

Firewall und Datenschutz – Grundlegende Betrachtungen

zusammengestellt von Mag. Georg Strauss

Firewall-Systeme

Unter einer Firewall („Brandschutzmauer“) wird eine Schwelle zwischen zwei Netzen verstanden, die erst überwunden werden muss, um Rechner im jeweils anderen Netz zu erreichen. Die Firewall hat die Aufgabe, nur zugelassene netzübergreifende Aktivitäten zu ermöglichen und Missbrauchsversuche frühzeitig zu erkennen. Firewall-Lösungen sind auch geeignet, „grenzüberschreitende“ Aktivitäten interner Nutzer zu überprüfen. Firewall-Systeme weisen folgende Charakteristika auf:

- Die Firewall ist definierte und kontrollierte Schnittstelle zwischen dem zu schützenden und dem nicht vertrauenswürdigen Netz.
- Im durch Firewall geschützten Netz wird ein einheitliches Sicherheitsniveau gewährleistet.
- Die Anforderungen aller vernetzten Stellen werden in einer „**Security Policy**“ (Sicherheitspolitik) definiert.
- Die Benutzerprofile der internen Teilnehmer, die mit Rechnern in externen Netzen kommunizieren dürfen, werden auf der Firewall abgebildet und jeweils kontrolliert.
- Die Stärke der Firewall hängt wesentlich von der eingesetzten Technik und ihrer korrekten Administration ab. Für die Sicherheit sind aber auch die Staffelung und die organisatorische Einbindung der Firewall in die IT-Infrastruktur entscheidend.

Datenschutz

Nach allgemeinem Datenschutzrecht tragen Daten verarbeitende Stellen für die Sicherheit ihrer gespeicherten Daten die Verantwortung. Spezifische Rechtsvorschriften für Firewall-Dienste finden sich im Telekommunikations-, Tele- und Mediendiensterecht.

Ein Firewall-Betreiber hat üblicherweise folgende Aufgaben zu erfüllen:

- Er hat den ordnungsgemäßen und zugelassenen Netzverkehr zu sichern,
- unzulässige bzw. rechtswidrige Nutzung abzuwehren (Hacking von außen, unerlaubte Nutzung von innen),
- Angriffe von außen abzuwehren (eingeschleuste Viren abfangen) und
- revisionsfähige Abrechnungen von Leistungen für die Nutzer zu erstellen.

Üblicherweise werden mit der Firewall neben der reinen Transportsteuerung auch andere Dienste angeboten, z.B. ein DNS-Dienst, Proxy Server und zentrale Virenkontrollen. Die technische Ebene der Netze wird in diesen Fällen rechtlich überlagert von der Diensteebene, die den Transport in definierten Transportbehältern regelt. Für die individuelle Nutzung solcher Dienste gelten:

- das **Teledienstegesetz (TDG)**, das einheitliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der elektronischen Informations- und Kommunikationsdienste schafft, und
- das **Teledienstedatenschutzgesetz (TDDSG)**, das die Datenschutzvorschriften für den Betrieb von Telediensten enthält.

Technikfolgenabschätzung

Ziel einer Technikfolgenabschätzung ist es, die Beherrschbarkeit neuer Informations- und Kommunikationsverfahren vor deren Einführung zu überprüfen. Mit ihr werden die Abläufe der automatisierten Datenverarbeitung transparent gemacht, Gefahren für die Rechte der betroffenen Bürgerinnen und Bürger aufgezeigt, Risiken abgeschätzt und Sicherungskonzepte entworfen.

Die Methodik ist auch geeignet, Lösungen für einen datenschutzgerechten Technikeinsatz zu finden. Verantwortliche in Wirtschaft und Verwaltung sollten vor einem Anschluss ihrer internen Netze an fremde Netze eine solche Technikfolgenabschätzungen durchführen.

Die Datenschutzrichtlinie der Europäischen Union verpflichtet auch die Wirtschaft, bei Einführung von neuen automatisierten Verfahren „Vorabkontrollen“ durchzuführen, die die spezifischen Risiken für die Rechte und Freiheiten der betroffenen Personen untersuchen.

Bei der Beurteilung der Frage, ob ein Anschluss fremder Netze erforderlich ist, sollte ein strenger Maßstab anzulegen. Auch wenn die Erforderlichkeit bejaht wird, ist zu prüfen, ob der Verwendungszweck nicht schon durch den Anschluss eines isolierten Rechners erreicht werden kann.

Die Art des Zugangs hängt wesentlich davon ab, welche Dienste im Netzverbund genutzt werden sollen. Die Kommunikationsanforderungen müssen auf Grund der unterschiedlichen Aufgaben sowohl für den zentralen Zugang zu fremden Netzen als auch für jeden einzelnen Rechner analysiert werden. Ausgangspunkte einer Technikfolgenabschätzung sind der Schutzbedarf der zu verarbeitenden Daten, die Sicherungsziele der Stelle und die Risiken der unterschiedlichen Dienste.

Vor der Entscheidung über den Anschluss an das Internet sollten in einer Technikfolgenabschätzung folgende Fragen beantwortet werden:

- Welche Datenpakete dürfen auf der Grundlage welchen Protokolls bis zu welchem Rechner im Netz weitergeleitet werden?
- Welche Informationen sollen nicht nach außen gelangen?
- Wie können z.B. die interne Netzstruktur und Benutzernamen nach außen unsichtbar gemacht werden?
- Welche Authentisierungsverfahren sollen benutzt werden; sind benutzerspezifische Authentisierungsverfahren notwendig?
- Welche Zugänge werden benötigt (z.B. nur über einen Internet-Service-Provider)?
- Welche Datenmengen werden voraussichtlich übertragen?
- 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?
- Welche Aktivitäten im Netz sollen protokolliert werden? (Dabei werden ggf. Fragen des Arbeitnehmerdatenschutzes tangiert)
- 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)?
- Welcher Schaden kann im zu schützenden Netz verursacht werden, wenn Unberechtigte Zugang erhalten?
- Welche Restrisiken verbleiben, wenn die vorgesehenen Schutzmaßnahmen realisiert wurden?

Ergibt die Untersuchung ein unvertretbares Restrisiko, muss auf einen Anschluss des jeweiligen Netzes an das Internet bzw. sonstige unsichere Netze verzichtet werden.

Auswahl, Konfiguration und Wartung von Firewall-Systemen

Wichtig für die Auswahl eines Firewall-Systems ist es, für den zu schützenden Bereich das erforderliche

Schutzniveau zu definieren. Drei Lösungsvarianten sind anzutreffen:

1. hohes Schutzniveau im internen Netz orientiert am höchsten vorhandenen Schutzbedarf;
2. niedriges Schutzniveau orientiert an Verfahren mit geringem oder mittlerem Schutzbedarf und
3. mittleres Schutzniveau mit zusätzlichen Maßnahmen für einzelne Netzkomponenten mit höherem Schutzbedarf.

Die Varianten 1 und 2 entsprechen am ehesten zentralen Firewall-Lösungen. Die Variante 2 ist jedoch indiskutabel und mit dem Datenschutzrecht unvereinbar. Variante 3 entspricht einem System gestaffelter Firewall. Neben einer zentralen Firewall, die das innere Netzwerk nach außen sichert, werden Netze mit höherem Schutzbedarf durch weitere Firewall abgesichert. Gestaffelte Firewall-Systeme können selbst bei einheitlich

hohem Schutzniveau im Gesamtnetz sinnvoll sein, um mögliche Schäden auf einzelne Netzsegmente zu begrenzen.

Firewall-Systeme müssen transparent und einfach aufgebaut sein. Mit zunehmender Komplexität steigt die Wahrscheinlichkeit von Fehlern. Daher sollten alle nicht für den Betrieb der Firewall benötigte Anwendungen und Systemprogramme gelöscht werden. Bedienung und Konfiguration der Firewall müssen benutzungsfreundlich sein, da sonst unbeabsichtigte Fehleinstellungen zu besorgen sind. Außerdem sollten „**black boxes**“ vermieden werden. Vertrauenswürdige Systeme müssen ihre Funktionsweise offenlegen, denn nur dann ist es Experten möglich, Hintertüren zu verschließen und die Gefahr von Sicherheitslücken fundiert zu bewerten.

Bei der Anschaffung von Firewall-Systemen sollte man nicht die allerneuesten Produkte auswählen, da diese noch „Kinderkrankheiten“ und unerkannte Sicherheitsschwächen haben können.

Statt dessen ist ein gut untersuchtes und zertifiziertes Produkt zu bevorzugen, bei dem zum einen die Stabilität gewährleistet ist und zum anderen etwaige Mängel ausgeräumt werden können. Durch den Einsatz verschiedener Produkte, die unabhängig voneinander entwickelt wurden und arbeiten, lässt sich das Sicherheitsniveau steigern. „Monokulturen“ sollten vermieden werden, denn wenn ein Angreifer einen bisher unentdeckten Fehler ausnutzt, kann leicht der gesamte Schutzwall zusammenbrechen.

Bei der Konfiguration einer Firewall folgt man am besten der Regel:

„Alles, was nicht ausdrücklich erlaubt ist, ist verboten.“

Dies trägt zur Übersichtlichkeit und Sicherheit bei. Wenn man bei der Definition der Regeln etwas übersehen hat, wird nur die Funktionalität und nicht die Sicherheit eingeschränkt. Während man eine Einschränkung der Funktionalität im Bedarfsfall schnell merkt, bleiben Einbußen in der Sicherheit oft unerkannt. Sicherlich gibt es keine 100%ige Sicherheit. Meist erhöht sich im Laufe der Zeit das Missbrauchsrisiko, z.B. durch Bekanntwerden von Schwachstellen, Herausbilden neuer Angriffsformen oder auch durch Verbessern der Systemausstattung von Angreifern. Daher sollten Administratoren ständig die Diskussion um Sicherheitslücken verfolgen und das Sicherheitsniveau regelmäßig neu bewerten, damit die Sicherung dem Stand der Technik entspricht.

Firewall-Checkliste

Die folgende Checkliste ermöglicht eine Selbstkontrolle einer installierten Firewall. Sie konzentriert sich auf die Gesichtspunkte des technisch-organisatorischen Datenschutzes.

Die Checkliste unterteilt folgende Bereiche:

- Angriffe auf das Firewall-System,
- Angriffe aus dem Internet auf das gesicherte Netz sowie
- zusätzliche Sicherungsmaßnahmen.

Zur Durchführung der Selbstkontrolle Ihrer Firewall sollten sie folgende Informationen und Unterlagen zusammentragen und auswerten:

Informationen und Unterlagen	Bemerkungen
Bestandsaufnahme aller Systeme Modem, PC, Server, Router, Bridge, Anwender-Software	
Netztopologie Verbindungen der Rechner untereinander, Zugangspunkte zu fremden Netzen und Systemen	
Dokumentation des Betriebssystems Keine Systemdienste, keine Standardbenutzer, kein Routing	
Dokumentation über die Firewall-Software Funktionseinstellungen, Rechte je Nutzer, Authentisierung, Referenzen, Firewallzertifizierung	
Dokumentation über die Administrierung Oberfläche, Gliederung, Funktionskennzeichnung, Art der Kontrollabfragen, Schutz vor Fehlbedienung, Art und Umfang der Inanspruchnahme der Dienste	
Dokumentation über die Netzintegration Firewall als Gateway, Nebenzugänge, Fax-/Modem-/Mailserver	
Dokumentation der Verantwortlichkeiten (Systemverwalter, Netzadministrator)	
Schwachstellenanalyse Selbst erstellt oder Berichte über Sicherheitslücken	
Dokumentation über Reaktionsszenarien für Angriffe im Bereich des Systems, der Benutzer, der Administratoren	
Art und Umfang der Wartungsverträge (ggf. beifügen)	

Sicherheitsrisiken im Internet

Protokollimmanente Sicherheitsrisiken

Sowohl die Nutzerkennung als auch das Passwort werden bei Internet-Diensten im Klartext über das lokale Netz (z.B. Ethernet) und über das Internet übertragen. Mit Programmen, die unter der Bezeichnung LAN-Analyzer bekannt sind (wie z.B. Packet Sniffer), kann der Datenverkehr im Netz bzw. auf den Netzknoten belauscht und nach interessanten Informationen durchsucht werden. So können diese Abhörprogramme zahlreiche Nutzerkennungen mit den zugehörigen Passwörtern ausspähen, mit deren Hilfe sich ein Angreifer einen unberechtigten Zugriff auf andere Rechner verschaffen kann.

Gegenmaßnahmen:

Verschlüsselung der Daten

Datenpakete können nicht nur abgehört, sondern auch manipuliert werden, z.B. lassen sich die IP-Adressen von Sender und Empfänger fälschen, die TCP Sequence Number von Paketen kann häufig vorhergesagt werden, und der Übertragungsweg ist bei dynamischem Routing modifizierbar. 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 autorisierten Nutzers mitschneiden und später wiedereinspielen (Replay Attack), wodurch sich der Angreifer bei vielen Diensten die Rechte des Nutzers verschafft (z.B. beim Festplattenzugriff über NFS (Network File System)).

Gegenmaßnahmen:

Gegen eine unerkannte Manipulation von Nachrichten können digitale Signaturen eingesetzt werden. Für starke Authentisierung eignen sich Einmalpasswörter oder Challenge-Response-Systeme gegen Replay Attacks.

Für Router sollte nach Möglichkeit statisches Routing konfiguriert werden. Außerdem sollte das „Source Routing“ abgestellt sein.

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 (IP-Spoofing) ans fremde Rechnersystem schickt. Sofern das System die IP-Adresse für vertrauenswürdig hält, wird dem Eindringling ein Zugang, unter Umständen sogar mit unbeschränkter Administratorberechtigung, gewährt.

Gegenmaßnahmen:

*Konfiguration eines Packet Filters, so dass alle Pakete mit ungültigen IP-Adressen *) und mit offensichtlich gefälschten IP-Adressen (z.B. IP-Pakete von außen mit internen Adressen) verworfen werden und nicht ins System gelangen können. Hierbei sollte man ebenfalls verhindern, dass IP-Pakete mit ungültigen Adressen das eigene System verlassen können. **)*

**) definiert im RFC 1597*

****) Weitere Hinweise: RFC 2267 (Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing)*

Angriffe mit gefälschten Paketen von ARP (Address Resolution Protocol) oder ICMP (Internet Control Message Protocols) basieren ebenfalls darauf, dass sich Rechner allein durch ihre IP-Adresse als legitimer Absender ausgeben können. So kann ein Angreifer bei einem Missbrauch von ARP die IP-Adresse eines anderen Benutzers in einem lokalen Netz übernehmen und damit selbst Verbindungen herstellen oder die Erreichbarkeit des anderen Rechners vollständig verhindern. Auch Firewalls, die aufgrund von IP-Adressen entscheiden, ob eine Verbindung zulässig ist, lassen sich dadurch täuschen. Bei ICMP-Angriffen werden gefälschte Statusmeldungen verschickt,

die beispielsweise eine Umleitung der Pakete über einen Router des Angreifers bewirken oder die gesamte Kommunikation eines Rechners nach außen verhindern (Denial of Service Attack).

Der „Ping of Death“ ist ein besonderer ICMP-Angriff, bei dem zu große Pakete beim Empfänger einen Überlauf des Empfangspuffers verursachen und den Rechner zum Absturz bringen.

Ein ähnlicher Effekt wird bei vielen Windows-Rechnern durch das Senden spezieller Pakete (Out-of-Band (OOB)) bevorzugt auf den Port 139 erreicht. Gegen diesen Winnuke-Angriff können einige Windows-Versionen durch Patches geschützt werden.

Gegenmaßnahmen:

Installation von Patches, starke Authentisierung.

Durch den „TCP Syn Flood“-Angriff können ebenfalls Rechner blockiert werden. Dabei wird ein WWW-Server mit Anmeldeversuchen, die einseitig abgebrochen werden, penetriert und über einen längeren Zeitraum lahmgelegt.

Gegenmaßnahmen:

Installation von Patches.

Dienstespezifische Sicherheitsrisiken

E-Mail und Usenet-News

Private Nachrichten (E-Mails) können mitgelesen werden, sofern sie nicht verschlüsselt sind. E-Mails und News-Artikel ohne eine digitale Signatur lassen sich leicht verändern oder fälschen. Über den elektronischen Postweg können - wie bei einem Transfer per Diskette - Programme und Textdokumente mit Viren ins System gelangen. Selbst ein automatisches Durchsuchen der Nachrichten nach Viren bietet keinen vollständigen Schutz.

Gegenmaßnahmen:

Verschlüsselung und digitale Signatur, Virenschutzsysteme.

Sendmail, das auf UNIX-Rechnern am häufigsten eingesetzte Programm zum Verschicken elektronischer Post, weist eine ganze Reihe von Sicherheitslücken auf, die zu einer Zugangsmöglichkeit mit Administratorrechten führen können.

Gegenmaßnahmen:

Installation von Patches, Verfolgen der Meldungen neuer sicherheitsrelevanter Fehler.

Telnet

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

Gegenmaßnahmen:

Einschränkung der Telnet- und verwandten Dienste auf die notwendigen Adressen und Ports an einer Firewall.

Mit Hilfe verschiedener Programme (wie z.B. das Cracker-Tool „Juggernaut“) können mittlerweile Telnet-Verbindungen „entführt“ werden, d.h. der Angreifer kann damit nicht nur Passwörter mitlesen, sondern auch in die Verbindung eingreifen, den ursprünglichen

Benutzer abhängen und statt dessen sich selbst einklinken. Ähnliche Sicherheitsrisiken bestehen für „R-Utilities“ wie rlogin.

Gegenmaßnahmen:

Vollständiger Verzicht auf den Telnet-Dienst sowie auf rlogin, rsh und rcp, statt dessen Verwendung von SSH (Secure Shell), wodurch mit anerkannten kryptographischen Verfahren eine zuverlässige gegenseitige Authentisierung und eine transparente Verschlüsselung des gesamten Datenstroms erreicht wird. Das SSH-Paket steht für alle gängigen Betriebssysteme zur Verfügung.

FTP

Schlecht gewartete FTP-Server stellen ein Risiko dar, da in älteren Versionen bestimmter FTP-Server (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 anonym eigene Dateien in Verzeichnissen ablegen können, wo andere sie sich holen können, kann sich der FTP-Server schnell zu einem Umschlagplatz von Raubkopien entwickeln.

Gegenmaßnahmen:

Am besten ebenso wie bei Telnet Ersatz des FTP-Dienstes (incl. rcp) durch Programme aus dem SSH-Paket (scp), Beschränkung durch Vergabe von entsprechenden Zugriffsrechten.

WWW

Gefährdungen entstehen bei WWW-Servern durch fehlerhafte Software oder Konfigurationen. Ohne den Einsatz von SSL (Secure Socket Layer) oder anderen Verschlüsselungen lässt sich die Kommunikation abhören. Außerdem können Skripte zur dynamischen Generierung von Dokumenten Sicherheitslücken aufweisen.

Ende 1996 wurde die Angriffsmethode Web-Spoofing bekannt, bei dem ein Angreifer seinen Server zwischen das eigentliche Zielsystem und den Rechner des Benutzers schaltet. Der Angreifer erstellt auf seinem System eine täuschend echte Kopie der Daten, die er komplett kontrollieren und für seine Belange modifizieren kann. Danach hat er nach Belieben die Möglichkeit, vom Benutzer verschickte Informationen abzufangen oder zu manipulieren.

Gegenmaßnahmen:

Verschlüsselung und digitale Signatur für die Kommunikation, Zertifikate für Web-Server, gegenseitige Authentisierung von Nutzer und Web-Server.

DNS

Auch beim Domain Name Service (DNS) gibt es mittlerweile die Angriffsmethode des Spoofing. Mit gefälschten Informationen im DNS können Datenströme in beliebige Bahnen gelenkt werden, wenn der Benutzer statt der numerischen IP-Adresse den leichter zu merkenden Rechnernamen angibt.

Gegenmaßnahmen:

Adressierung durch die numerische IP-Adresse; Einsatz eigener Domain Name Server

Finger

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. Berühmt 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 (Buffer Overflow Bug). Bei geschickter Wahl der übergebenen Zeichenreihe kann so beliebiger Code zur Ausführung kommen. Ähnliche Programmierfehler finden sich auch heute noch in vielen anderen Serverprogrammen.

Gegenmaßnahmen:

*Abschalten der Dienste, über die sich Angreifer sicherheitsrelevante Informationen aus dem System beschaffen können: finger, rcp, rusers, rwho, SMTP EXPN, SMTP VRFY.
Installation von Patches gegen den Buffer Overflow Bug.*

SNMP

Mit Hilfe des Simple Network Management Protocol-Dienstes können Netzwerkkomponenten von zentraler Stelle aus verwaltet werden. Dazu können Informationen über die Konfiguration und den Betriebszustand der Komponenten abgefragt und verändert werden. Dies bietet dem Angreifer u. U. wertvolle Hinweise über die eingesetzte Hard- und Software, die für weitergehende Attacken ausgenutzt werden können. Besondere Bedeutung kommt dabei den sog. Community Strings zu, die eine einfache Form der Authentisierung bei SNMP darstellen. Häufig ist bei Auslieferung der Community String „public“ eingestellt, der einen unberechtigten Zugriff auf den Dienst sehr erleichtert.

Gegenmaßnahmen:

*Verwendung schwer zu erratender Community Strings, jedenfalls nicht „ public“
Begrenzung der von SNMP zur Verfügung gestellten Informationen auf das Erforderliche*

Sicherheitsrisiken durch aktive Elemente

ActiveX

ActiveX steht für eine Reihe von Technologien, die dafür sorgen, dass Windows Anwendungen mit dem Internet oder Intranet zusammenarbeiten. WWW-Seiten können mit dieser Technologie um eine Vielzahl von multimedialen Effekten, unterschiedlichen Layouts und ausführbaren Applikationen, die über das Internet geladen werden, erweitert werden. Die Technologie besteht im Wesentlichen aus folgenden Elementen: ActiveX-Controls, Active Documents und Active Scripting.

ActiveX-Controls sind Programme, die auf einer WWW-Seite dargestellt oder als eigene Programme aufgerufen werden können. Active Documents ermöglicht die Anzeige und Betrachtung von Nicht- HTML-Dokumenten (z.B. Word oder Excel) innerhalb eines Browsers. ActiveX Scripting ermöglicht das Verwalten und die Kommunikation von ActiveX-Controls, beinhaltet einen Java-Compiler und ist eine Umgebung zur serverseitigen Nutzung von ActiveX-Controls.

Eine ActiveX- Sicherheitsarchitektur gibt es nicht. Die vorhandenen Sicherheitsmechanismen bieten kein in sich konsistentes Sicherheitssystem. Microsoft setzt auf die Nachvollziehbarkeit der Herkunft der heruntergeladenen Codes durch Codesignierung. Für die Codesignierung setzt Microsoft die selbstentwickelte Authenticode Technologie ein. Sie beruht auf einer digitalen Signatur und erlaubt neben der sicheren Identifikation des Absenders den Nachweis der Echtheit der übertragenen Codes. Dieses Verfahren macht aber keine Aussage über die Funktionsweise der Software selbst und ob sie gewollt oder ungewollt (Programmierfehler) schadensstiftende Wirkung entfalten kann. Microsoft arbeitet mit der Firma Verisign als Zertifizierungsstelle zusammen und vergibt zwei unterschiedliche Zertifikate: Individualzertifikate und kommerzielle Zertifikate. Es existiert ein mehrstufiges Sicherheitssystem im Zusammenspiel von ActiveX und den unterschiedlichen Browsern. Neben der Möglichkeit, die ActiveX-Funktionalität (gilt für alle Browser) abzuschalten, besteht auch die Option, im Internet-Explorer einen Sicherheitslevel (hoch, mittel und niedrig) vorzugeben. Bei einem hohen Sicherheitslevel werden nur zertifizierte ActiveX-Controls akzeptiert. Bei einem mittleren Level müssen nicht zertifizierte ActiveX-Controls explizit freigegeben

werden. Ein niedriger Level bietet gar keinen Schutz. Eine weitere Möglichkeit, sich zu schützen, bieten ActiveX-Filter, die Listen mit Servern definieren, von denen ActiveX-Komponenten akzeptiert werden. Der Einsatz des Internet-Explorer-Administration-Kit (IE-AK) ermöglicht die Erstellung von spezifisch angepassten Internet-Explorern.

ActiveX-Komponenten stellen, da sie keinerlei Einschränkungen bzgl. der Windows- und System-Funktionalität unterliegen, ein immenses Sicherheitsrisiko dar. Folgende Sicherheitsrisiken sind bisher bekannt: Ausforschung von Nutzern und Computersystemen, Installieren und Ausführen von Viren und Trojanischen Pferden, Beschädigung von Systemressourcen und Überlasten des Systems.

Gegenmaßnahmen:

Abschalten der ActiveX-Unterstützung, Verwendung des Microsoft-Authenticodes, Aktivieren einer Hohen Sicherheitsstufe im Internet-Explorer, Einsatz von ActiveX-Filtern und des Internet-Explorer-Administration-Kits in Netzwerken.

Als Letztes sei noch auf die unzureichenden Sicherheitsmechanismen der Betriebssystemplattformen hingewiesen. Die Plattform Windows 95 verfügt über keinerlei eingebaute Sicherheitsmechanismen zur Abwehr von Angriffen, und unter Windows NT laufen ActiveX-Controls im Rechneraum (mit den Zugriffsrechten) des gerade angemeldeten Benutzers.

Java

Java ist eine objektorientierte Programmiersprache, die unabhängig von der jeweiligen Systemplattform nutzbar ist. Sie wurde von Sun Microsystems entwickelt. Java bietet die Möglichkeit, Stand-Alone-Anwendungen (Java-Applikationen) sowie Anwendungen für das WWW (Java-Applets) zu schreiben. Java-Applets können in HTML-Seiten integriert, über das Internet angefordert und auf beliebigen Rechnern ausgeführt werden, ohne dass der Entwickler die lokale Umgebung des Anwenders kennen muss. Einzige Bedingung für die Lauffähigkeit ist die Verfügbarkeit der JVM (virtuelle Java Maschine) auf der Plattform. Java verfügt über ein integriertes Sicherheitssystem. Das Sandbox-System ist mehrstufig bezogen auf die vier Softwareebenen, die bei der Herstellung und Ausführung von Java-Funktionen beteiligt sind :

- Programmiersprache Java,
- Virtuelle Java Maschine,
- Lader für Java-Klassen und
- Java Bibliotheken.

Ist JVM Bestandteil des HTML-Viewers, werden Applets ausgeführt, die sehr strengen Sicherheitskontrollen unterliegen. Applets, die über das Netz geladen werden, haben auf dem Client keine Lese- und Schreibrechte, können keine fremden Programme starten, können keine Systemfunktionen

aufrufen und können keine Netzwerkverbindung zu anderen Rechnern aufbauen. Applets können im Standardfall nur definierte Systemeigenschaften lesen (z.B. Windows NT).

Sun bietet in neueren Versionen die Möglichkeit mit signierten Applets zu arbeiten. Die Applets werden zertifiziert und mit einer digitalen Signatur versehen, bevor sie im Netz zur Verfügung gestellt werden. Somit kann der Client die Authentifikation und die Herkunft prüfen. Die Signierung

sagt nichts über die Funktionalität des Programmes. Java bietet mit seinen durchdachten Mechanismen eine ausreichende Sicherheit, aber durch Implementierungsfehler wurden Angriffe durch Java-Applets möglich. Hier muss man unterscheiden zwischen Angriffen, die das System und seine Ressourcen modifizieren (durch Programmier- und Implementationsfehlern in den Ablaufumgebungen) oder die eine weitere Nutzung des Systems verhindern (Überlasten des Systems) oder die Nutzer ausforschen oder belästigen. Es bieten sich mehrere Optionen an, um sich vor Angriffen zu schützen. Zusätzlich zu dem eigenen Sicherheitssystem kann im Browser die Java-Funktionalität abschalten. Einen weiteren Schutz bieten Java-Filter, die Listen mit Servern definieren, von denen Java-Applets akzeptiert werden. In neueren Browser-Versionen ist das Arbeiten mit signierten Applets möglich.

Gegenmaßnahmen:

Abschalten der Java-Funktionalität, Einsatz von Java-Filtern, Arbeiten mit signierten Applets, saubere Implementation in den Browsern.

JavaScript 6

JavaScript ist eine von der Firma Netscape Communication entwickelte Skriptsprache, die plattformunabhängig ist. Sie wird direkt in die HTML-Seiten eingebettet und über einen Interpreter ausgeführt. Die Motivation für die Entwicklung von JavaScript waren die Unzulänglichkeiten der vorhandenen Techniken (HTML und CGI) für Benutzer-Interaktivitäten. Jede Interaktion musste an den Server gesendet werden, um mit Hilfe des CGI-Programms Plausibilitätsprüfungen durchzuführen.

Durch den Einsatz von JavaScript wurde die Anzahl der notwendigen Verbindungen zum Server drastisch verringert. Dynamisch zur Laufzeit können mit JavaScript beispielsweise Eingaben überprüft oder auch Berechnungen durchgeführt werden. Außerdem lassen sich wichtige Funktionen des Browsers, wie Öffnen und Schließen von Fenstern, Manipulieren von Formularelementen und das Anpassen von Browser-Einstellungen verwirklichen. Ein Zugriff auf Dateisysteme anderer Rechnern ist nicht möglich. Netscape bietet die Möglichkeit, mit zertifizierten JavaScript-Codes zu arbeiten. Es wurden jedoch Sicherheitsprobleme in zwei Bereichen bekannt, zum einen in der Ausforschung von Nutzern und Computersystemen und zum anderen in der Überlastung von Rechnern. Hier muss man unterscheiden zwischen Angriffen, die das System und seine Ressourcen durch Programmierfehler und Implementationsfehler in den Ablaufumgebungen modifizieren oder eine weitere Nutzung des Systems -vorsätzlich erzeugt oder ungewollt durch Programmierfehler- verhindern oder die das Lesen von fremden Nachrichten, Ändern von Nachrichten und Verschicken von Texten ermöglichen. Die meisten Sicherheitslöcher sind implementationsabhängig.

Gegenmaßnahmen:

Arbeiten mit zertifizierten Javascript-Codes oder das Abschalten der JavaScript-Funktionalität, Saubere Implementation in den Browsern.

Plug-Ins

Browser Plug-Ins sind auf dem Client laufende Software Module, die den Funktionsumfang des Browsers erweitern und beispielsweise die Darstellung von Audio- und Videodaten erlauben. Plug-Ins sind plattformabhängig, belegen lokalen Plattenspeicher und müssen vom Benutzer beschafft und installiert werden.

Gegenmaßnahmen:

Schulung der Benutzer, um unbeabsichtigtes Installieren der Software verhindern.

Cookies

Cookies (engl. cookie = Keks) sind kleine Datenmengen, die zusammen mit den eigentlich angeforderten Daten aus dem Internet an den Computer des Benutzers übermittelt werden. Dort werden diese Daten gespeichert und für einen späteren Abruf bereitgehalten. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Benutzers (exakt: des Browsers auf dem Computer, den er verwendet) auf das Internet-Angebot erkennbar, doch die Anwendungsmöglichkeiten gehen weit über diese Feststellung hinaus.

Typischerweise werden Cookies eingesetzt, damit der Nutzer das Angebot des angewählten Webservers auf seine persönliche Belange hin abstimmen kann, bzw. um dem Webserver zu ermöglichen, sich selbsttätig auf die (vermuteten) Bedürfnisse des Nutzers einzustellen. Ein Betreiber von WWW-Diensten kann jedoch aus geeigneten gewählten und eingerichteten Cookies ein Nutzungsprofil erstellen, das vielfältige Auskunft über den Benutzer gibt und ihn so als geeignete Zielperson z.B. für Werbebotschaften identifiziert, die in WWW-Seiten eingeblendet werden. Eine Manipulation des Computers über die Speicherung und Abfrage der Cookie-Daten hinaus ist allerdings nicht möglich.

Problematisch sind Cookies trotz dieses vergleichsweise geringen Gefährdungspotentials für die Computersicherheit aufgrund ihrer geringen Transparenz für den Benutzer. Der Datenaustausch mittels Cookies erfolgt vollkommen im Hintergrund zwischen den beteiligten Computern, ohne dass der Benutzer über Inhalte, Zweck, Umfang, Speicherdauer oder Zugriffsmöglichkeiten auf die Cookie-Daten informiert wird, sofern er keine besonderen Maßnahmen ergreift. Diese Parameter sind innerhalb der Cookies selbst festgelegt und werden somit allein vom Betreiber des WWW-Servers bestimmt; der Internet-Nutzer hat hierauf im normalen Betrieb keinen Einfluss. Es hängt wesentlich von der Initiative des Nutzers und seiner technischen Kenntnis und Ausrüstung ab, ob er Cookies bemerkt und sich ggf. vor ihnen schützen kann.

Gegenmaßnahmen

Konfiguration des Browsers, so dass

- *Cookies nicht oder wenigstens nicht automatisch akzeptiert werden*
- *Cookies, die gespeichert werden sollen, angezeigt werden*
- *Löschen bereits gespeicherter Cookies (z.B. Datei cookies.txt bei Netscape-Browsern)*
- *Einsatz von Cookie-Filtern*