle vorgeben.

Content-Filter von ZyXEL

Kontrollierter Webzugriff mit Content-Filter. Die Kontrolle über die besuchten Websites ist ein wachsendes Bedürfnis von Unternehmen, Schulen und Familien mit Kindern. Mit einem Content-Filter-Service auf der ZyWALL können Webseiten anhand von bestimmten, bereits vordefinierten Kategorien vor Zugriffen gesperrt werden.

Funktion:

Bei ZyXEL greift der Content-Filter auf eine Online-Datenbank beim Dienstanbieter Blue Coat zu und garantiert einen laufend aktualisierten Service. Fast fünf Millionen Webseiten sind derzeit in einer oder mehreren der über 50 Kategorien eingetragen. Noch nicht kategorisierte Webseiten durchlaufen im Hintergrund ebenfalls verschiedene Filter, die auf auffällige Muster reagieren. Unter den noch nicht eingestuften Websites werden diejenigen mit den meisten Zugriffen laufend kategorisiert. Der im Jahresabonnement eingeschlossene Online-Report gibt Aufschluss über die Internetnutzung. Ersichtlich ist der Anteil der verschiedenen Kategorien und die aufgerufenen Websites. Persönlichkeitsrechte bleiben dabei gewahrt, da die IP-Adressen der Benutzer nicht erfasst werden.

Cookie,

Kleine Textdateien, die beim Besuch einer Webseite auf dem Rechner des Benutzers abgelegt werden. Mit Hilfe von Cookies lassen sich beispielsweise persönliche Einstellungen einer Internet-Seite speichern. Allerdings können sie auch dazu missbraucht werden, die Surfgewohnheiten des Benutzers zu erfassen und damit ein Nutzerprofil zu erstellen.

DDoS-Attacks, (Distributed-Denial-of-Service Attacks)

Eine DoS Attacke, bei der das Opfer von vielen verschiedenen Systemen aus gleichzeitig angegriffen wird.

Defacement,

Verunstaltung von Webseiten.

Dialer,

Dialer sind kleine Programme, die einen Internetzugang mit entsprechender Telefonnummer einrichten und sich anschliessend über das Modem oder die ISDN-Karte ins Internet einwählen. Dadurch können kostenpflichtige Internet-Dienste über die Telefonrechnung beglichen werden. Diese an und für sich nützliche Funktion wird leider durch unerwünschte Dialer auch missbraucht. Solche Dialer gelangen über Webinhalte oder heruntergeladene Dateien aus dem Internet, die als „Software Updates“, „Zusatzsoftware“ oder „kostenlose Zugangssoftware“ angeboten werden, auf den Rechner. Um die Installation eines unerwünschten Dialers zu starten, genügt vielfach nur der Aufruf einer entsprechenden Webseite.

Hinweise:

- Benutzer, die nur Breitbandanschlüsse (z.B. Kabelmodem, ADSL) gebrauchen, sind von diesem Problem nicht betroffen.
- Die Betreiber der 0900er-Nummern können nachgeschlagen werden.

Gefahren:

- Verbindungsaufbau ins Internet über teure Mehrwertdienste (z.B. 0900er-, 0901er- und 0906er-Nummern) oder Satellitenverbindungen ohne Wissen des Benutzers.
- Dauerhafte Veränderung des Einwahlvorgangs, so dass künftige Internetverbindungen ebenfalls immer über teure Einwahlnummern laufen.

Massnahmen:

- Einschränkung von Einwahlnummern
Fachgeschäfte bieten sogenannte Dialerblocker für Analog- sowie ISDN Anschlüsse an. Diese Geräte erlauben lediglich einen Verbindungsaufbau über programmierbare Einwahlnummern.
- Sperrung von Telefonnummern
Eine weitere Möglichkeit besteht in der Sperrung von Telefonnummern. Dies kann bei Ihrem Anbieter kostenlos beantragt werden.
- Telefonrechnung limitieren
Die maximale Höhe der Telefonrechnung kann durch den Benutzer festgelegt werden. Informationen dazu sind beim jeweiligen Anbieter zu beziehen.
- Dialerblocker Software
Es gibt kostenlose Programme, die entweder den Dialer oder aber das Einwählen auf teure Telefonnummern erkennen können.

Dial-Up,

Bedeutet „Einwahl“ und bezeichnet das Erstellen einer Verbindung zu einem anderen Computer über das Telefonnetz.

Digitales Zertifikat,

Beglaubigt die Zugehörigkeit eines öffentlichen Schlüssels (PKI) zu einem Subjekt.

DMZ (De-Militarized-Zone)

Öffentliche Server werden am besten in einer geschützten Zone des Netzwerks, der sogenannten DMZ, installiert. Die DMZ wird von der Firewall kontrolliert und geschützt, doch der öffentliche Zugriff auf die Server aus dem Internet ist dennoch möglich.

DNS, (Domain Name System)

Am Internet angeschlossene Rechner kommunizieren über das Internetprotokoll (IP) und haben dafür eine Adresse (z.B. 162.23.39.56). Mit Hilfe von DNS lässt sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z.B. www.heiniger-ag.ch).

DNS-Amplification-Attack,

Denial of Service (DoS)-Angriff, der öffentlich zugängliche DNS-Server missbraucht und als Amplifier (Verstärker) benutzt.

DOS-Attacke, (Denial-of-Service-Attacke)

Hat zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken. Eine populäre Variante von DoS Attacken im IT-Bereich ist das Senden sehr vieler Anfragen an einen Rechner/Dienst. Durch die vielen Anfragen wird der Rechner/Dienst so überlastet, dass er für die Antworten sehr viel Zeit benötigt oder gar ganz ausfällt.

Download

Unter einem Download versteht man den Abruf von Dateien oder Programmen aus dem Internet oder sonst einem Computernetz. Beim Download (=Herunterladen) werden Daten von einem externen Rechner auf Ihren eigenen übertragen.

DSL (Digital Subscriber Line)

Es gibt unterschiedliche DSL-Varianten, welchen die Basistechnologie „Digital Subscriber Line“ gemeinsam ist. ADSL ist eine Variante von DSL und bedeutet „Asymmetric Digital Subscriber Line“. Die ADSL-Technologie benutzt die Telefonleitung, bietet aber in den beiden Übertragungs-Richtungen unterschiedliche Geschwindigkeiten. Daher kommt die Bezeichnung „asymmetrisch“. Im Downstream, also zum Nutzer hin sind Übertragungsraten von bis zu 2 Mbps möglich (ISDN: 64 Kbps bzw. 128 Kbps mit Kanalbündelung). Im Upstream werden bis zu 384 Kbps erreicht. Würde beide Kanäle die gleiche Bandbreite zugewiesen werden, spräche man von SDSL („Synchronous ...“). Weitere DSL-Techniken sind für spezifische Anwendungen verfügbar. G.SHDSL wird für Vernetzungen bis 7 km über 2-Draht-Technologie eingesetzt. VDSL findet Einsatz auf kurzen Distanzen bei höherer Bandbreite.

Dual-Band

Die Dual-Band-Technologie unterstützt den 802.11a- und 802.11g-Standard. Die Komponenten werden wahlweise im «g»-Modus (54 Mbps, 2,4 GHz) oder im «a»-Modus (54 Mbps, 5 GHz) betrieben. Der Standard 802.11a bietet 8 nicht überlappende Frequenzkanäle an. Damit können in überlasteten 802.11g-Gebieten weitere Funknetzverbindungen aufgebaut werden.

Dynamische IP-Adresse

Beim Internetzugang über einen ISP (Internet Service Provider) ist dies das gängige Verfahren eines Sharings von IP-Adressen. D. h. bei Einwahl über einen ISP wird beim LogOn dem Client (eingewählter Rechner) eine freie IP-Adresse des ISP dynamisch (temporär) zugeordnet. Damit wird der Client während der online-Zeit ein Server des Internet. Nach dem LogOff (Beenden der Verbindung) ist diese IP-Adresse wieder verfügbar und wird einer anderen vom ISP vermittelten Verbindung zugeordnet.

ENUM (Electronic-Number-Mapping)

ENUM referenziert Telefonnummern auf Internetadressen. ENUM ermöglicht somit das Zusammenwachsen der alten und neuen Telefoniewelt. Eine weltweite Datenbank ordnet jede bestehende Telefonnummer einer Kommunikationsadresse zu. ENUM basiert auf dem bereits bekannten Domain-Name-System (DNS).

Exploit-Code, (kurz: Exploit)

Ein Programm, ein Script oder eine Codezeile, mit der sich Schwachstellen in Computersystemen ausnutzen lassen.

Finger

Ist ein nur noch wenig genutzter Internetdienst. Mit ihm werden unter anderem Benutzer ausfindig gemacht, die gerade auf einen Server eingeloggt sind.

Firewall,

Eine Firewall (engl. für Brandmauer) schützt Computersysteme, indem sie ein- und ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. So gesehen ist eine Firewall mit einem Wachposten an einem Schlosstor zu vergleichen. Die Entscheidung, welche Verbindungen zugelassen oder zurückgewiesen werden, erfolgt anhand von einfachen Regeln, die bei jedem neuen Verbindungsaufbau abgefragt werden. Durch Firewalls kann das Risiko von unrechtmässigen Zugriffen durch Hacker (Computereindringlinge) gesenkt sowie die Gefahren von Trojanischen Pferden, Spyware oder Würmern minimiert werden. Die meisten Unternehmen schützen ihr Netzwerk mit einer leistungsstarken Firewall, die auf einem speziell dafür vorgesehenen Rechner installiert und zwischen Internet und dem eigenen Netzwerk platziert wird.

Im Gegensatz dazu ist eine Personal Firewall (auch Desktop-Firewall) für den Schutz eines einzelnen Rechners ausgelegt und wird direkt auf dem zu schützenden System – das heisst auf Ihrem Rechner – installiert.

Firmware,

Befehlsdaten zur Steuerung eines Gerätes (z.B. Scanner, Grafikkarten, usw.), die in einem Chip gespeichert sind. Diese Daten können in der Regel über Upgrades geändert werden.

Freeware,

Programme, die kostenlos genutzt werden können.

FTP (File Transfer Protocol)

Es ist ein Protokoll zum Übertragen von Dateien zwischen verschiedenen Rechnern über das Netz. FTP ist einer der am meisten genutzten Dienste im Internet. Einerseits ist es möglich, mit FTP „private“ Dateien von einem Rechner zum anderen zu übertragen. Hierfür benötigt man natürlich auf den beteiligten Rechnern die entsprechenden Zugriffsrechte.

Seine enorme Bedeutung für das Internet erhält FTP jedoch durch weltweit verteilte frei zugängliche Anonymous FTP Server. Das sind Rechner, auf denen immense Mengen an unterschiedlichsten Dateien über FTP zur Verfügung gestellt werden. Man findet auf diesen Archiven Software für fast alle denkbaren Rechnertypen, Dokumente jeglicher Art in allen möglichen Formaten, Bilder, Videosequenzen, Sounddateien und vieles mehr.

G.SHDSL (Global Standard for Single-Pair Highspeed DSL)

Im Jahr 2001 eingeführter Standard für die Übertragung von Daten mit bis zu 2.3 Mbps Upload und 2.3 Mbps Download (symmetrisch) - über herkömmliche, zweiadrige Kupfer-Telefonleitungen. Die Leitungslänge kann im Vergleich zum davor verwendeten SDSL um bis zu 30% grösser sein - maximal 3,5 km sind möglich. G.SHDSL eignet sich für LAN-LAN-Verbindungen und für Broadband-Internetzugang von Firmen, die in beide Richtungen grosses Datenaufkommen haben. Da 2-Draht-Kupferleitungen günstig gemietet werden können, sind diese Lösungen sehr kosteneffektiv und ermöglichen den Einsatz von Broadband-Applikationen wie Streaming und Video-Conferencing.

Hardware,

Sämtliche „anfassbaren“ Teile eines Computers, inklusive Tastatur, Maus, Drucker, externe Datenträger, Grafikkarte, usw.

Hoax,

E-Mails mit Meldungen über neue und angeblich besonders gefährliche Viren sind fast immer Falschmeldungen oder sogenannte Hoaxes (engl. für Falschmeldung, Scherz). Hoaxes sind stets nach dem gleichen Muster aufgebaut. Sie warnen vor einem neuen, überaus gefährlichen Virus, der nicht einmal mit Hilfe einer aktuellen Antiviren-Software bekämpft werden kann. Zudem wird darauf hingewiesen, dass diese Meldung von einem renommierten Unternehmen aus der IT-Branche stammt und an möglichst viele Bekannte weitergeleitet werden soll.

Neben Falschmeldungen über Viren sind auch unterschiedliche Meldungen, die beispielsweise auf das Schicksal von kranken Menschen aufmerksam machen oder ein dubioses Angebot unterbreiten, im Umlauf. Solche Falschmeldungen werden auch als Kettenbriefe bezeichnet.

Gefahren

- Befolgung von im Hoax vorgeschlagenen Massnahmen können zu Datenverlust oder zur Unbrauchbarmachung des Rechners führen.
- Erzeugung von Panik und unnötigem Datenverkehr
- Überlastung der E-Mail-Infrastruktur

Massnahmen

- Im Zweifelsfall weitere Informationen besorgen
Holen Sie im Zweifelsfalle Informationen auf Webseiten von Antiviren-Software Anbietern ein und überprüfen Sie, ob es sich bei einer empfangenen E-Mail um einen Hoax handelt.
- Anweisungen im E-Mail nicht ausführen
Führen Sie keinesfalls die im Hoax empfohlenen Anweisungen aus. Dies betrifft vor allem das Löschen von Dateien, die Installation eines genannten Programms oder das Weitersenden der Meldung an Bekannte.
- Sender auf den Hoax aufmerksam machen
Falls Ihnen der Sender bekannt ist, so machen Sie ihn darauf aufmerksam, dass es sich bei seinem E-Mail um eine Falschmeldung handelt.

Host,

Wurde und wird in der IT vor allem für Rechner mit sehr grosser Rechenleistung verwendet (Bankenumfeld). Heute bezeichnet man damit aber auch kleinere Computersysteme (Computer von Privatanwendern, Webserver usw.).

Host-Files,

Datei, in der IP-Adressen Rechnernamen zugeordnet werden. Diese Datei ist auf jedem Computer vorhanden und wird bei der Auflösung von Rechnernamen/IP-Adressen in der Regel als erste konsultiert (noch vor dem DNS).

Hotfix,

Ein Update, das ein Problem (Fehler, Sicherheitslücke) in einem Programm behebt. Der Begriff Hotfix wird häufig als Synonym für „Patch“ verwendet.

HTML₁ (Hyper Text Markup Language)

In HTML werden die Webseiten erstellt. Damit lassen sich die Eigenschaften der Webseiten (z.B. der Seitenaufbau, das Layout, die Links auf andere Seiten, usw.) vorgeben. Da HTML aus ASCII-Zeichen besteht, kann eine HTML-Seite mit einem gewöhnlichen Textverarbeitungsprogramm bearbeitet werden.

HTTP (Hyper Text Transfer Protocol)

Es wird zum Surfen im World Wide Web (WWW) verwendet und überträgt die im Internet angebotenen HTML Seiten auf den lokalen Rechner, wo sie dann mit Hilfe eines Browsers dargestellt werden.

Zu beachten ist, dass die Kommunikation nicht verschlüsselt erfolgt. Für sicherheitskritische Webseiten wie z.B. Online Banking, Shops etc. sollte HTTP nicht benutzt werden, sondern die verschlüsselte Variante HTTPS.

HTTPS (Hyper Text Transfer Protocol Secure)

Eine Variante von HTTP, bei der die Daten mit Hilfe der SSL Verschlüsselung gesichert übertragen werden. Wird benutzt um bei der Übertragung sensibler Daten das mithören zu verhindern.

IDENT

Ein Dienst, mit dem einem anderem System Benutzerdaten zugestellt werden. Er wird auch als AUTH bezeichnet. Manche Server (z.B. NNTP, IRC, etc.) verwenden diesen Dienst, um die Identität zu überprüfen bevor ein Zugriff erlaubt wird. Die Information ist aber in der Regel nicht vertrauenswürdig, da der befragte Client keinen Beweis über die Richtigkeit seiner Informationen erbringen muss.

IDP (Intrusion Detection & Prevention)

Die IDP erkennt Schädlinge anhand von Mustern (Signaturen) und abnormalem Verhalten. Sie überprüft den Dateninhalt von mehreren IP-Paketen. Durch die Anomalie-Erkennung werden unbekannte Attacken auch aufgedeckt, ohne dass eine neue Signatur vorhanden sein muss.

IDP versus Firewall

Eine Firewall kontrolliert Ports und IP-Adressen. Mit dem Stateful-Packet-Inspection-Mechanismus überprüft sie zudem ganze IP-Sessions auf die korrekte Einhaltung von RFC-Spezifikationen. Eine Intrusion-Prevention-Lösung hingegen untersucht den Dateninhalt von Paketen. Die Lösung von ZyXEL kann sogar fragmentierte IP-Pakete erkennen und analysieren.

IDS₁ (Intrusion Detection System)

Systeme, mit denen man unautorisierte Zugriffe auf Daten oder Rechner erkennen kann.

IGMP-Snooping

Die Funktion IGMP-Snooping verringert den Multicast-Traffic und optimiert die Bandbreitenausnutzung für datenintensive Anwendungen, etwa Videoübertragungen.

IMAP (Internet Message Access Protocol)

Im Gegensatz zu POP3 ist es mit IMAP möglich E-Mails direkt aus der Mailbox auf dem Server zu lesen und zu bearbeiten, ohne dass sie zuerst heruntergeladen werden müssen. Darüber hinaus bietet es gegenüber POP3 eine effizientere Abfrage der E-Mails von verschiedenen Servern.

IMAPS

Eine Variante von IMAP, bei der die Daten mit Hilfe der SSL Verschlüsselung gesichert übertragen werden. Wird benutzt um bei der Übertragung sensibler Daten das mithören zu verhindern.

Instant Messaging,

Siehe „Chat / Instant Messaging“

Internet Service Provider,

Siehe ISP.

IP-Adresse,

Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert. (Beispiel: 130.92.3.15).

IPsec (IP Security)

Entwickelt, um Schwächen des Internetprotokolls (IP) zu beseitigen. Hauptsächlich wird IPsec durch die Protokolle Authentication Header (AH), Encapsulated Security Payload (ESP) und dem Internet Key Exchange (IKE) beschrieben.

IPSec zeichnet sich durch folgende Sicherheitsdienste aus:

- Authentizität (authenticity)
- Unversehrtheit (integrity)
- Vertraulichkeit (confidentiality)

IRC₁ (Internet Relay Chat)

Eine Form des Instant Messaging (IM)-Protokolls.

ISDN₁ (Integrated Services Digital Network)

Digitale Telefonleitung, die gleichzeitig zwei Dienste erlaubt. So ist es beispielsweise möglich, zu telefonieren und zur selben Zeit im Internet zu surfen. Die Datenübertragung ist mit 64, respektive 128 Kbit höher als bei analogen Telefonanschlüssen.

ISP₁ (Internet Service Provider)

Internet-Dienstanbieter, die meist gegen Entgelt verschiedene Leistungen erbringen, die für die Nutzung oder den Betrieb von Internet-Diensten erforderlich sind.

JavaScript,

Eine objektbasierte Scriptingsprache zur Entwicklung von Applikationen. JavaScripts sind im HTML-Code integrierte Programmteile, die bestimmte Funktionen im Internet Browser ermöglichen. Ein Beispiel kann das Kontrollieren von Benutzereingaben bei einem Webformular sein. So kann überprüft werden, ob alle eingegebenen Zeichen bei geforderter Angabe einer Telefonnummer auch wirklich Zahlen sind.

Wie ActiveX Controls werden JavaScripts auf dem Rechner des Webseitenbesuchers ausgeführt. Neben nützlichen, lassen sich leider auch schädliche Funktionen programmieren. Im Gegensatz zu ActiveX werden JavaScripts von allen Browsern unterstützt.

Kabelmodem,

Geräte, die Daten über das Fernseekabel übertragen und empfangen und somit die Nutzung des Internets ermöglichen.

Keylogger,

Geräte oder Programme, die zwischen den Rechner und die Tastatur geschaltet werden, um Tastatureingaben aufzuzeichnen. Diese Aufzeichnungen werden meist in einer Datei auf dem Rechner abgelegt oder direkt über das Internet an einen Server übermittelt. Software-Keylogger sind häufig Bestandteil von Trojanischen Pferden.

Kritische (nationale) Infrastrukturen,

Infrastruktur oder Teil der Wirtschaft, deren Ausfall oder Beschädigung massive Auswirkungen auf die nationale Sicherheit oder die ökonomische und/oder soziale Wohlfahrt einer Nation hat. In der Schweiz sind folgende Infrastrukturen als kritisch definiert worden: Energie- und Wasserversorgung, Notfall- und Rettungswesen, Telekommunikation, Transport und Verkehr, Banken und Versicherungen, Regierung und öffentliche Verwaltungen. Im Informationszeitalter hängt ihr Funktionieren zunehmend von Informations- und Kommunikationssystemen ab.

LAN (Local Area Network)

Sind Rechnernetze, die heute meist als Ethernet über Twisted-Pair-Kabel installiert werden.

LDAP (Lightweight Directory Access Protocol)

Ist ein auf hierarchisch geordnete Informationen optimiertes Protokoll das auf dem Standard von X.500 basiert. Anwendung findet es vor allem bei Verzeichnisdiensten wie z.B. Microsoft Active Directory, SUN One Directory Server und Novell eDirectory.

LDAPS (Lightweight Directory Access Protocol Secure)

Eine Variante von LDAP, bei der die Daten mit Hilfe der SSL Verschlüsselung gesichert übertragen werden. Wird benutzt um bei der Übertragung sensibler Daten das mithören zu verhindern.

Lifeline

Geräte mit Lifeline haben einen Port für den Anschluss an das bestehende Telefonnetz. Sollte der Internetanschluss einmal nicht verfügbar sein, kann darüber weiter telefoniert werden. Mit einem Prefix wählt man für einzelne Gespräche zwischen einem Anruf über VoIP oder das Festnetz. Ausserdem bietet die Lifeline Sicherheit bei Stromausfall, da Anrufe automatisch auf die Lifeline umgeschaltet werden.

Logic Bomb,

Ein Programm, welches beim Eintreffen eines bestimmten Ereignisses eine Funktion auslöst. Logic Bombs werden oftmals von Viren, Würmern oder Trojanischen Pferden genutzt. Die implementierten Schadensfunktionen laufen so zu einem vordefinierten Zeitpunkt ab. Zum Beispiel soll ein Trojanisches Pferd erst dann Tastatureingaben aufzeichnen, wenn der Internet Browser gestartet wird und sich der Benutzer bei einem Online-Dienst anmeldet.

MAC-Adresse, (Media Access Control)

Hardware-Adresse eines Netzwerkadapters zu dessen weltweiten und eindeutigen Identifizierung. Die MAC-Adresse wird vom jeweiligen Hersteller in das ROM des Adapters geschrieben (Beispiel: 00:0d:93:ff:fe:a1:96:72).

Malicious Code,

Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt. Zu dieser Gruppe gehören u.a. Viren, Würmer, Trojanische Pferde. Siehe auch Malware.

Malware,

Setzt sich aus den englischen Begriffen „Malicious“ und „Software“ zusammen. Siehe Malicious Code.

Massenmail-Virus,

Malware, die sich durch Versenden von Mails weiterverbreitet. Häufig wird dafür auch der Begriff „E-Mailwurm“ verwendet.

MIMO (Multiple Input – Multiple Output)

MIMO ist eine neue WLAN-Technologie. Dank mehrerer Antennen werden Daten simultan gesendet und empfangen. Die Vorteile der ZyXEL MIMO-Lösungen (XtremeMIMO) sind ein hoher Datendurchsatz bis 108 Mbps und grössere Reichweiten als mit bisherigen WLAN-Technologien.

MITM, (Man-in-the-Middle Attacke)

Attacke, bei der sich der Angreifer unbemerkt in den Kommunikationskanal zweier Partner hängt und dadurch deren Datenaustausch mitlesen oder verändern kann.

MMS, (Multimedia Messaging Service)

Dienst zum Versenden von Texten, Bildern, Animationen, Audio- und Videodaten an Mobiltelefonteilnehmer.

MP3,

Ein Kompressionsverfahren für Audio-Daten.

MPEG,

Ein Kompressionsverfahren für Multimedia-Daten (z.B. Video), wobei es mehrere Standards gibt (MPEG 1 – 4).

MS RPC

MS RPC ist die Microsoft Implementation von RPC.

MS Terminal Service

Ist eine Grafische PC Fernsteuerungs-Software von Microsoft. Diese ermöglicht es den PC von überall her aus zu benutzen.

NAT (Network-Address-Translation)

Die NAT-Funktion übersetzt die vom Provider erhaltene öffentliche IP-Adresse in interne (private) Adressen. Die IP-Adresse des einzelnen PCs ist somit vom Internet her aus nicht erkennbar, somit auch nicht ansprechbar. Deshalb bietet NAT schon einen gewissen Grund-Schutz.

NetBIOS (Network Basic Input Output System)

Eine Schnittstellenspezifikation für lokale Netzwerke (LAN's), die mit dem Client für Microsoft-Netzwerke und anderen LAN-Betriebssystemen verwendet wird. Anwendungsprogramme verwenden NetBIOS für die Client/Server oder Peer-to-Peer Kommunikation, um die gemeinsame Nutzung von Dateien und Druckern zu unterstützen.

NNTP (Network News Transfer Protocol)

NNTP ist ein Protokoll dass für das Verteilen von Diskussionsforen-Nachrichten zwischen verschiedenen News Servern dient. Weiter wird das Protokoll benutzt für die Kommunikation zwischen den Clients und den News Servern.

NNTPS (Network News Transfer Protocol Secure)

Eine Variante von NNTP, bei der die Daten mit Hilfe der SSL Verschlüsselung gesichert übertragen werden. Wird benutzt um bei der Übertragung sensibler Daten das mithören zu verhindern.

OSPF V2 (Open-Shortest-Path-First)

OSPF ist ein dynamisches Routing-Protokoll und kommt dank der flexiblen Konfiguration vor allem bei mittleren bis grösseren Netzwerken zum Einsatz.

OTIST (One-Touch-Intelligent-Security-Technology)

Der ZyXEL proprietäre Standard OTIST vereinfacht die Wireless Konfiguration mit WPA-PSK Sicherheit, indem der Access-Point seine Sicherheitseinstellungen (SSID, WPA-Schlüssel) direkt mit dem Wireless-Client austauscht.

P2P₁ (Peer to Peer)

Eine Netzwerkarchitektur, bei der die beteiligten Systeme gleiche Funktionen übernehmen können (im Gegensatz zu Client-Server Architekturen). P2P wird häufig zum Austausch von Daten genutzt.

Packet-Filter

Beim Packet-Filter werden die Datenpakete bezüglich Quell- und Zieladresse sowie Protokolltyp analysiert und die Zugriffsbeschränkungen entsprechend der Konfiguration umgesetzt. Die Vorteile eines Packet-Filters sind volle Transparenz und hohe Geschwindigkeit.

Leider werden lediglich Ports gesperrt oder freigeschaltet. Mit Hacker-Techniken wie IP-Spoofing (Vortäuschen berechtigter IP-Adressen) oder Source-Routing (Umleiten von Datenpaketen) können solche Packet-Filter-Firewalls überlistet werden.

Patch

Eine Software, die den fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z.B. eine Sicherheitslücke behebt. Siehe auch Hotfix.

pcAnywhere

Ist eine kommerzielle Fernsteuerungs-Software für den PC. Siehe auch MS Terminal Service.

PDA₁ (Personal Digital Assistant)

Ein kleines elektronisches Gerät, das verschiedene Funktionen (z.B. Agenda, Notizblock, Adressverwaltung, Textverarbeitungsprogramme, E-Mail- und Internet-Zugang) anbietet.

Personal Firewall

Eine Firewall (engl. für Brandmauer) schützt Computersysteme, indem sie ein- und ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. Die Entscheidung, welche Verbindungen zugelassen oder zurückgewiesen werden, erfolgt anhand von einfachen Regeln, die bei jedem neuen Verbindungsaufbau abgefragt werden. Durch Firewalls kann das Risiko von unrechtmässigen Zugriffen durch Hacker (Computereindringlinge) gesenkt sowie die Gefahren von Trojanischen Pferden, Spyware oder Würmern minimiert werden.

Die meisten Unternehmen schützen ihr Netzwerk mit einer leistungsstarken Firewall, die auf einem speziell dafür vorgesehenen Rechner installiert und zwischen Internet und dem eigenen Netzwerk platziert wird.

Im Gegensatz dazu ist eine Personal Firewall (auch Desktop-Firewall) für den Schutz eines einzelnen Rechners ausgelegt und wird direkt auf dem zu schützenden System - d.h. auf Ihrem Rechner - installiert.

Massnahmen:

• Personal Firewall einsetzen

Wie Antiviren-Programme sind auch Personal Firewalls als Zusatzsoftware erhältlich und können teilweise kostenlos vom Internet heruntergeladen werden. Einige Betriebssysteme (z.B. Windows XP, Mac OS X oder Linux) sind bereits mit einer Personal Firewall ausgestattet, die Sie nutzen sollten.

• Personal Firewall kommt vor dem Internet-Anschluss

Wenn Ihr Rechner über ein Personal Firewall verfügt, so aktivieren Sie diese unbedingt bevor Sie den Rechner (zum ersten Mal) am Internet anschliessen. Das Herunterladen von Software Updates sowie weiteren Programmen und Dateien sollte nur bei aktivierter Personal Firewall erfolgen.

Pharming

Manipulation der Namensauflösung via DNS oder via lokale Konfiguration (z.B. Hosts-File) mit dem Ziel Benutzer auf gefälschte Server umzuleiten und so an vertrauliche Daten (Login Daten) zu gelangen.

Phishing

Das Wort Phishing setzt sich aus den englischen Wörtern „Password“, „Harvesting“ und „Fishing“ zusammen. Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen E-Mails mit gefälschten Absenderadressen zustellen. In den E-Mails wird das Opfer beispielsweise darauf hingewiesen, dass seine Kontoinformationen und Zugangsdaten (z.B. Benutzernamen und Passwort) nicht mehr sicher oder aktuell sind und es diese unter dem im E-Mail aufgeführten Link ändern soll. Der Link führt dann allerdings nicht auf die Originalseite des jeweiligen Diensteanbieters (z.B. der Bank), sondern auf eine vom Betrüger identisch aufgesetzte Webseite.

Gefahren

- Mit den erschlichenen Daten kann ein Betrüger im Namen des Opfers (Internet-Benutzer) beispielsweise Banküberweisungen tätigen oder Angebote bei einer Online-Versteigerung platzieren.

Massnahmen

• Vorsicht bei E-Mails

Die E-Mail-Adresse des Absenders lässt sich einfach fälschen, muss also nicht vom vorgegebenen Dienstleistungsanbieter (z.B. der Bank) stammen. Misstrauen bei Links in E-Mails ist angebracht, vor allem dann, wenn diese auf Webseiten führen, die Sie zur Eingabe von vertraulichen Daten auffordern. Gleiches gilt für Formulare in E-Mails. Kein seriöser Dienstleistungsanbieter wird Sie nach einem Passwort fragen.

• Vorsicht bei der Weitergabe von Informationen

Geben Sie keine vertraulichen Informationen (z.B. Benutzername, Passwort, usw.) weiter. Falls jemand auf solchen Informationen besteht, so melden Sie dies Ihrem Vorgesetzten, dem Systemverantwortlichen oder nehmen Sie Kontakt mit dem Dienstleistungsanbieter (z.B. Bank, Internet Service Provider, usw.) auf und fragen Sie nach.

• Software Update des Browsers

Im Zusammenhang mit Phishing werden oftmals auch Fehler (Sicherheitslücken) von Internet Browsern ausgenutzt. Führen Sie deshalb regelmässige Software Updates durch.

PKI (Public Key Infrastructure)

PKI ist die Kombination von Software, Verschlüsselungs-Technologien und -Services, die es Firmen ermöglicht, Sicherheit zu gewährleisten. In einer PKI-Umgebung wird jedem Benutzer ein öffentlicher und ein privater Schlüssel ausgestellt. Der private Schlüssel wird geheim gehalten. Speziell wenn verschiedene Firmen ein VPN untereinander aufbauen, kann eine PKI die Verwaltung der Schlüssel stark vereinfachen. Die Partner müssen sich nicht mehr untereinander auf Schlüssel einigen, sondern können sich gegenseitig ihre Zertifikate schicken, die anhand der Unterschrift der Zertifizierungsstelle und der aktuellen CRL (Certificate-Revocation-List) geprüft werden können. Im laufenden Betrieb kann es sein, dass ein digitales Zertifikat frühzeitig für ungültig erklärt, d.h. gesperrt werden muss, falls der private Schlüssel eines Benutzers gestohlen oder kopiert wurde oder sich andere Änderungen ergeben haben. Wenn ein Benutzer aus einer Firma ausscheidet, wird dies z.B. in der CRL eingetragen. Alle anderen Benutzer können unverändert auf das Netzwerk zugreifen. Ist für alle dynamischen Benutzer «nur» ein und derselbe Pre-Shared-Key konfiguriert, muss bei allen dieser Key geändert werden.

Plug-In,

Eine Zusatzsoftware, welche die Grundfunktionen einer Anwendung erweitert. Beispiel: Acrobat Plug-Ins für Internet Browser erlauben die direkte Anzeige von PDF-Dateien.

PoC, (Proof of Concept)

Ein kurzer, nicht zwangsläufig kompletter Beweis, dass eine Idee oder Methode funktioniert. Beispielsweise werden häufig Exploit-Codes als PoC veröffentlicht, um die Auswirkungen einer Schwachstelle zu unterstreichen.

PoE (Power-over-Ethernet)

Diverse Geräte werden mittels PoE über das Ethernetkabel mit Strom versorgt. Ein Steckernetzteil entfällt.

POP3 (Post Office Protocol, Version 3)

Ist ein Protokoll, das es dem Benutzer erlaubt, seine Email von einem Mail Server auf seinen Rechner herunterzuladen. Dazu werden ankommenden Emails in einem Postfach auf einem Server solange gespeichert, bis der Benutzer sie auf seinen lokalen Rechner herunterlädt.

POP3S

Eine Variante von POP3, bei der die Daten mit Hilfe der SSL Verschlüsselung gesichert übertragen werden. Wird benutzt um bei der Übertragung sensibler Daten das mithören zu verhindern.

Port

Das Internet-Protokoll IP verfügt über mehrere Ports. Über einen Port kommunizieren Applikationen oder Server. Die Ports können aber auch von Hacker für einen unerwünschten Zugriff verwendet werden. Port 80 z. B. steht für HTTP und wird von jedem Browser verwendet.

Port-Mirroring

Port-Mirroring, das Spiegeln eines Ports, erlaubt ein Mitschneiden der übertragenen Daten und bezweckt die Analyse des Datenflusses.

Port-Trunking

Mehrere physikalische Ports werden zu einem logischen Port zusammengefasst. Dadurch wird der Datendurchsatz zwischen zwei Switches erhöht und eine Leitungsredundanz geschaffen.

PPPoE (PPP over Ethernet)

PPPoE ist ein Protokoll, das bei ADSL eingesetzt wird. Über PPPoE identifiziert sich der ADSL-Benutzer beim Provider für seinen Account. PPPoE muss per Software von einem PC oder hardwaremässig von einem Router unterstützt werden.

Proxyserver,

Wird oft als Synonym für HTTP Proxy verwendet. Ein System, welches Browseranfragen entgegennimmt und weiterleitet. Wird u.a zur Beschleunigung von gleichen Anfragen, Überprüfung von Inhalten und zur Anonymisierung benutzt.

QoS

QoS bezeichnet die Priorisierung von IP-Datenpaketen anhand bestimmter Merkmale. Somit können VoIP-Datenpakete, welche einen verzögerungsfreien und kontinuierlichen Datenstrom benötigen, gegenüber anderen Anwendungen bevorzugt werden. Weniger Priorität erhält zum Beispiel ein Download von einem Dateiserver oder der Aufruf von Websites. IPv4 und IPv6 besitzen standardmässig ein Flag im Header (DiffServ, ToS), das die Wichtigkeit der Daten in jedem Paket kennzeichnet. Anhand dieses Flags werden die Datenpakete priorisiert (d.h. bevorzugt) behandelt.

RADIUS-Server

RADIUS-Server werden zur Authentifizierung von Benutzern eingesetzt. Sie geben über einen Benutzernamen und Passwort den Netzwerkzugang frei.

RAID, (Redundant Array of Independent Disks)

Ein Verfahren, bei dem die Daten gleichzeitig auf mehrere Festplatten abgelegt werden. Im Falle eines Festplattenfehlers kann somit Datenverlust vermieden werden. Mit RAID-Systemen ist es auch möglich, die Datentransferraten der Festplatten erheblich zu steigern.

Ransomware,

Malware, mit der die Besitzer der infizierten Rechner erpresst werden sollen (ransom: englisch für Lösegeld). Typischerweise werden Daten verschlüsselt oder gelöscht und erst nach Lösegeldzahlungen der zur Rettung nötige Schlüssel vom Angreifer zur Verfügung gestellt.

Rate-Limiting

Rate-Limiting wacht über die Einhaltung von Bandbreiten auf Eingangs- oder Ausgangsschnittstellen.

Redirect, (dt. Weiterleitung)

Meist benutzt im Zusammenhang mit Webseiten, welche den Leser automatisch auf eine andere Seite weiterleiten.

ROM, (Read Only Memory)

Ein Speicher, bei dem Daten lediglich gelesen, nicht aber überschrieben werden können.

Rootkit,

Eine Ansammlung von Programmen und Techniken, welche es erlauben, unbemerkten Zugriff auf und Kontrolle über einen Rechner zu haben.

RPC (Remote Procedure Call)

Es ist ein Protokoll mit dem in einem Client-/Server-Modell auf einem entfernten Rechner Anwendungen genutzt werden können. Bei Aufruf einer solchen Anwendung auf einem Server werden benötigte Parameter mit übergeben und der Client wartet mit seinem Prozess auf die Antwort. In der Antwort sind die Ergebnisse des Prozesses auf dem Server, mit der der Aufrufer dann weiter arbeiten kann.

RPC ist die konsequente Fortsetzung der Modularisierung in der Programmierung. Prozesse werden ausgelagert und entlasten damit den lokalen Rechner. So können sie auf spezialisierten Plattformen ablaufen, z. B. Datenbank-Server.

RSA-Verschlüsselung,

Abkürzung für Rivest-Shamir-Adleman Verschlüsselung. Verschlüsselungsverfahren mit öffentlichen Schlüsseln, das 1978 eingeführt wurde. RSA ist ein asymmetrisches Verfahren.

RTP / SDP

Für ein Internet-Telefonat braucht es mehr als nur SIP! SIP ermöglicht lediglich die Verbindung zwischen den Teilnehmern – der eigentliche Datenaustausch findet über andere Protokolle statt. Hierzu werden das Realtime-Transport-Protocol (RTP) und das Session-Description-Protocol (SDP) eingesetzt. Die Aufgabe von RTP ist es, den Multimedia-Datenstrom (Audio, Video, Text usw.) zu transportieren, d. h. die von den Codecs codierten und komprimierten Daten zu paketieren und versenden. SDP handelt die zwischen den Endpunkten verwendeten Codecs (z. B. G.711, G.729 für Komprimierung), Transportprotokolle usw. aus.

SCADA-Systeme, (Supervisory Control And Data Acquisition Systeme)

Werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z.B. Energie- und Wasserversorgung).

Server,

Computersystem, welches Clients bestimmte Ressourcen, wie z.B. Speicherplatz, Dienste (z.B. E-Mail, Web, FTP, usw.) oder Daten, anbietet.

Shareware,

Software, die für eine bestimmte Zeit kostenlos getestet werden kann. Oftmals sind in diesen Versionen nicht alle Funktionen nutzbar. Nach Ablauf dieser Zeit sollte das Programm ohne Bezahlung nicht mehr gebraucht werden.

Sicherheitslücke,

Software besteht aus Anweisungen, die dem Rechner die auszuführenden Aktionen vorgeben. Anwendungen setzen sich nicht selten aus Millionen Zeilen solcher Anweisungen zusammen. Bei dieser grossen Anzahl verwundert es nicht, dass sich auch Fehler einschleichen. Design- und Programmierfehler in weit verbreiteten Programmen werden beinahe täglich entdeckt und veröffentlicht. Die meisten dieser Fehler haben allerdings keinen Einfluss auf die Sicherheit eines Systems oder einer Anwendung. Sicherheitsrelevante Fehler können jedoch dazu führen, dass unautorisierte Zugriffe auf Daten und Systeme möglich werden. Solche Fehler bezeichnet man als Sicherheitslücken (engl. Vulnerabilities).

Massnahmen

• Updates

Führen Sie regelmässige Updates von Ihrem Betriebssystem (z.B. Windows XP, Windows 2000, Mac OS X, Linux, usw.) und Ihren Anwendungen (z.B. Internet Browser, E-Mail Client, Media Player usw.) aus. Einige Produkte stellen dafür eine automatische Update-Funktion zur Verfügung. Überprüfen Sie regelmässig, ob diese aktiviert ist.

SIP (Session-Initiation-Protocol)

SIP orientiert sich an der Architektur bekannter Internet-Anwendungen. SIP vereinbart eine Verbindungssession zwischen zwei oder mehreren Teilnehmern.

Die Verbindungen können beliebige Multimedia-Ströme, Konferenzen, Computerspiele etc. sein. SIP basiert unter anderem auf dem HTTP-Protokoll – es verwendet eine ähnliche Header-Struktur und basiert ebenfalls auf Text.

SMB (Server Message Block)

Ein Client/Server orientiertes Protokoll für LAN's, das auf Basis von Anfrage und Rückmeldung (engl. Request und Response) arbeitet. Microsoft benutzt es für MS-DOS und Windows for Workgroups 3.11 sowie Windows 9x, Windows NT und Nachfolger.

Ein Client sendet Anfragen mit SMB mit Hilfe von NetBIOS an einen Server, um freigegebene Ressourcen, wie Drucker, Dateien usw., nutzen zu können. Dabei stehen eine Reihe von Nachrichtentypen zur Verfügung, die in vier Hauptgruppen unterteilt werden können: Sitzungssteuerung, Datei, Drucker und Nachricht.

SMB wird von Microsoft unter CIFS weiter entwickelt. Für das Betriebssystem Linux existiert ein Implementation namens Samba.

SMS, (Short Message Service)

Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer.

SMTP (Simple Mail Transfer Protocol)

Es dient zum Versand von Emails über das Internet. Zu beachten ist dass die Kommunikation nicht verschlüsselt erfolgt.

SMTPS

Eine Variante von SMTP, bei der die Daten mit Hilfe der SSL Verschlüsselung gesichert übertragen werden. Wird benutzt um bei der Übertragung sensibler Daten das mithören zu verhindern.

SNMP (Simple Network Management Protocol)

Es stellt Funktionen zur Verfügung um ein Netzwerk zu überwachen und zu managen.

Social Engineering,

Social Engineering Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Aktionen zu bewegen. Neben allen Angriffsmöglichkeiten ist dies nach wie vor eine der erfolgreichsten. Ein Angreifer kann mittels Social Engineering beispielsweise versuchen, an Benutzernamen und Passwörter von Mitarbeitern eines Unternehmens gelangen, indem er sich am Telefon als Systemadministrator oder Sicherheitsverantwortlicher ausgibt. Durch Vorgeben akuter Computerprobleme und Vortäuschen von Betriebskenntnissen (z.B. Namen von Vorgesetzten, Arbeitsabläufe, usw.) wird das Opfer so lange verunsichert, bis es die gewünschten Informationen preis gibt.

Zur Ausbreitung von Viren oder Trojanischen Pferden werden oft Methoden des Social Engineering angewandt, etwa wenn der Name des E-Mail-Anhangs mit einem Virus einen besonders interessanten Inhalt verspricht (z.B. „I love you“, „Anna Kournikowa“, usw.). Phishing ist ebenfalls eine spezielle Form eines Social Engineering-Angriffs.

Gefahren

- Preisgabe von vertraulichen Informationen
- Betrug
- Verbreitung von Viren und Trojanischen Pferden

Massnahmen

- Vorsicht bei der Weitergabe von Informationen
Geben Sie keine vertraulichen Informationen (z.B. Benutzername, Passwort, usw.) an Personen weiter. Falls jemand darauf besteht, so melden Sie dies Ihrem Vorgesetzten, dem Systemverantwortlichen oder dem Dienstleistungsanbieter (z.B. Bank, Internet Service Provider, usw.). Kein seriöser Dienstleistungsanbieter wird Sie nach einem Passwort fragen.

SOCKS

Ist ein Protokoll, das den Transfer der Pakete über einen Proxy Server überwacht.

Das Protokoll überwacht die ein- und ausgehenden Pakete und verhindert, dass Datagramme, die für interne IP-Adressen bestimmt sind, das Internet erreichen. Ebenso werden Datagramme abgewiesen, die nicht für das hinter dem Proxy-Server liegende Netzwerk bestimmt sind.

Weiter an Bedeutung gewinnt SOCKS bei Multimedia-Anwendung die über eine Firewall kommunizieren müssen.

Eines der wichtigste Elemente ist, dass SOCKS die Authentifizierung eines Benutzers erlaubt bevor diesem Zugriff gewährt wird.

Software Update,

Sicherheitsrelevante Software Updates (sogenannte Patches) schliessen Sicherheitslücken, welche beinahe täglich entdeckt werden. Sicherheitslücken können unrechtmässige Zugriffe auf Ihre Daten oder die Ausbreitung von Würmern ermöglichen und sind sowohl in Betriebssystemen (z.B. Windows XP, Windows 2000, Mac OS X, Linux, usw.) wie auch in Anwendungen (z.B. IIS, Apache, Internet Explorer, Media Player, usw.) vorhanden. Um die Sicherheit Ihrer Daten zu erhöhen, kommt dem Einspielen von Software Updates deshalb eine grosse Bedeutung zu.

Massnahmen

- Regelmässige Updates von Betriebssystem und Anwendungen
Einige Produkte stellen dazu eine automatische Update-Funktion zur Verfügung, die Sie unbedingt nutzen sollten. Überprüfen Sie regelmässig, ob diese aktiviert ist. Informationen zu aktuellen Software Updates sind in der Regel auf den Web-Seiten der jeweiligen Hersteller zu finden.
- Information über Software Updates verfolgen
Weitere Stellen informieren regelmässig über neu aufgetauchte Sicherheitslücken (sogenannte Vulnerabilities) sowie entsprechende Updates (oder weitere Massnahmen).

Source-Code, (dt. Quelltext)

Für den Menschen lesbare Form eines Computerprogrammes.

Spam,

Spam ist der Überbegriff für unerwünschte Werbemails oder Kettenbriefe. Als Spammer bezeichnet man den Verursacher dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird. Gemäss verschiedenen Studien macht der Anteil von Spam bereits mehr als 60% des weltweiten E-Mailverkehrs aus; die Tendenz ist steigend.

Gefahren

- Arbeitszeitverlust, der beim Durchlesen und anschliessendem Löschen der jeweiligen Nachrichten anfällt.
- Immense Belastung der IT-Infrastruktur (Internet, Mailserver).

Massnahmen

- **Vorsichtiger Umgang mit der E-Mail-Adresse**
Die E-Mail-Adresse nur an so wenige Personen wie notwendig weitergeben und ausschliesslich für wichtige Korrespondenz verwenden.
- **Anlegen einer zweiten E-Mail-Adresse**
Für das Ausfüllen von Webformularen, das Abonnieren von Newslettern, Einträge in Gästebücher, usw. empfiehlt es sich, eine zweite E-Mail-Adresse zu verwenden. Diese kann bei verschiedenen E-Mail-Diensten kostenlos beantragt werden. Ist diese Adresse von Spam betroffen, kann sie gelöscht und ersetzt werden.
- **Keine kurzen E-Mail-Adressen**
Spammer setzen Programme ein, die alle Kombinationen kurzer Adressen (z.B. xyz@yahoo.com) ausprobieren. Die Wahl einer langen E-Mail-Adresse kann gewissen Schutz bieten (z.B. hans.muster@heiniger-ag.ch).
- **Spam nicht beantworten**
Wird auf Spam geantwortet, so weiss der Sender, dass die E-Mail-Adresse gültig ist und wird weiter Spam verschicken oder sogar Ihre E-Mail-Adresse weiteren Spammern zur Verfügung stellen. Mit Vorsicht ist auch Spam mit „Abbestelloption“ zu geniessen. Darin wird versprochen, dass man durch Senden einer E-Mail mit bestimmtem Inhalt von der Verteilerliste gestrichen wird. In diesem Zusammenhang sind auch automatische Antwortmails bei Ferienabwesenheit zu beachten. Sie sollten lediglich bei bekannten Adressen aktiviert werden.
- **Filter von E-Mail-Programmen**
Viele E-Mail-Programme weisen Funktionen auf, die das Filtern der eingehenden E-Mails ermöglichen.
- **Spam-Filter**
Auch für den Heimbutzer sowie kleinere und mittlere Unternehmen sind Lösungen entwickelt worden, die das Spam-Problem minimieren sollen. Dabei werden eingehende E-Mails auf bestimmte Kriterien hin untersucht (z.B. Betreffzeile, Absenderadresse, Schlüsselwörter im E-Mail-Text, usw.) und je nach installierten Regeln als erwünschte oder unerwünschte E-Mails eingestuft. Die Schwierigkeit besteht in der Konfiguration dieser Regeln, so dass der Unterhalt eines effektiven Spam-Filters aufwendig ist.
- **Benutzung von Blindkopien beim Versand an viele Adressen**
Bei einem Versand sind die E-Mail Adressen im Empfängerfeld „An“ repektive „To“ oder im Feld für die Kopien „CC“ (Carbon Copy) für alle Mitempfänger sichtbar. Bei einer grossen Anzahl von Empfängern könnten E-Mail-Adressen so in die Hände von Spammern gelangen. Beim Versenden von E-Mails an viele Adressaten sollten Sie die Empfänger ins Feld für Blindkopien „BCC“ (Blind Carbon Copy) eintragen. Der Inhalt des Feldes BCC ist für die Empfänger nicht sichtbar.

Spear Phishing,

Gezielte Phishing Attacke. Dem Opfer wird zum Beispiel vorgegaukelt, mit einer ihr vertrauten Person via E-Mail zu kommunizieren. Dadurch wird das Opfer verleitet, Daten an den Angreifer zu senden oder Programme zu installieren. Das persönliche Umfeld des Opfers wird dabei zuerst in Erfahrung gebracht.

Spyware,

Der Begriff „Spyware“ setzt sich aus den englischen Wörtern „Spy“ (Spion) und „Software“ zusammen. Spyware soll ohne Wissen des Benutzers Informationen über dessen Surfgeohnheiten oder Systemeinstellungen sammeln und diese an eine vordefinierte Adresse übermitteln. Welche Informationen ausgelesen werden, hängt dabei von der jeweiligen Spyware ab und kann von Surfgeohnheiten bis hin zu Passwörtern gehen. Spyware gelangt meist über heruntergeladene Programme auf den Rechner.

Gefahren

- Ausspähen von vertraulichen Daten (z.B. Passwörtern)
- Gefährdung der Privatsphäre
- Ungewollte Werbung

Massnahmen:

- kostenlose wie auch kommerzielle Tools (Werkzeuge) zum entfernen von Adware.
- Installieren Sie eine Personall Firewall (dadurch kontrollieren Sie die Verbindungen vom und zum Internet)
- sorgsamer Umgang mit E-Mails und dem Herunterladen von Dateien aus dem Internet

SSH (Secure Shell)

Mit SSH kann man sich auf einem entfernten Rechner im Netz (Internet) einloggen. Man hat dann die Möglichkeiten ähnlich wie in einem Terminal Fenster zu arbeiten, nur dass sich der Rechner, auf dem man arbeitet am anderen Ende der Welt stehen kann. Im Gegensatz zu Telnet ist die Kommunikation bei SSH verschlüsselt.

SSID, (Service Set Identifier)

Identifiziert den Netzwerknamen des WLAN. Sämtliche Access Points und Endgeräte des WLAN müssen den selben SSID verwenden, um miteinander kommunizieren zu können.

SSL, (Secure Sockets Layer)

Ein Protokoll, um im Internet sicher zu kommunizieren. Der Einsatz von SSL liegt heute beispielsweise im Bereich von Online-Finanz-Transaktionen.

SSL-Zertifikat, (Secure Sockets Layer Zertifikat)

Zertifikat, das benötigt wird, um über SSL zu kommunizieren. Der Einsatz von SSL liegt heute beispielsweise im Bereich von Online-Finanz-Transaktionen.

Stateful-Packet-Inspection

Stateful-Packet-Inspection bietet einem Netzwerk-Schutz vor unerlaubtem Zugriff aus dem Internet. Gleichzeitig wird der Zustand einer Verbindung kontrolliert, d.h. ob die Antwort auf eine Anfrage aus dem internen Netzwerk zurückzuführen ist. In einer internen Tabelle werden diese Verbindungskontrollen verwaltet und überwacht. Dies ist die Basis für die Entscheidung, ob die Firewall ein Datenpaket passieren lässt, oder ob es blockiert wird. Die Einschränkung der Kontrolle auf IP-Adressen und Protokolle unterscheidet die Firewall von Intrusion-Detection-Prevention-Systemen.

STP (Spanning-Tree-Protokoll)

Der integrierte Spanning-Tree-Algorithmus untersucht das Netzwerk auf Ringschlüsse. Ein Ringschluss kann in komplizierten oder doppelt ausgelegten Netzwerken entstehen. Spanning-Tree erkennt dies und sendet die Daten auf dem kürzesten Weg zum Ziel, um die Leistung und Effizienz des Netzwerkes zu maximieren.

Telnet

Mit Telnet kann man sich auf einem anderen Rechner im Netz (Internet) einloggen. Man hat dann die Möglichkeiten ähnlich wie in einem Terminal Fenster zu arbeiten, nur dass sich der Rechner, auf dem man arbeitet am anderen Ende der Welt stehen kann.

Zu beachten ist dass die Kommunikation nicht verschlüsselt erfolgt. Von der Verwendung von Telnet ist aus Sicherheitsgründen abzuraten. Eine sichere und verschlüsselte Alternative bietet SSH.

Timbuktu

Ist eine kommerzielle Fernsteuerungs-Software für den PC. Siehe auch MS Terminal Service.

Tool,

dt. Werkzeug, Dienstprogramm

Traffic-Redirect

Leitet beim Internetverbindungs-Ausfall den Internetverkehr direkt auf einen anderen Internet-Gateway um.

Trapdoor,

Ein verborgener und nicht bekannter Zugang zu einem Rechner oder einer Applikation, der den vorgesehenen Anmeldevorgang (Login-Prozess) umgeht. Trapdoors werden häufig zur Unterstützung der Programmierer während der Entwicklungsphase einer Software eingebaut und bei der Auslieferung nicht immer entfernt.

Trojanisches Pferd,

Trojanische Pferde (häufig als Trojaner bezeichnet) sind Programme, die im verborgenen schädliche Aktionen ausführen und sich dabei für den Benutzer als nützliche Anwendung oder Datei tarnen. Häufig sind Trojanische Pferde Programme, die im Internet heruntergeladen werden. Jedoch auch bei Musikstücken oder Filmen (z.B. im heute üblichen MP3 oder MPEG-Format) kann es sich um Trojanische Pferde handeln. Diese nutzen Sicherheitslücken in den jeweiligen Abspielprogrammen (z.B. Media Player), um sich unbemerkt auf dem System zu installieren. Häufig werden Trojanische Pferde ebenfalls über Anhänge in E-Mails verbreitet.

Gefahren

- Ausspionieren von vertraulichen Daten (z.B. Passwörter für Online-Dienste, Zugangscodes für das Internet-Banking) durch Aufzeichnung der Tastatureingaben und Übermittlung an den Angreifer.
- Unberechtigter Zugriff auf den Rechner (z.B. durch Installation oder Benutzung einer Hintertüre)
- Missbrauch Ihres Rechners, um Spam zu versenden

Massnahmen

- Antiviren-Software
Installieren Sie eine Antiviren-Software und sorgen Sie dafür, dass diese regelmässig aktualisiert wird. Die meisten dieser Produkte verfügen über eine automatische Update-Funktion, die Sie aktivieren sollten.
- Personal Firewall
Installieren einer Personal Firewall. Dadurch können Sie bestimmen, welche Programme Verbindungen ins Internet aufbauen und welche Programme Verbindungen aus dem Internet empfangen dürfen.
- E-Mail- und Internet-Nutzung
Neben technischen Massnahmen trägt vor allem der sorgsame Umgang mit E-Mails und dem Herunterladen von Dateien aus dem Internet zur Sicherheit Ihrer Daten bei (siehe Seite Verhaltensregeln).

Turbo-Card von ZyXEL

Um den Service Anti-Virus/IDP zu aktivieren, installiert man die Turbo-Card im Erweiterungs-Slot. Den äusserst rechenintensive Scan des Datenverkehrs nach Signaturen lagert die ZyWALL auf diese Turbo-Card aus. So bleibt die Performance auch mit aktivierten Services erhalten. Die benötigte Prozessorleistung bietet der speziell für diese Aufgabe entwickelte „SecuASIC-Chip“. Diese Turbo-Card wird bei den Firewallsystemen von ZyXEL eingesetzt.

UPnP (Universal Plug and Play)

Es ist eine Erweiterung des Plug and Play Standards von Microsoft für Netzwerkumgebungen. Der Vorteil ist, dass Netzwerk Komponenten nicht manuell eingebunden und konfiguriert werden müssen.

URL₁ (Uniform Resource Locator)

Die Web-Adresse eines Dokuments bestehend aus Protokoll, Server-Name, sowie Dateiname mit Pfad (z.B. <http://www.heiniger-ag.ch>).

USB₁ (Universal Serial Bus)

Serieller Bus, welcher (mit entsprechender Schnittstelle) den Anschluss von Peripheriegeräten, wie Tastatur, Maus, externe Datenträger, Drucker, usw. erlaubt. Der Rechner muss beim Ein- beziehungsweise Ausstecken eines USB-Gerätes nicht heruntergefahren werden. Die neuen Geräte werden meist (allerdings abhängig vom Betriebssystem) automatisch erkannt und konfiguriert.

USB Memory Stick₁,

Kleine Datenspeichergeräte mit grosser Kapazität (>1GByte), die über die USB-Schnittstelle an einen Rechner angeschlossen werden.

UTM (Unified-Threat-Management)

Virenschutz (Anti-Virus), Intrusion-Detection-Prevention, Anti-Spam und Content-Filter bilden mit der Firewall ein vereintes Sicherheitsteam gegen Gefahren. In einer Hardware aufeinander abgestimmt (All-in-One) bilden sie bereits am Gateway eine widerstandsfähige Schranke gegen verschiedenste Angriffe. Wie beim Sport braucht es auch für den Netzwerkschutz mehrere Stufen für die Abwehr des Gegners resp. der Gefahr.

Gründe für all-in-one

Im KMU-Markt sind All-in-One-Lösungen der Trend. Höhere Kosten und der schwierige Unterhalt von verschiedenen Produkten führen dazu, möglichst viele Sicherheitsaufgaben mit einer Hardware wahrzunehmen.

Viren₁,

Ein Virus besteht aus Programmanweisungen, die dem Rechner die auszuführenden Aktionen vorgeben. Um sich weiterzuverbreiten, nistet sich der Virus in einem „Wirtprogramm“ ein. Das „Wirtprogramm“ kann eine Anwendung (z.B. heruntergeladene Software) oder ein Dokument (z.B. eine Word-Datei, Excel-Datei) sein. Beim Ausführen der Anwendung oder beim Öffnen des Dokuments wird der Virus aktiviert, so dass der Rechner dazu gebracht wird, schädliche Aktionen auszuführen.

Viren gelangen häufig über Anhänge in E-Mails oder über infizierte Dateien, die vom Internet heruntergeladen werden, auf den Rechner. Einmal aktiviert, können sie sich auch per E-Mail an Kontakte im Adressbuch weiterversenden. Weitere Verbreitungswege sind externe Datenträger (z.B. CD-ROM, USB-Memory-Stick, usw.).

Gefahren

- Manipulieren, zerstören und löschen von Daten
- Veränderung von Bildschirminhalten und Anzeigen von Mitteilungen

Massnahmen

- Antiviren-Software
Installieren Sie eine Antiviren-Software und sorgen Sie dafür, dass diese regelmässig aktualisiert wird. Die meisten dieser Produkte verfügen über eine automatische Update-Funktion, die Sie aktivieren sollten.
- E-Mail- und Internet-Nutzung
Neben technischen Massnahmen trägt vor allem der sorgsame Umgang mit E-Mails und dem Herunterladen von Dateien aus dem Internet zur Sicherheit Ihrer Daten bei (siehe Seite Verhaltensregeln).

VNC (Virtual Network Computing)

Es ist eine frei erhältliche Fernbedienungs-Software, welche für die unterschiedlichsten Plattformen verfügbar ist. Durch die Plattform Unabhängigkeit kann man z.B. mit einem Mac einen Windows PC fernsteuern. Siehe auch MS Terminal Service.

VoIP₁ (Voice over IP)

Voice over IP Telefonie über das Internet Protokoll (IP). Häufig verwendete Protokolle: H.323 und SIP.
(Siehe auch SIP, RTP/SDP)

VPN (Virtual Private Network)

Für die Vernetzung von Firmen-Niederlassungen und Heimarbeitsplätzen ist VPN nicht mehr wegdenkbar. Die verfügbaren Netzwerkressourcen (Programme, Dateien, etc.) sind damit über verteilte Standorte nutzbar. Doch nicht nur die VPN-Unterstützung, sondern auch die Verschlüsselungstiefe (DES, 3DES und AES), der mögliche Datendurchsatz und die Authentifizierungsmöglichkeiten stehen für die Qualität einer VPN-Firewall. Die Abfrage von Benutzernamen und Passwort oder die Verwendung von Zertifikaten beim Aufbau einer VPN-Verbindung werden immer häufiger als weitere Sicherheitselemente gefordert. Diese Authentifizierung ist für VPN- und Wireless-LAN-Verbindungen möglich.

Gängige Techniken zum Aufbau von VPNs sind L2TP, PPTP, IPsec, SSL, OpenVPN und PPP über SSH.

VRPT (Vantage-Reporting-Toolkit) von ZyXEL

Das Vantage-Reporting-Toolkit ist nicht zu verwechseln mit Vantage CNM. VRPT ist ein eigenständiges Tool, das grafische Reports erstellt. Es sammelt Informationen von verteilten ZyWALLs und generiert bis zu 26 vordefinierte Reports wie z. B. Bandbreiten- oder Attackenübersicht. Täglich oder wöchentlich lassen sich die Berichte als PDF automatisch per E-Mail versenden.

Automatische Reports

Die VRPT-Server-Lösung ist einfach über einen Browser zu bedienen. Per Knopfdruck werden Reports über Attacken, Intrusions, Bandbreiten-Auslastung, Servicebenutzung etc. erstellt. Verteilte Firewalls können auch getrennt analysiert werden.

Bandbreiten-Report

Dieser Report zeigt einem IT-Administrator ein anomales Verhalten auf. Generiert z.B. eine IP-Adresse aus dem LAN ein erhöhtes Datenvolumen im Vergleich zu den anderen Adressen, könnte auf diesem Rechner ein Schädling am Werk sein. Der betroffene Rechner kann nun gezielt in Quarantäne gesetzt und gesäubert werden.

RRRP (Virtual-Router-Redundancy-Protocol)

RRRP dient einer hochverfügbaren Parallelschaltung (Redundanz) von Switches. Fällt ein Switch unerwartet aus, übernimmt der Parallelgeschaltete, bis der erste wieder einsatzfähig ist.

WDS (Wireless-Distribution-System)

Über das Wireless Distribution System kann zwischen zwei Access Points zusätzlich zu den Client-Verbindungen eine Bridge-Verbindung hergestellt werden. Damit kann beispielsweise der Internet-Zugriff über einen zweiten Access-Point erweitert werden.

WEP, (Wired Equivalent Privacy)

Ein Verschlüsselungsverfahren, das bei WLAN-Verbindungen eingesetzt wird. Verschlüsseln Sie Ihr WLAN wenn möglich mit WPA2, andernfalls WPA oder - wenn nichts anderes verfügbar - WEP.

WLAN, (Wireless Local Area Network)

WLAN steht für drahtloses lokales Netzwerk. In einem WLAN kommuniziert das Endgerät (z.B. ein Laptop, PDA, usw.) über eine drahtlose Verbindung mit einem so genannten WLAN Access Point, welcher seinerseits (wie ein normaler Rechner) über ein Kabel an das Internet oder das lokale Netzwerk angeschlossen wird. Durch die wegfallende Verkabelung der Endgeräte sind die Benutzer mobiler, was der Vorteil eines WLAN ausmacht. Die Reichweite in Gebäuden ist abhängig von den baulichen Gegebenheiten und fällt wesentlich geringer aus als im Freien, wo WLAN-Verbindungen über eine Distanz von mehr als 200 Metern möglich sind.

Gefahren

- Unvorsichtige Konfiguration des WLAN Access Points kann zu uneingeschränktem Zugang zum lokalen Netzwerk (oder Internet) führen. Zugriffe auf Rechner und Daten sowie der Missbrauch des Internetanschlusses sind möglich.

- Unzureichende Verschlüsselung von WLAN-Verbindungen erlaubt das Mitlesen von Daten mit relativ einfachen technischen Hilfsmitteln.

Massnahmen

- **Schutz der Administrationsseite**
Die meisten WLAN Access Points verfügen zur Administration über eine Benutzeroberfläche, die mit einem Browser zugänglich ist. Mit dieser Oberfläche können auch die nachfolgend beschriebenen Einstellungen ausgeführt werden. Der Zugang zu dieser Administrationsseite ist mit einem Standardpasswort geschützt, das umgehend geändert werden sollte.
- **Ändern der Netzwerkkennung**
Ändern Sie die standardmässig vergebene Netzwerkkennung (SSID).
- **Aussendung der Netzwerkkennung unterdrücken**
Verhindern, dass der WLAN Access Point regelmässig seine Netzwerkkennung (SSID) aussendet. Dazu muss die Option „Broadcast SSID“ auf „Nein“ gesetzt werden.
- **Beschränkung des Zugriffs auf Ihre Endgeräte**
Schränken Sie den Zugriff auf Ihren Access Point so ein, dass lediglich Ihre Endgeräte mit ihm kommunizieren dürfen. Dies kann durch Erfassen der MAC-Adresse der Endgeräte erreicht werden.
- **Verschlüsselung einschalten**
Aktivieren Sie an Ihrer WLAN-Hardware die WPA- oder WPA2-Verschlüsselung und wählen Sie dafür ein starkes, schwer zu ratendes Passwort (siehe Verhaltensregeln). Unterstützt Ihre WLAN-Hardware noch kein WPA oder WPA2, aktivieren Sie die WEP-Verschlüsselung. Der WEP-Schlüssel (mit von Ihnen gewählter Schlüssellänge, wenn möglich 128 Bit) muss sowohl dem Access Point wie auch dem Endgerät bekannt sein.
- **Sichere Protokolle verwenden**
Falls vertrauliche Daten über Ihr WLAN übermittelt werden, empfiehlt sich der Einsatz von Protokollen, bei denen die Daten (zusätzlich) verschlüsselt übertragen werden (z.B. VPN, https, ssh, usw.).

WMM (Wi-Fi-Multimedia)

Wurde von der Wi-Fi-Allianz ins Leben gerufen und garantiert eine bessere Übertragung von Audio, Video und Sprache über WLAN. Multimediale Daten werden bevorzugt priorisiert (QoS). WMM ist eine Teilimplementation des IEEE 802.11e-Standards und wird von vielen Unterhaltungsgeräte-Herstellern unterstützt.

WPA (Wi-Fi Protected Access)

WPA ist die Weiterentwicklung von WEP (Wired-Equivalent-Privacy) und bietet dank des dynamischen Schlüsselaustausches eine sehr hohe Sicherheit. WEP wurde vor einigen Jahren geknackt und gilt heute als unsicher. WPA erfordert eine Authentifizierung der User und verschlüsselt die Daten. Für den Verbindungsaufbau wird ein WPA-PSK (Pre-Shared-Key) verwendet. Dieser Schlüssel wird automatisch alle dreissig Minuten ausgewechselt.

Sichert die Daten vor unerwünschtem Mithorchen durch stetiges Ändern des Chiffrierungsschlüssels.

WPA2 (Wi-Fi Protected Access 2)

WPA2 basiert auf dem Standard IEEE 802.11i und eignet sich für professionelle Anwendungen. Die Verschlüsselung basiert auf AES (Advanced-Encryption-Standard). Es stehen dabei zwei Methoden zur Auswahl: WPA2 Personal und WPA2 Enterprise.

Der *WPA2-Personal-Mode* arbeitet mit einem Pre-Shared-Key (PSK). Diese Sicherheitsstufe eignet sich für Infrastrukturen mit wenigen Usern. Nachteil: Wenn eine Person nicht mehr auf das Netzwerk zugreifen darf, muss der PSK bei allen WLAN-Stationen neu definiert werden.

Der *WPA2-Enterprise-Mode* verlangt für den Datenaustausch eine 802.1x-Benutzer-Authentifizierung. Jeder Benutzer muss also Benutzernamen und Passwort eingeben, bevor der Netzwerkzugang freigeschaltet wird. Diese Account-Informationen lassen sich im Windows XP-Client mit SP2 inklusive Security-Update (Microsoft Knowledgebase KB893357) hinterlegen.

Wurm,

Würmer bestehen, wie Viren, aus Programmanweisungen, die dem Rechner die auszuführenden Aktionen vorgeben. Im Gegensatz zu Viren benötigen Würmer zur Verbreitung jedoch kein Wirtprogramm. Vielmehr nutzen sie Sicherheitslücken oder Konfigurationsfehler in Betriebssystemen bzw. Anwendungen, um sich selbständig von Rechner zu Rechner auszubreiten.

Mögliches Ziel für einen Wurm sind Rechner, die Sicherheitslücken oder Konfigurationsfehler aufweisen und in irgendeiner Form mit anderen Rechnern (z.B. über das Internet, das lokale Netzwerk, usw.) verbunden sind.

Gefahren

- Unberechtigter Zugriff auf den Rechner
- Löschen von Daten
- Ausspähen vertraulicher Daten
- Versenden von Spam

Massnahmen

- Updates
Führen Sie regelmässige Updates von Ihrem Betriebssystem (z.B. Windows XP, Windows 2000, Mac OS X, Linux, usw.) und Ihren Anwendungen (z.B. Internet Browser, E-Mail Client, Media Player usw.) aus. Einige Produkte stellen dafür eine automatische Update-Funktion zur Verfügung. Überprüfen Sie regelmässig, ob diese aktiviert ist.

- **Antiviren-Software**

Installieren Sie eine Antiviren-Software, da diese teilweise auch Würmer erkennen kann. Die meisten dieser Produkte verfügen über eine automatische Update-Funktion, die Sie aktivieren sollten.

- **Personal Firewall**

Installieren Sie eine Personal Firewall. Dadurch können Sie bestimmen, welche Programme Verbindungen ins Internet aufbauen und welche Programme Verbindungen aus dem Internet empfangen dürfen.

- **Keine Freigaben**

Vermeiden Sie es, Freigaben auf Ihrem System einzurichten. Würmer können Freigaben zur Verbreitung nutzen (siehe Seite Verhaltensregeln).

Zertifikat

Ein digitales Zertifikat besteht aus Daten, die einen öffentlichen Schlüssel mit einer Benutzererkennung beglaubigen. Dadurch wird verhindert, dass ein falscher Schlüssel zur persönlichen Nutzung dient. Zertifikate enthalten ein Ablaufdatum, den Namen der Zertifizierungsstelle, die das Zertifikat ausgestellt hat und eine eindeutige Seriennummer. Jedes Zertifikat verfügt über ein Ausstellungs- und Verfalldatum. Nur während der Gültigkeitsdauer kann ein Zugriff gewährleistet werden. Wichtig ist ausserdem die digitale Unterschrift.

, Quelle:

Melde- und Analysestelle
Informationssicherung Schweiz MELANI
www.melani.admin.ch

Heiniger Kabel AG

Hauptsitz

Sägestrasse 65
CH-3098 Köniz
www.heiniger-ag.ch

Bereich EDV-Netzwerke

Tel: 031 970 55 50
Fax: 031 970 55 59
cnet@heiniger-ag.ch

Bereich Installationskabel

Tel: 031 970 55 70
Fax: 031 970 55 79
installation@heiniger-ag.ch

Bereich Industriekabel

Tel: 031 970 55 30
Fax: 031 970 55 39
industrie@heiniger-ag.ch

Zweigstellen

Heiniger Câbles SA

Zone industrielle
CH-1564 Domdidier
Tél: 026 676 96 70
Fax: 026 676 96 79
vente@heiniger-ag.ch

Bereich Konfektion

Sumpfstrasse 22
CH-6312 Steinhausen
Tel: 041 749 16 66
Fax: 041 741 29 01
konfektion@heiniger-ag.ch