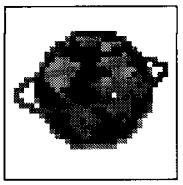
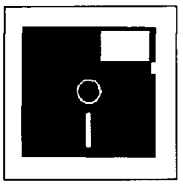



Orientierungshilfe zu Datenschutzfragen bei der Nutzung des Internet durch die öffentliche Verwaltung – Teil II

(Fortsetzung von Teil I, JurPC 7/96, S. 252–256.)

Der saarländische Landesbeauftragte für Datenschutz

III Sicherheitsrisiken im Internet

Zugang bedeutet Risiko.

Mit dem Zugang zum Internet sind Risiken verbunden, die größtenteils daraus resultieren, daß dieses Datennetz historisch gewachsen ist und nicht unter Sicherheitsaspekten entwickelt wurde. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Übertragungswegen und Rechnersystemen. So gibt es beispielsweise keine sicheren Mechanismen zur Identifikation und Authentisierung im Netz. Ohne besondere Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu fremden Rechnern verschaffen und dort Daten ausspähen oder sogar manipulieren oder zerstören. Abgerufene Programme und Dokumente können bekannte und unbekannte Viren enthalten. Programme, Dokumente und Bilder können verfälscht sein. Dies ist besonders gravierend, weil aufgrund der riesigen Zahl von Internet-Teilnehmern auch die Zahl der potentiellen Angreifer, die diese Sicherheitslücken ausnützen und somit die am Internet angeschlossenen Verwaltungsrechner und -netze bedrohen, sehr groß ist.

Kein 100 %iger Schutz möglich.

Die nachfolgend dargestellten Sicherheitsrisiken spiegeln lediglich einen kleinen Ausschnitt der möglichen Angriffe auf Rechnersysteme mit Internet-Anschluß wieder. Selbst wenn Gegenmaßnahmen gegen die bekannten Gefährdungen getroffen werden, läßt sich ein hundertprozentiger Schutz ohne Verzicht auf die Netzanbindung nicht realisieren. Sobald ein Rechner Zugang zu einem Datennetz hat, ist er von den anderen angeschlossenen Rechnern aus erreichbar. Damit wird der eigene Computer der Gefahr einer unberechtigten Nutzung ausgesetzt. Es gibt jedoch eine Reihe von Schutzvorkehrungen, um das Sicherheitsrisiko zu vermindern.

1) Protokollimmanente Sicherheitrisiken

Abhören des Datenaustausches

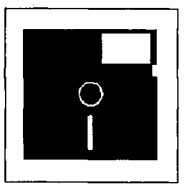
Im allgemeinen werden bei den gängigen Diensten die Daten (z. B. Benutzerkennung, Paßwort; aber auch Kreditkarten- und Kontonummern, Bestell- und Abrechnungsdaten) im Klartext über das lokale Netz (z. B. Ethernet) und über das Internet übertragen. Welchen Weg die Daten nehmen, hängt von der aktuellen Verfügbarkeit und Auslastung der einzelnen Knoten ab und ist nicht vorhersehbar. Jeder Knotenbetreiber, über dessen Rechner die Daten laufen, ist in der Lage, die Daten abzuhören/mitzuschneiden und mißbräuchlich zu benutzen. Mit Programmen, die unter dem Namen Packet Sniffer bekannt und in öffentlichen Mailboxen oder in Internet-Servern abrufbar sind, kann der Datenverkehr im Netz bzw. auf den Netzknoten sogar automatisch belauscht und nach interessanten Informationen durchsucht werden. So können diese Abhörprogramme u. a. zahlreiche Nutzerkennungen mit den zugehörigen Paßworten ausspähen, mit deren Hilfe sich ein Angreifer einen unberechtigten Zugriff auf andere Rechner verschaffen kann. Auf ähnlichem Wege gelang es auch einem Hacker, Kreditkartennummern in Erfahrung zu bringen und damit Zahlungsvorgänge zu Lasten der ahnungslosen Besitzer auszulösen. Der Datenschutz der auf den Rechnern anfallenden Protokolldaten kann nicht gewährleistet werden.

Manipulation von Datenpaketen

Datenpakete können nicht nur abgehört, sondern auch manipuliert werden; z. B. lassen sich die IP-Adressen von Sender und Empfänger fälschen und der Übertragungsweg kann bei dynamischem Routing geändert werden. Pakete können abgefangen werden, so daß sie nicht an ihrem Ziel ankommen; ein Angreifer kann sie durch eigene Pakete ersetzen. Weiterhin läßt sich die Kommunikation eines autorisieren Nutzers mitschneiden und später wieder einspielen (Replay-Attack), wodurch sich der Angreifer bei vielen Diensten die Rechte des Nutzers, in besonderen Fällen sogar des Systemverwalters, verschafft (z. B. beim Festplattenzugriff über ein nicht sicher implementiertes NFS (Network File System) oder bei Fernwartung von Rechnern und Netzen über das Internet).

Bei vielen Internet-Diensten erfolgt die Authentisierung der Rechner lediglich über die IP-Nummer des Nutzers. Dies kann sich ein Angreifer zunutze machen, indem er IP-Pakete mit gefälschten Absenderadressen (bekannt unter dem Begriff IP-Spoofing) ans fremde Rechnersystem schickt. Sofern das System die IP-Adresse für vertrauenswürdig hält, wird

Der saarländische Landesbeauftragte für Datenschutz. Referat für "Kommunikations-, Informations- und Bürotechnik".



dem Eindringling ein Zugang, unter Umständen sogar mit Administratorrechten, gewährt. Nach Erkenntnissen des BSI (Bundesamt für die Sicherheit der Informationstechnik) gibt es etwa jeden Monat eine neue Meldung über Sicherheitslücken oder erfolgreiche Manipulationsversuche im Internet.

2) *Dienste-spezifische Sicherheitsrisiken*

E-Mail und Usenet News

Der elektronische Postweg: Das Tor für Manipulationen

Private Nachrichten können mitgelesen werden, sofern sie nicht verschlüsselt sind. E-Mails und News-Artikel ohne eine digitale Signatur lassen sich leicht verändern oder fälschen, ohne daß dies erkannt werden kann. Es ist nicht sichergestellt, daß jede Mail auch ihren Empfänger erreicht. Jeder kann eine beliebige E-Mail mit einem beliebigen Absender versenden und sich damit für einen Anderen ausgeben. Über den elektronischen Postweg können Programme oder Textdokumente mit Viren ins eigene System gelangen, wenn sie von verseuchten Servern abgerufen werden. Selbst ein automatisches Absuchen der übertragenen Informationen nach Viren bietet keinen vollständigen Schutz, da Virenscanner nur die Viren erkennen können, auf die sie programmiert sind, während fast täglich neue oder Varianten existierender Viren entwickelt werden. Die Informationen über Datum und Uhrzeit der Erstellung einer Nachricht können zu einem Persönlichkeitsprofil des Absenders ausgewertet werden. Daneben forschen Adreßsammler nach E-Mail- und Post-Adressen, um unaufgefordert Werbung zuzuschicken.

Sendmail

Privilegierte Accounts leicht zu erlangen

Das auf UNIX-Rechnern am häufigsten eingesetzte Programm zum Verschicken elektronischer Post weist zudem eine ganze Reihe von sicherheitsrelevanten Fehlern auf, die zu einer Zugangsmöglichkeit mit Administratorrechten führen können.

Telnet

Nichtprivilegierter Accounts: Mißbrauchsmöglichkeiten

Ist der Telnet-Dienst nicht eingeschränkt, sondern von beliebigen Adressen aus zu beliebigen Ports auf dem eigenen Rechner möglich, wird die Zugangskontrolle gefährdet. Auch ein Angreifer, dem es nicht gelingt, sich einen Zugang mit Administratorrechten zu verschaffen, hat häufig die Möglichkeit, einen nichtprivilegierten Account auf dem Rechner zu nutzen. Dieser Account kann dann als Ausgangsbasis für den Angriff auf weitere Rechner verwendet werden.

FTP

Umschlagplatz für Raubkopien

Schlecht gewartete FTP-Server stellen ein Risiko dar, da in älteren Versionen des FTP-Server-Programms (ftpd) Sicherheitslücken existieren, die zur Erlangung von Administratorrechten führen können. Besondere Vorsicht ist geboten, da viele Beschreibungen zur Installation und Konfiguration von Anonymous-FTP-Servern sicherheitsbedenkliche Fehler enthalten. Bei Fehlkonfigurationen kann es einem Angreifer gelingen, die Datei mit den verschlüsselten Paßwörtern aller Benutzer auf seinen Rechner zu laden und dort in aller Ruhe zu entschlüsseln. Läßt man zu, daß Benutzer eines FTP-Servers eigene Dateien in Verzeichnissen ablegen können, wo andere sie sich holen können, kann sich der FTP-Server schnell zu einem Umschlagplatz von Raubkopien entwickeln.

WWW

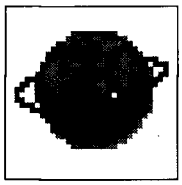
Fehlerhafte Software und Konfiguration

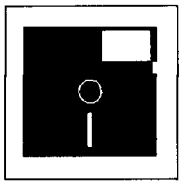
Gefährdungen entstehen bei WWW-Servern durch fehlerhafte Software oder Konfigurationen. Ohne den Einsatz von SSL (Secure Socket Layer) läßt sich die Kommunikation abhören. Außerdem weisen CGI-Skripte häufig Sicherheitslücken auf. Die Ver- und Entschlüsselungstechnik des Browsers NETSCAPE wurde im Oktober 95 durch Hacker aufgedeckt; an einem Update wird gearbeitet.
Zur Zeit sind WWW-Browser in der Entwicklung, die das Ablegen von Dateien auf dem Server erlauben. Dies kann zu weiteren Sicherheitsproblemen führen.
Bei der Nutzung des World Wide Web können zahlreiche Daten über den Anwender und sein Verhalten (was hat wer wann aufgerufen und wie lange gelesen?) protokolliert werden so daß ein umfassendes Persönlichkeitsprofil erstellt werden kann.

Finger

Ausgabe von Nutzerkennungen ermöglicht Angriffe.

Die Daten, die der Finger-Dienst ausgibt, können einem Angreifer Informationen über die Nutzerkennungen auf dem System liefern, die gezielt für einen Angriff genutzt werden können.
Bekannt geworden ist dieser Dienst 1988 durch den sogenannten Internet-Wurm. Dabei handelte es sich um ein Angriffsprogramm, das ausnutzte, daß die beim Aufruf von Finger übergebenen Parameter in einen Puffer fester Länge geschrieben wurden. Die Daten die





nicht mehr in den Puffer paßten, überschrieben den Stack im Arbeitsspeicher, wo sie als Programmcode behandelt und ausgeführt wurden. Bei geschickter Wahl der übergebenen Zeichenreihe kann so beliebiger Code zur Ausführung kommen.

3) Risiken durch unsichere Implementation und Konfiguration

Mangelnde Sorgfalt gefährdet die Sicherheit.

Bei nicht sorgfältiger oder aufgrund mangelhafter Kenntnisse vorgenommener Implementation und Konfiguration können Gefährdungen vorhanden sein, die die Sicherheit des Systems und seiner Daten tangieren und illegale Zugriffe von außen erleichtern.
Unter anderem ist zu nennen:

- Beibehaltung der Schreiberlaubnis für die Root-Partition der Festplatte,
- freier Zugriff auf den Domain Name Server, der die Umsetztabelle für interne in externe Adressen enthält,
- Weitergabe von Konfigurationsdaten durch Befehle wie showmount, rpcinfo, netstat,
- Verfügbarkeit des unsicheren Kommandos rlogin,
- guest-Account ohne Paßwort.

Testprogramme können Sicherheitslücken aufdecken.

Diese und andere Lücken im System werden durch Testprogramme wie ISS (Internet Security Scanner) und Satan (Security Administration Tool for Analysing Networks) aufgedeckt und können legal durch Systemadministratoren aber auch illegal durch Hacker genutzt werden. Diese Programme sind im Internet auf Servern abrufbar, deren Adresse leicht mit Archie gefunden werden kann.

Sicherheitslücken durch Programmierfehler (nicht nur unter UNIX)

Programmierfehler, insbesondere fehlende Kontrolle von Pufferüberläufen, finden sich auch heute noch in vielen anderen Serverprogrammen und sind nicht auf das Betriebssystem UNIX beschränkt. Zum Beispiel ist gerade Ende 1995 ein weiterer solcher Fehler im Programm Sendmail bekannt geworden. Der Protokollierbefehl Syslog und manche WWW-Browser (auch für MS-Windows) enthalten ebenfalls Fehler aus dieser Klasse. Durch eine Zertifizierung unter Zugrundelegung der IT-Sicherheitskriterien ITSEC sollen solche Programmierfehler erkannt und behoben werden. Begünstigend für das Aufdecken und Ausnutzen dieser Lücken für Manipulationen ist auch die allgemeine Verfügbarkeit der Programmquellen des Betriebssystems UNIX bzw. der genannten Dienste und die aufgrund verbreiteter Kenntnisse relativ leichte Recompilierung lauffähiger Software.

Risikovermeidung

Risiken durch die Dienste "Finger" und "Whois" können vermieden werden, wenn der Dienst "tftp" nicht implementiert wird.
Einen weiteren Schutz bieten die Adreßzuweisungen für "Private Internet Netzwerke", wie sie im RFC 1597 definiert sind. Da "private Adressen" keine globale Bedeutung haben, werden Pakete mit solchen Ziel- und Quelladressen von den Netzwerkroutern der Service-Provider ausgefiltert.

Besonders riskant: PC-Einsatz in einem LAN

Der Einsatz von PC in einem LAN stellt ein besonderes Problem dar, da jeder Nutzer Programme zum Mitlesen oder Verändern der auf dem Netz laufenden Daten einspielen kann, wenn er eine Zugangsmöglichkeit zur Betriebssystemebene hat.

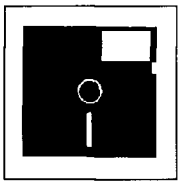
4) Risiken durch Viren

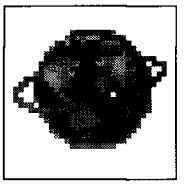
Viren lauern überall.

Bei der Übernahme von Programmen und Dokumenten können unbemerkt bekannte oder unbekannte Viren in das eigene System gelangen. Während Programmviren schon seit längerer Zeit bekannt sind und am Markt entsprechende Prüfprogramme verfügbar sind, sind neuerdings auch Makro-Viren in Winword-Dokumenten bekannt geworden, über deren Risiken noch keine abschließenden Erkenntnisse vorhanden sind. Virenprüfprogramme können nur die Viren erkennen, für die sie programmiert wurden. Es muß aber davon ausgegangen werden, daß weltweit Personen aus verschiedensten Gründen mit krimineller Energie daran arbeiten, neue Viren zu entwickeln, die vorhandene Suchstrategien austricksen können. In Mailboxen und in der Literatur werden unkontrolliert Bauanleitungen zur Virenkonstruktion angeboten; es gibt sogar automatische Virengeneratoren, die vorhandene Viren so modifizieren, daß Virenscanner sie nicht mehr erkennen können. Einige Viren mutieren sich bei ihrer Verbreitung selbst.

Virenschutzmaßnahmen

Neben der Anwendung von permanent aktualisierten Virensuchprogrammen (im Internet verfügbar) kann den Risiken teilweise auch dadurch begegnet werden, daß Programme nur im Quellcode übernommen werden, der geprüft werden kann und daß Programme und Dokumente über Prüfsummenbildung oder Verschlüsselung so gesichert werden, daß sie ohne Gefahr zwischen zwei vertrauenswürdigen Instanzen ausgetauscht werden können.





Anmerkungen

Die vorgestellten Sicherheitsrisiken spiegeln lediglich einen kleinen Ausschnitt der möglichen Angriffe auf Rechnersysteme mit Internet-Anschluß wieder. Selbst wenn Gegenmaßnahmen gegen die bekannten Gefährdungen getroffen werden, läßt sich ein hundertprozentiger Schutz ohne Verzicht auf die Netzanbindung nicht realisieren. Sobald ein Computer Zugang zu einem Datennetz hat, ist er von den anderen angeschlossenen Rechnern aus erreichbar. Damit wird die eigene Maschine der Gefahr einer unberechtigten Nutzung ausgesetzt. Es gibt jedoch eine Reihe von Schutzvorkehrungen, um das Sicherheitsrisiko zu minimieren.

IV Verschlüsselung, Authentisierung

Enkryption und Authentisierung

Beim Datentransport, insbesondere von Email, die vertraulich ist und unter Umständen auch für sichere Zahlverfahren genutzt werden soll, muß sichergestellt sein, daß ein Unberechtigter nicht in der Lage ist, die übertragenen Daten zu lesen (Enkryption), und daß die Daten von einem berechtigten Absender stammen (Authentisierung).

Verschlüsselungsmethoden

Es gibt sehr sichere Verschlüsselungsmethoden (DES, Triple-DES, RSA, IDEA usw.), bei denen der Aufwand zur Entschlüsselung ohne bekannten Schlüssel so hoch ist, daß der Angreifer in einem ausreichenden Zeitraum nicht zum Ziel kommt.

Symmetrische Verfahren

Bei klassischen, "symmetrischen" Verfahren (z. B. DES) müssen sich Absender und Empfänger über den jeweils verwendeten Schlüssel verständigen, was in jedem Falle über einen anderen "Kanal" erfolgen muß, als den der Datenübertragung. Als geeignete PC-Software sei auf das Produkt Wiso-Crypt der Fa. CE Infosys und MIC des BSI verwiesen (siehe Top 4 der AIK-Sitzung vom 17.5.95). Auch beim Produkt Safeguard ist eine Verschlüsselung verfügbar, die auch hardwareunterstützt ablaufen kann. Oft ist es schwierig einen sicheren Kanal zu finden; vor allem aber muß bei wechselnden Partnern eine Vielzahl von Schlüsseln mit großem Aufwand verwaltet werden.

Asymmetrische Verfahren

Bei "asymmetrischen" Verfahren (Public-Key-Verfahren, z. B. RSA) besitzt und benötigt jeder Anwender nur ein Schlüsselpaar aus privatem (geheimem) und öffentlichem Schlüssel. Der öffentliche Schlüssel kann offen mitgeteilt bzw. in öffentlichen Datenbanken gehalten werden. Beim Verschlüsseln wird der öffentliche Schlüssel des Empfängers benutzt, um die Daten für einen Unbeteiligten unlesbar zu machen. Der Empfänger entschlüsselt die Daten mit seinem geheimen Schlüssel.

Eine Variante dieses Verfahrens erlaubt auch eine Authentisierung übertragener Daten (elektronische Unterschrift). Dazu erzeugt der Absender mit seinem privaten Schlüssel und einem geeigneten Verfahren eine Prüfsumme der Daten, die den übermittelten Daten beigefügt ist. Da nur der Absender in der Lage ist, die Daten mit seinem privaten Schlüssel zu kodieren, läßt sich vom Empfänger damit unter Benutzung des öffentlichen Schlüssels des Absenders die Echtheit der Nachricht überprüfen.

Als geeignete Software, die ein Public-Key-Verfahren sowohl für die Ver- und Entschlüsselung als auch für die elektronische Unterschrift nutzt, kann auf die im Internet verfügbare und sowohl auf DOS/Windows-, OS/2-, UNIX- und Großrechner-Systemen anwendbare Software PGP (Pretty Good Privacy; siehe auch Top 4 der AIK-Sitzung vom 17.5.95) oder das Produkt PEM (Privacy Enhanced Mail) der Fa. Trusted Systems Inc. verwiesen werden. Am Markt sind auch hardwaregestützte Produkte verfügbar, und solche, die in Kombination mit einer Chipkarte arbeiten. Bei Public-Key-Verfahren kommt als Problem die sichere Erzeugung von Schlüsselpaaren und die Vertrauenswürdigkeit öffentlicher Schlüssel hinzu. Dies soll durch sogenannte Trust-Center gewährleistet werden, die als zentrale Instanz Schlüssel erzeugen, bei Bedarf verwalten und durch ihre Integrität für die Vertrauenswürdigkeit bürgen. Ein Prüfsummenverfahren zur Sicherstellung der Konsistenz von Dateien ist auch durch das Produkt VALIDATE verfügbar, das in der Landeslizenz für den Virenscanner von McAfee enthalten ist.

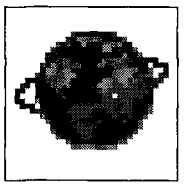
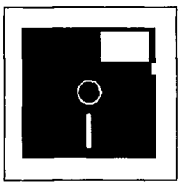
Internet: Einbeziehung neuer Public-Key-Variante

Im Internet, insbesondere beim WWW wird versucht, die Datensicherheit durch eine Einbeziehung des Public-Key-Verfahrens in das Übertragungsprotokoll herzustellen durch Entwicklung einer neuen Variante SHTTP (Secure HyperText Transport Protocol). Noch besser ist allerdings eine automatische Absicherung auf niedrigeren Schichten des Protokolls, da hier keine besonderen Benutzeraktivitäten erforderlich und auch Verkehrdaten einbezogen sind. Hierzu ist eine Variante des IP-Protokolls in Entwicklung, die unter dem Arbeitstitel "IPv6" läuft und 1996 zur Verfügung stehen soll.

Die Authentisierungsverfahren versucht man durch die Verwendung von Einmalpaßwörtern und sogenannten "Challenge-Response-Verfahren" sicherer zu machen. Als Lösung im Internet sei auf das Produkt "skey" verwiesen.

Die Probleme wachsender kommerzieller Netz-Nutzung

Bei zunehmender kommerzieller Nutzung des Netzes wird es zum Problem, aus Abrechnungsgründen zuverlässig festzustellen, welcher Nutzer auf welchem Rechner welche

Dienste in Anspruch genommen hat und nachzuweisen, daß er eine finanzielle Transaktion (Bestellungen, Kontoführung, kostenpflichtiger Informationsabruf) auch selbst verursacht hat. Eine gerichtsfeste Klärung dieser Fragen wird wohl nur mit Verschlüsselung und elektronischen Unterschriften möglich sein. Auf die Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Datenschutz bei elektronischen Mitteilungssystemen wird in diesem Zusammenhang verwiesen.

V. Kommunikationsanalyse, Risikoanalyse und Sicherheitskonzept

Ermittlung des Kommunikationsbedarfs

Bevor eine öffentliche Stelle einen Zugang zum Internet realisiert, muß sie eine Analyse des Kommunikationsbedarfs durchführen. Die Art des zu realisierenden Zugangs hängt wesentlich davon ab, welche Dienste des Internet genutzt werden sollen. Dabei ist zu unterscheiden zwischen Diensten, die von lokalen Benutzern im Internet abgerufen werden, Diensten, die von lokalen Rechnern für Benutzer im Internet erbracht und werden und Diensten, die das Internet als Transportmedium für Verwaltungsdaten nutzen sollen. Auch ist zu klären, ob ein zentraler oder mehrere dezentrale Zugänge zu Internet genutzt werden sollen. Diese Kommunikationsanforderungen müssen aufgrund der unterschiedlichen Aufgaben sowohl für jeden einzelnen Rechner als auch für die Zugänge zum Internet analysiert werden. Aus Sicherheitsgründen ist ein zentraler Zugang vorzuziehen. Es dürfen nur die IP-Pakete weitergeleitet werden, die für den zu nutzenden Dienst – bezogen auf den nutzungsberechtigten Rechner – notwendig sind.

Notwendige Sicherheitsbetrachtungen

Wird bei der Analyse des Kommunikationsbedarfs festgestellt, daß die Anbindung an das Internet auf IP-Ebene notwendig ist, das TCP/IP-Protokoll also in seiner vollen Funktionalität genutzt werden soll, müssen Sicherheitsbetrachtungen durchgeführt werden, die Voraussetzung für die Planung und Realisierung von Sicherheitskonzepten sind. Ausgangspunkte einer derartigen Risikoanalyse sind der Schutzbedarf der zu verarbeitenden Daten und die Sicherheitsziele der öffentlichen Stelle. Auf die im IK-Ausschuß vorgestellte Sicherheitsstrategie auf der Basis eines Schutzstufenkonzeptes wird verwiesen.

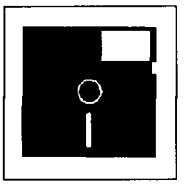
14 Fragen zur Feststellung des Schutzbedarfs

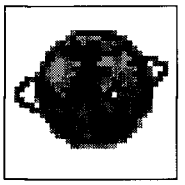
In Anlehnung an die Empfehlungen des BSI-Grundschutzhandbuches sind zur Feststellung des Schutzbedarfs folgende Fragen zu beantworten:

- Ist eine Netzanbindung unbedingt erforderlich, oder reicht es auch aus, die Informationen aus dem Internet mit isolierten PC abzurufen bzw. Angebote für den Zugriff auf dem Internet auf isolierten Servern bereitzustellen?
- Welche Informationen sollen nicht nach außen gelangen?
- Welche Zugänge werden benötigt (Internet-Service-Provider, Zahl der Zugänge, Zahl der Leitungen)?
- Welche Datenmengen werden voraussichtlich übertragen?
- Welche Authentisierungsverfahren sollen genutzt werden; sind benutzerspezifische Authentisierungsverfahren notwendig?
- Welche Dienste sollen auf keinen Fall genutzt werden?
- Wird sichergestellt, daß nur die Dienste genutzt werden können, die ausdrücklich freigegeben worden sind (was nicht erlaubt ist, ist verboten)?
- Welche Datenpakete dürfen auf der Grundlage welchen Protokolls bis zu welchem Rechner im Netz weitergeleitet werden?
- Wie können die interne Netzstruktur und die Benutzernamen nach außen unsichtbar gemacht werden?
- Welche Rechner mit welchen Daten befinden sich im Netz, die geschützt werden müssen?
- Welche Nutzer gibt es im Netz, und welche Dienste sollen dem einzelnen Nutzer zur Verfügung gestellt werden?
- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn Unberechtigte Zugang erhalten?
- Welche Restrisiken verbleiben, wenn die vorgesehenen Schutzmaßnahmen realisiert wurden?
- Welche Einschränkungen würden Benutzer durch den Einsatz von Schutzmaßnahmen akzeptieren?

Um im Rahmen der empfohlenen Kommunikationsanalyse beurteilen zu können, welche Dienste von welchem Nutzer an welchem Rechner tatsächlich benötigt werden, sollten die jeweiligen Stellen zunächst versuchen, sich genaue Kenntnisse über die Möglichkeiten und Gefährdungen der angebotenen Kommunikationsdienste zu verschaffen (etwa durch entsprechende Tests mit an das Internet angeschlossenen Einzelplatz-PC).

Ein Entwurf zum Thema "Internet-Firewalls: Maßnahmeempfehlungen des mittleren Schutzbedarfs für eine Anbindung an das Internet" wird derzeit im BSI erarbeitet.





VI Firewalls

Während bei der Nutzung von Internet im privaten oder wissenschaftlichen Bereich vorhandene Sicherheitslücken nur eine untergeordnete Rolle spielen, kann im Bereich der öffentlichen Verwaltung ein leichtfertiger Umgang mit der Anbindung an das Internet nicht toleriert werden, wenn der Schutz von sensiblen, insbesondere personenbezogenen Daten sichergestellt sein muß.

Das Sicherheitskonzept "Firewall"

Um die oben genannten Schwächen des Internet auszugleichen, wurden unterschiedliche Konzepte und Mechanismen entwickelt, die es unter Beibehaltung eines notwendigen Sicherheitsstandards ermöglichen, die Dienste des Internet zu nutzen. Diese Konzepte sind unter der Bezeichnung "Firewalls" bekanntgeworden.

Funktionsweise

Unter einem Firewall ("Brandschutzmauer") wird eine Schwelle zwischen zwei Netzen verstanden, die überwunden werden muß, um Systeme im jeweils anderen Netz zu erreichen.

Die Hauptaufgabe eines Firewalls besteht darin, zu erreichen, daß jeweils nur zugelassene netzübergreifende Aktivitäten möglich sind und daß Mißbrauchsversuche frühzeitig erkannt werden können. Sie verhindern eine unkontrollierte Kopplung zwischen dem lokalen Behördennetz und dem unüberschaubaren, anonymen Internet.

Üblicherweise wird dabei davon ausgegangen, daß die Teilnehmer des internen Netzes vertrauenswürdiger sind, als die Teilnehmer des externen Netzes. Gleichwohl sind Firewall-Lösungen auch geeignet, die "grenzüberschreitenden" Aktivitäten der internen Nutzer zu beschränken.

Charakteristika

Firewalls weisen die folgenden Charakteristika auf:

- der Firewall ist die definierte und kontrollierte Schnittstelle zwischen dem zu schützenden und dem nicht vertrauenswürdigen Netz;
- im internen Netz besteht jeweils ein einheitliches Sicherheitsniveau; eine weitere Differenzierung nach Sicherheitsstufen geschieht – zumindest auf der Ebene des Netzes – nicht;
- der Firewall setzt eine definierte Sicherheitsstrategie für das zu schützende Netz voraus; in diese müssen die Anforderungen aller vernetzten Stellen einfließen,
- es besteht die Notwendigkeit einer firewall-bezogenen Benutzerverwaltung derjenigen internen Teilnehmer, die mit Rechnern in dem externen Netz kommunizieren dürfen.

Faktoren der Schutzstärke

Die Stärke der Firewalls hängt wesendich von der eingesetzten Technik und ihrer konkreten Administration ab; entscheidend für die Sicherheit sind jedoch auch die Staffelung und die organisatorische Einbindung der Firewalls in die IuK-Infrastruktur.

Es sollten möglichst Firewalls in Form eines "dual-home-gateway" eingesetzt werden, um eine logische und physikalische Netzabtrennung zu erreichen. Das lokale Netz ist dann für das Internet praktisch unsichtbar. Die Software des Firewall sollte möglichst die Anforderungen der IT-Sicherheitskriterien ITSEC Stufe E3 erfüllen.

Definition des Schutzbedarfs

Von besonderer Relevanz ist der Aspekt, daß für den von einem Firewall geschützten Bereich der erforderliche Schutzbedarf definiert wird. Diese Anforderung kann mit zwei Lösungsvarianten erfüllt werden:

1. einheitlich hoher Schutzbedarf im internen Netz einschließlich seiner Subnetze, d. h. Orientierung am höchsten vorhandenen Schutzbedarf und entsprechende Auslegung des Schutzniveaus des zentralen Firewalls;
2. mindestens mittlerer Schutzbedarf für das angekoppelte Netz und entsprechende Auslegung des Firewall-Schutzniveaus, falls der Schutzbedarf der kritischsten Anwendung des Netzes nicht höher ist, sowie Durchführung zusätzlicher Maßnahmen zum Schutz von Netz-Komponenten mit höherem Schutzbedarf bzw. Einrichtung zusätzlicher abgestufter, dezentraler Firewalls mit höherem Schutzniveau für Subnetze mit höherem Schutzbedarf (bereichsbezogen und bedarfsorientiert).

Weitere Absicherungsmöglichkeiten

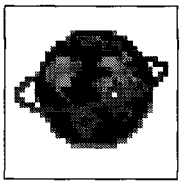
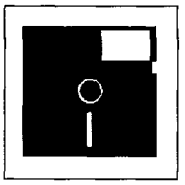
Von außen kommende Zugriffe auf interne Informationen können auch dadurch abgesichert werden, indem der Internet-Server vor dem Firewall und nicht im dahinterliegenden Netz installiert wird und ausschließlich für diese Funktion bereitgehalten wird. Durch zeitschrankengebundene Zugriffsintervalle kann die Sicherheit weiter verbessert werden.

1) Zentrale Firewalls

Charakteristika

Rein zentrale Firewall-Lösungen sind durch folgende Aspekte charakterisiert:

- der zentrale Firewall bildet die einzige Schnittstelle zwischen dem kompletten zu schützenden Verwaltungsnetz und dem übrigen Internet;
- innerhalb des Verwaltungsnetzes besteht ein einheitliches Sicherheitsniveau, eine weitere Differenzierung nach Sicherheitsstufen erfolgt nicht;
- eine Kontrolle der internen Verbindungen durch den Firewall ist nicht möglich; der zentrale Firewall setzt eine definierte Sicherheitsstrategie für das gesamte Verwaltungsnetz

voraus; abweichende Sicherheitsstrategien für besonders schützenswerte Bereiche sind auf Netzebene nicht durchsetzbar;
- es besteht die Notwendigkeit einer zentralen Benutzerverwaltung. Für jeden Teilnehmer muß sowohl auf Dienstebene als auch bezogen auf die zugelassenen Adressen die zulässige Kommunikation festgelegt werden; die Zuordnung zwischen internen und externen Adressen wird durch einen Name-Server hergestellt, so daß das interne Netz nach außen unsichtbar ist.

Durch Zusammenfassung aller internen Internet-User in einem physikalischen Segment des lokalen Netzes können Durchbrüche von außen kommender Angreifer verhindert werden.

Das Schutzniveau richtet sich nach den sensibelsten Daten.

Da ein zentraler Firewall eine Differenzierung nach Teilnetzen nicht unterstützt und dementsprechend ein einheitliches Sicherheitsniveau für das gesamte Verwaltungsnetz voraussetzt, muß sich der Grad des gewährleisteten Schutzes nach den sensibelsten Daten bzw. Anwendungen richten und ist dementsprechend hoch. Dies hat jedoch für Verwaltungsbereiche mit weniger sensiblen Daten den Nachteil, unnötig hohe Schranken zu errichten. Daraus ergibt sich die Gefahr, daß von diesen Stellen "mit Bordmitteln" zusätzliche Internet-Zugänge mit geringeren Restriktionen geschaffen werden, wodurch der gesamte Zweck der Firewalls ad absurdum geführt wird.

Hoher Administrationsaufwand

Ein weiterer Nachteil zentraler Firewalls besteht in dem hohen Administrationsaufwand und dem – auch aus dem Großrechnerbereich bekannten – Problem, daß eine Benutzerverwaltung, die fernab von dem jeweiligen Fachbereich erfolgt, häufig zu schwerfällig zu handhaben und aktuell zu halten ist.

Da sich Firewall-Lösungen primär zum Schutz gegen Zugriffe von außen eignen, sekundär auch zum Schutz gegen Zugriffe von innen nach außen, jedoch nicht zur Kontrolle der rein internen Zugriffe, besteht bei rein zentralen Lösungen die Gefahr, daß das gesamte Verwaltungsnetz als eine Einheit betrachtet wird und insofern nur die Zugriffe von oder nach außen einer Beschränkung unterworfen werden. Dieser Aspekt ist zwar nur mittelbar Teil des Themas "Internetanbindung", muß bei einer Gesamtbetrachtung von Netzwerksicherheit jedoch unbedingt einbezogen werden.

Nicht geeignet für behördenübergreifende Netzstrukturen

Der Einsatz eines alleinigen zentralen Firewall ist allenfalls dann vertretbar, wenn es sich um ein einziges Netz handelt bzw. alle angeschlossenen Teilnetze über ein gleiches Sicherheitsbedürfnis bzw. -niveau verfügen und zudem nicht die Gefahr des internen Mißbrauchs besteht. Falls komplexe, behördenübergreifende Netzstrukturen mit einer Vielzahl darin betriebener Rechner angeschlossen werden soll, sollte jedoch das Konzept der gestaffelten Firewalls realisiert werden.

2) Gestaffelte Firewalls (Voraussetzungen, Einsatzmöglichkeiten, Forderungen)

Charakteristika

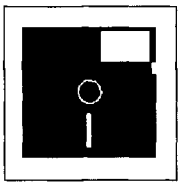
Gestaffelte Firewall-Lösungen sind durch folgende Aspekte charakterisiert:
- es handelt sich um eine Kombination zentraler und dezentraler Komponenten, wobei durch einen zentralen Firewall ein Mindestschutz für das Gesamtnetz gegenüber dem Internet realisiert wird und dezentrale Firewalls in Subnetzen mit besonderem Schutzbedarf ein angemessenes Schutzniveau sicherstellen;
- innerhalb des jeweiligen geschützten Subnetzes besteht jeweils ein einheitliches Sicherheitsniveau;
- eine Kontrolle der verwaltungsinternen Verbindungen ist möglich, sofern die Kommunikation den durch dezentrale Firewalls geschützten Bereich überschreitet;
- auch ein gestaffeltes Firewall-System setzt eine definierte Sicherheitsstrategie für das Gesamtnetz voraus; in diese müssen insbesondere die Anforderungen an einen zu garantierenden Grundschutz für mittleren Schutzbedarf einfließen; darüber hinaus sind für die Subnetze gesonderte Sicherheitsanforderungen zu definieren;
- die Benutzerverwaltung kann weitgehend dezentralisiert werden. Allerdings sind einheitliche Regeln festzulegen, nach denen Benutzer das Recht haben, über den zentralen Firewall mit Systemen im Internet in Verbindung zu treten.

Gewährleistet: Autonomer Schutz von Subnetzen

Für die dezentralen Firewalls bieten sich prinzipiell die gleichen Mechanismen wie bei einem zentralen Firewall an. Die Kombination zentraler und dezentraler Schutzmechanismen erlaubt die Realisierung des Prinzips eines autonomen Schutzes; bei sorgfältiger Konfiguration bleiben besonders geschützte Subnetze auch dann gesichert, wenn der zentrale Firewall durch einen Eindringling überwunden wurde.

Das Prinzip der informationellen Gewaltenteilung

Mit gestaffelten Firewalls kann – anders als bei zentralen Lösungen – das datenschutzrechtlich bedeutsame Prinzip der informationellen Gewaltenteilung abgebildet werden, mit dem es nicht zu vereinbaren wäre, wenn die Verwaltung als informatorisches Ganzes betrachtet würde. Die Teilnetze könnten sowohl gegen Angriffe von außen – aus dem Internet – als auch untereinander abgeschottet werden.



Der Preis: Ein hoher Aufwand

Da gestaffelte Lösungen besser als ausschließlich zentrale Firewalls die Anforderungen der Benutzer abbilden können, ist auch die Gefahr der Umgehung der kontrollierten Schnittstellen durch Schaffung "wilder" Internetzugänge geringer. Zudem würden sich die Folgen derartiger Verstöße gegen die festgelegte Sicherheitsstrategie besser isolieren lassen.
Auch gestaffelte Firewalls sind mit einem insgesamt hohen Administrations- und Pflegeaufwand verbunden, der jedoch auf den zentralen Firewall und die Firewalls der jeweiligen Bereiche verteilt ist. Die Festlegung der individuellen Benutzerrechte kann dabei im wesentlichen den dezentralen, anwendernäheren Firewalls zugeordnet werden.

Erhöhte Anforderungen an Systembetreuer

Firewall-Konzepte entlasten die zentralen und dezentralen Verwalter von vernetzten Systemen nicht von ihrer Verantwortung zur Gewährleistung des Datenschutzes; vielmehr erhöhen sich mit der Vernetzung die Anforderungen an die lokale Systemverwaltung und damit an die Qualifikation der damit betrauten Personen, da Administrationsfehler ungleich schwerwiegendere Konsequenzen haben könnten als bei stand-alone betriebenen Rechnern.

Literatur

Quellen zum Datenschutz

Bauer F. L.: Kryptologie, Springer, Berlin 1994

Braun, C : Unix-Systemsicherheit, Addison Wesley 1993

BSI, IT-Grundschutzhandbuch, Maßnahmenempfehlungen für den mittleren Schutzbedarf, Band 3, Bundesanzeiger Verlag, Bonn 1995

CERT Advisory 95:1: IP Spoofing Attacks and Hijacked Terminal Connections, Pittsburg, 23. Januar 1995

CERT Advisory 95:05: Sendmail Vulnerabilities, Pittsburg, 22. Februar 1995

Cheswick W. R./Belovin S. M.: Firewalls and Internet Security, Addison Wesley 1994

Collardin, M.: Straftaten im Internet, Fragen zum internationalen Strafrecht, Computer & Recht 10/95

Datenschutzberater: Kryptographie: Diskussion der Datenschutzbeauftragten, DSB 14. 6.95

Ellermann U.: Netzabsicherung durch Firewalls, Tagungsband 4. Deutscher IT-Sicherheitskongreß, Bad Godesberg 1995

Fuhrberg, K.: Sicherheit auf der Datenautobahn, Tagungsband 4. Deutscher IT-Sicherheitskongreß, Bad Godesberg 1995

Fuhrberg, K.: Internet-Firewalls: Maßnahmenempfehlungen des mittleren Schutzbedarfs für eine Anbindung an das Internet, Bundesamt für die Sicherheit in der Informationstechnik , Bonn Entwurf Stand: 02.10.95

Heuser A.: Verschlüsselungssysteme: Bedrohungen und Anforderungen, Tagungsband 4. Deutscher IT-Sicherheitskongreß, Bad Godesberg 1995

King M.: International Approach to Cryptography, Tagungsband 4. Deutscher IT-Sicherheitskongreß, Bad Godesberg 1995

Killmann W.: Sicherheitsmanagement kryptographischer Mechanismen in lokalen Netzen, Tagungsband 4. Deutscher IT-Sicherheitskongreß, Bad Godesberg 1995

Klau P.: Das Internet – Weltweit vernetzt, IWI-Verlag München, 1994

Koritnik, A.: Firewalls für's Internet – Alle Schotten dicht?, Zeitschrift KES 3/95

Lux, H.: Der Internet–Markt in Deutschland. Provider und Diensdeister, ständig aktualisiert im Internet unter:
http//:www.dpunkt.de/produkte/Internet-Markt.html

Rihaczek K.: Der elektronische Beweis – die Lücke bei der Umsetzung von Technik zum Rechtsgebrauch, Datenschutz und Datensicherung 3/94

Schneider, G.: Eine Einführung in das Internet, Informatik-Spektrum, Springer 18/95

Hersteller von Firewall-Produkten im Internet unter:
http://www.access.digex.net/bdboyle/firewall.vendor.html