Grundschutz durch Firewall

Orientierungshilfe und Checkliste

Der Landesbeauftragte für den Datenschutz Niedersachsen

Vorbemerkung

Das Internet hat sich zum mächtigsten globalen Informations- und Kommunikationsmedium entwickelt. Für viele erscheint der Anschluss notwendig, um aktuelle Informationen schnell und weiterverarbeitungsfähig zu gewinnen. Wirtschaft und Verwaltung sehen Chancen zum modernen Kunden- bzw. Bürgerservice durch eigene Veröffentlichungen. In der Wirtschaft wird das Internet darüber hinaus als kostengünstiges Übertragungsmedium der internen Kommunikation benutzt; das Standort-LAN wird so zu einem weltweiten Firmennetz erweitert. Nicht immer ausreichend bedacht wird dabei, dass mit dem Zugang zum Internet für jeden Benutzer zahlreiche Gefahren und signifikante Risiken verbunden sind. Schwächen finden sich z.B. in den Datenübertragungsprotokollen sowie in den Installationen der Programme. Sobald ein Computer an ein offenes Datennetz angeschlossen wird, ist er von einer unbekannten Zahl anderer Rechner aus erreichbar. Die gespeicherten Daten werden dadurch ausforschbar, die Vertraulichkeit der gespeicherten Daten und die Kommunikation sind gefährdet.

Die folgende Orientierungshilfe will Verantwortlichen aus Wirtschaft und Verwaltung, die ihre „internen" Netze an fremde, unsichere Netze anschließen wollen, deutlich machen , welche Gefahren für die Sicherheit ihrer Datenverarbeitung bestehen. Die Orientierungshilfe zeigt insbesondere Sicherheitsrisiken im Internet auf und beschreibt, wie man die Netzübergänge zwischen geschütztem LAN und unkontrollierbaren Bereichen durch Firewall sichern kann. Die Orientierungshilfe beschreibt unterschiedliche Firewall-Architekturen und gibt Empfehlungen zur Auswahl, Konfiguration und Wartung. Mit dem Betreiben eines Firewall-Systems sind viele Fragen in rechtlicher, technischer und organisatorischer Hinsicht verbunden. Sie zu erkennen und zu beantworten, ist Aufgabe der beigefügten Checkliste für den datenschutzgerechten Einsatz von Firewall-Systemen.

Zusammenschluss fremder Netze

Für den Zusammenschluss fremder Netze (z.B. LAN an das Internet) findet man häufig folgende technische Lösungen:

- Direktanschluss eines einzelnen Rechners ans Internet
  Ein einzelner Rechner wird per Modem und Telefonleitung über einen Internet-Provider an das „Netz der Netze" angeschlossen. Die „Insel"-Lösung spielt besonders bei kleinen Behörden und im privaten Bereich eine große Rolle. Bei Angriffsversuchen ist nur der einzelne Rechner gefährdet.

- LAN-Anbindung an ein Intranet
  Hier verfügt das LAN über eine Verbindung zu anderen Netzen des Unternehmens bzw. zu anderen Verwaltungsrechnern in einem Intranet. Bei eventuellen Angriffen besteht sowohl ein Sicherheitsrisiko für den an das Intranet angeschlossenen Rechner als auch für das gesamte LAN.

- Internet-Anschluss über eine zentrale Firewall
  Hier hat der Rechner einen Zugang zum Intranet (z.B. LAN, VLAN seines Unternehmens oder seiner Verwaltung und von dort aus besteht ein einziger zentraler Zugang zum Internet. Eventuelle Angriffe aus dem Internet können an der zentralen Übergangsstelle vom Internet zum Intranet abgefangen werden. Der einzelne Rechner bzw. das ungeschützte LAN bleiben trotz zentraler Firewall aus dem Intranet heraus angreifbar.

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 IuK-Infrastruktur entscheidend.

Datenschutz

Nach allgemeinem Datenschutzrecht tragen Daten verarbeitende Stellen für die Sicherheit ihrer gespeicherten Daten die Verantwortung. Für Stellen der Wirtschaft sind die datenschutzrechtlichen Pflichten im Bundesdatenschutzgesetz (BDSG) und für öffentliche Stellen des Landes Niedersachsen im Niedersächsischen Datenschutzgesetz (NDSG) geregelt. BDSG und NDSG sind allerdings nur Auffangnormen, soweit nicht bereichsspezifische Regelungen vorgehen. Solche spezifischen Rechtsvorschriften für Firewall-Dienste finden sich im Telekommunikations-, Tele- und Mediensdiensterecht.

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.

Die reine Transportsteuerung einer Firewall, die als Dienstleistung für Dritte angeboten wird, ist rechtlich gesehen „geschäftsmäßiges Erbringen von Telekommunikationsdiensten“ im Sinne des § 3 Nr. 5 des Telekommunikationsgesetzes (TKG). Die Leistung muss auf Dauer und auf Wiederholung gerichtet sein. Auf die Absicht zum Gewinnerzielen kommt es nicht an, vielmehr sind Umfang und Dauer des Angebots entscheidend. Anbieter von TK-Diensten haben das Fernmeldegeheimnis zu wahren (§ 85 TKG). Das Fernmeldegeheimnis wird auch als Transportgeheimnis bezeichnet; geheim zu halten sind der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem TK-Vorgang beteiligt ist oder war. Diensteanbieter dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur zum Erbringen der TK-Dienste verwenden. Selbstverständlich haben auch Betreiber von „Corporate Networks“ das Fernmeldegeheimnis zu wahren. Dies gilt in Niedersachsen z.B. für das Informatikzentrum Niedersachsen als TK-Netzbetreiber der Landesverwaltung sowie für Vereine und Verbände, die TK-Netze für ihre Mitglieder betreiben.

Auch Unternehmen und Behörden, die ihren Mitarbeitern Telekommunikationseinrichtungen zur privaten Nutzung gegen Entgelt zur Verfügung stellen, sind geschäftsmäßige TK-Diensteanbieter im Sinne des TKG. In dienstlicher Tätigkeit sind die Mitarbeiter allerdings nicht als Dritte anzusehen. Der Dienstherr kann und sollte den dienstlichen Umgang mit TK-Einrichtungen durch Betriebs- oder

Dienstvereinbarung regeln. Bei Mischformen dienstlicher und privater Nutzung muss er für eine Differenzierung im Umgang mit Protokolldaten sorgen, um das Fernmeldegeheimnis zu wahren. Ist dies technisch nicht möglich, muss der Dienstherr auf ein Monitoring verzichten.

Üblicherweise werden mit der Firewall neben der reinen Transportsteuerung auch andere Dienste angeboten, z.B. ein DNS-Dienst, Proxy Server und zentrale Virenkontrollen. Diese Dienstleistungen sind Teledienste im Sinne des neuen Teledienstерechts. 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.

Unter das Teledienstерecht fallen Dienste wie z.B. Internet-Zugang, elektronische Post, unmoderierte Chatrooms, das Telebanking, elektronische Buchungssysteme, Telespiele, Abrufdienste und auch elektronische Verwaltungsdienstleistungen. Elektronische Dienste, die sich an die Allgemeinheit richten, fallen unter das Medienrecht. Dazu gehören Dienste wie video on demand, Verteildienste mit redaktioneller Gestaltung, Fernsehtext/Radiotext, Push-Dienste, aber auch eigene, gestaltete Homepage mit Informationen von Behörden und Unternehmen. Diese Dienste fallen unter den **Mediendienste-Staatsvertrag (MDStV)**. Dienste, die darüber hinaus den Rundfunkbegriff erfüllen, werden von den Bestimmungen des **Rundfunkstaatsvertrags** erfasst, z.B. pay per channel, pay per view, near video on demand.

Vorabkontrolle (Technikfolgenabschätzung)

Ziel einer Vorabkontrolle 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 Vorabkontrolle durchführen. Für öffentliche Stellen des Landes Niedersachsen ist dies gesetzlich vorgeschrieben. Die Datenschutzrichtlinie der Europäischen Union und das BDSG verpflichten gegebenenfalls 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 Vorabkontrolle 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 Anlehnung an die Empfehlungen des BSI-Grundschutz-Handbuches in einer Vorabkontrolle 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)	

Zur Beantwortung der Checklisten-Fragen wird es in der Regel ausreichen, jeweils anzukreuzen „Erfüllt“, „Nicht erfüllt“, „Trifft nicht zu“. Diese Antworten können sie durch kurze Erläuterungen im Feld Bemerkung ergänzen. Auf diese Weise liegt nach Durcharbeiten der Checkliste eine übersichtliche Aufstellung der noch zu treffenden Maßnahmen vor.

I	Datenschutzrechtliche Anforderungen	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
1.1	**Grundsätzliche Anforderungen an den Betrieb einer Firewall**				
1.1.1	Alle Benutzer werden über die zu speichernden personenbezogenen Daten vorher informiert.				
1.1.2	Benutzer werden über Gefahren und Risiken der Internetnutzung umfassend aufgeklärt.				
1.1.3	Benutzer werden über Art und Umfang notwendiger technischer Kontrollen vorher unterrichtet.				
1.1.4	Kontrollen der Kommunikationsinhalte sind auf dienstliche Nutzungen beschränkt.				
1.1.5	Inhaltskontrollen ankommender Nachrichten werden nur im Auftrag der Empfänger durchgeführt.				
1.1.6	Inhaltskontrollen werden nur im Auftrag bzw. mit Einwilligung der Betroffenen durchgeführt. Sie beschränken sich auf: • automatisierte Kontrollen, • Administrator erhält nur in Ausnahmefällen Kenntnis vom Kontrollvorgang, • Virenkontrolle ist auf fest definierte Pattern beschränkt • Scanning nach frei wählbaren Textstellen ist verboten.				
1.1.7	Die Nutzer werden darüber informiert, wenn Nachrichten ausgefiltert werden.				
1.1.8	Private Adressen werden innerhalb der Firewall-Policy gesperrt.				
1.1.9	Zugriffsversuche auf gesperrte Adressen werden protokolliert und ausgewertet.				
1.1.10	Eine Vollprotokollierung aller erfolgreichen, zulässigen Verbindungen der Firewall ist verboten und wird technisch verhindert. Der Umfang der Protokolle ist auf das Erforderliche minimiert.				
1.1.11	Es werden nur solche Verbindungen oder Verbindungsversuche aufgezeichnet, die einen potentiellen Angriff darstellen., z.B. • Versuche, auf nicht freigegebene IP-Adressen und Portnummern zuzugreifen, • Hinweise auf Portscanner, • aus dem Internet kommenden Datenpakete,				

I	Datenschutzrechtliche Anforderungen	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
	die Adressen interner Rechner tragen oder • Versuche, sich unberechtigt als Systemverwalter an Firewallkomponenten anzumelden.				
1.1.12	Protokolle sind gegen unbefugte Kenntnisnahme gesichert.				
1.1.13	Protokolle werden zum frühestmöglichen Zeitpunkt gelöscht.				
1.1.14	Es ist ausgeschlossen, dass Dritte die Inanspruchnahme von Diensten zur Kenntnis nehmen können.				
1.1.15	Informationen über die Inanspruchnahme verschiedener Dienste werden auch intern nicht ausgewertet und zu Persönlichkeitsprofilen verdichtet.				
1.1.16	Mitbestimmungsgremien und betriebliche / interne Datenschutzbeauftragte werden bei der Festlegung der Protokollierung und bei der Kontrolle einbezogen.				
1.2	**Firewallbetrieb ist nur für dienstliche Zwecke zugelassen**				
1.2.1	Die außerdienstliche Nutzung des Internet-Anschlusses ist ausdrücklich untersagt.				
1.2.2	Der Eingang privater E-Mail von Dritten an Mitarbeiter wird durch Gestaltung der E-Mail-Adressen unterbunden (z.B. *poststelle@organisation*, *abteilung-x@firma-y* statt **vorname.name@organisation**)				
1.3	**Firewallbetrieb ist auch für Benutzung durch Dritte eingerichtet**				
1.3.1	Benutzer werden hinreichend über die Speicherung ihrer personenbezogenen Daten informiert.				
1.3.2	Daten der Nutzer werden ausschließlich zweckgebunden verwendet.				
1.3.3	Eine außerdienstliche Nutzung des Internet-Anschlusses ist auch Mitarbeitern gestattet.				
1.3.4	Die Nutzungsbedingungen können jederzeit elektronisch eingesehen werden.				
1.3.5	Den Nutzern werden anonyme bzw. pseudonyme Nutzungsformen angeboten.				

I	Datenschutzrechtliche Anforderungen	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
1.3.6	Das Fernmeldegeheimnis Dritter wird vom Firewall-Betreiber gewahrt.				
1.3.7	Der Auftraggeber bestimmt Nutzung und Umfang der Inhaltskontrolle.				
1.3.8	Der Auftraggeber bestimmt die technischen und organisatorischen Folgen bei ausgefilterten Nachrichten.				
1.3.9	Dienste werden nicht von einer Einwilligung des Nutzers in die Verarbeitung seiner Daten für andere Zwecke abhängig gemacht.				
1.3.10	Art, Umfang und Abrechnung einer privaten Nutzung des Internet-Anschlusses (E-Mail, WWW) sind in Nutzungsbedingungen klar geregelt.				
1.3.11	Der Eingang privater E-Mail wird durch organisatorische Maßnahmen unterbunden.				
1.3.12	Zwischen privaten und dienstlichen E-Mail-Accounts wird unterschieden (z.B. durch vorname.name@privat.organisation).				
1.3.13	Ggf. Zusatzfrage:				

2	Technische und organisatorische Maßnahmen gegen Angriffe auf das Firewall-System	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
2.1	Die Anmeldung des Administrators erfolgt über eine gesicherte Verbindung (z.B. Konsole in gesicherter Umgebung, verschlüsselte Verbindung, separates Netz,...)				
2.2	Die Anmeldung des Revisors erfolgt über eine gesicherte Verbindung.				
2.3	Vor dem Zugriff sind nicht sichtbare Kennungen für den Administrator und den Revisor vorhanden.				
2.4	Beim Ausfall der Protokollierung wird ein Alarm für den Administrator erzeugt (z.B. Ausfall einer Protokollkomponente, weil Datenträger voll ist)				
2.5	Beim Ausfall der Protokollierung wird die nicht-administrative Nutzung der Firewall verhindert.				
2.6	Die eingesetzten Programme und Dateien werden mindestens einmal täglich auf ihre Integrität geprüft (z.B. durch Prüfsummenkontrolle)				
2.7	Die Prüfprogramme sind auf Datenträgern untergebracht, die hardwareseitig sicherstellen, dass die Programme nicht verändert werden können (z.B. Starten der Programme von CD-ROM)				
2.8	Bei Verlust der Integrität wird die nicht-administrative Nutzung der Firewall automatisch verhindert.				
2.9	Bei einem Systemabsturz wird die nicht-administrative Nutzung der Firewall automatisch verhindert (z.B. Booten in den Singel-User modus)				
2.10	Auf den Firewall-Komponenten wird ausschließlich Software verwendet, die zur Funktionalität der Firewall erforderlich ist.				
2.11	Die eingesetzte Hardware und Software ist vollständig dokumentiert.				
2.12	Die aktuelle Firewall-System-Konfiguration ist vollständig dokumentiert.				
2.13	Ggf. Zusatzfrage:				

3	Technische und organisatorische Maßnahmen gegen Angriffe aus dem Internet auf das gesicherte Netz	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
3.1	**Allgemeine Fragen/Applikationsfilter**				
3.1.1	Die eingesetzten Filter sind so hintereinander angeordnet, dass beide Filter passiert werden müssen (Keine Umgehungsmöglichkeiten vorhanden).				
3.1.2	Die eingesetzten Filter verwenden unterschiedliche Hard- und Software.				
3.1.3	Die Syntax für die Beschreibung der Filterregeln ist unterschiedlich.				
3.1.4	Bei allen Komponenten sind nur diejenigen Verbindungen zugelassen, die explizit erlaubt wurden.				
3.1.5	Bei Ausfall der Firewall sind keine Verbindungen mehr möglich.				
3.1.6	Interne Netzstrukturen, wie Mail-Adressen, IP-Nummern, Rechnernamen etc., werden durch die Firewall versteckt (z.B. durch Einsatz von Applikationsfilter mit zwei DNS Servern).				
3.1.7	Die Firewall ist mit einer übersichtlichen, grafischen Benutzeroberfläche ausgestattet.				
3.1.8	Die Administration der Firewall erfolgt über ein eigenes Teilnetz oder eine verschlüsselte Verbindung.				
3.1.9	Der Verbindungsaufbau auf der Anwendungsschicht ist für jeden einzelnen Dienst durch die Firewall zeitlich und benutzerabhängig geregelt.				
3.1.10	Regelungen über die Authentisierung und Identifikation liegen dokumentiert vor.				
3.1.11	Die Filterregeln innerhalb der einzelnen Komponenten werden auf Konsistenz geprüft.				
3.1.12	Ein Abgleich der Filterregeln zwischen den Komponenten erfolgt.				
3.1.13	Kommende Telnet-Verbindungen werden durch gesonderte Verschlüsselung geschützt.				
3.1.14	Datentransferbefehle der Protokolle werden durch eigene Filterregeln für FTP-retr oder HTTP-post geprüft.				
3.1.15	Regelungen für Datentransferbefehle liegen vor.				

3	Technische und organisatorische Maßnahmen gegen Angriffe aus dem Internet auf das gesicherte Netz	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
3.1.16	Der Zeitraum, in dem ein Datentransfer möglich ist, ist auf das organisatorisch vertretbare Minimum begrenzt.				
3.1.17	Jede aufgebaute oder abgewiesene Verbindung wird protokolliert.				
3.1.18	Das Protokoll enthält alle notwendigen Informationen, wie Benutzer-ID, Datum/Zeit, IP-Adresse Quelle, IP-Adresse, Ziel und Portnummer.				
3.1.19	Aufgrund bestimmter Protokollmeldungen werden Alarme ausgelöst.				
3.1.20	Die Alarmweiterleitung erfolgt unmittelbar an den Administrator oder Vertreter.				
3.1.21	Protokollmeldungen werden gesichert an eine externe Stelle übertragen (z.B. zur zentralen Archivierung).				
3.2.	**Zusätzliche Fragen für Paket-Filter (Ebene 4 IP und TCP, UDP)**				
3.2.1	Jedes Paket wird nach den Filterregeln einzeln auf IP-Quell- und IP-Ziel-Adresse geprüft.				
3.2.2	TCP- und UDP-Verbindungen werden paketweise nach Quell- und Ziel-Port geprüft.				
3.2.3	Die Filterung nach den obigen Regeln erfolgt getrennt für jedes Interface (Adressen aus dem internen Netz dürfen bei ankommenden Paketen nicht vorkommen).				
3.2.4	Bei mehr als zwei Interfaces werden unterschiedliche Regeln für ein- und ausgehende Pakete definiert.				
3.2.5	Die Filterregeln sowie die Reihenfolge der Regeln darf von der Firewall nicht automatisch verändert werden.				
3.2.6	Bei IP-Paketen ist zwischen Verbindungsaufbau oder bestehender Verbindung zu unterscheiden.				
3.2.7	Es wird ausschließlich statisches Routing verwandt.				
3.2.8	Source-Routing Informationen werden verworfen.				
3.2.9	Das Protokoll enthält alle notwendigen Informationen, wie Benutzer-ID, Datum/Zeit, IP-Adresse Quelle, IP-Adress Ziel und Portnummer.				
3.2.10	Ggf. Zusatzfrage:				

4	Zusätzliche Sicherungsmaßnahmen Paketfilterung/Implementation der Regeln	Erfüllt	Nicht erfüllt	Trifft nicht zu	Bemerkung
4.1	Die Firewall fordert für die Länge der IP-Fragmente eine Mindestlänge.				
4.2	Durch den verwendeten Paketfilter wird ein Fragment-Offset größer Null erzwungen.				
4.3	Die Firewall filtert die ICMP Meldungen Destination Unreachable und Redirect.				
4.4	Die DNS-Spoofing Angriffe werden von der Firewall abgewiesen.				
4.5	Zonen-Transfer-Requests eines unbekannten Hosts werden abgewiesen, d.h. mit refused beantwortet.				
4.6	ARP-Tabellen im gesicherten Netz werden fixiert oder das ARP-Protokoll wird an der Firewall komplett abgewiesen.				
4.7	Der automatische ARP Ablauf wird bei Anfragen von außen verhindert.				
4.8	Für einzelne FTP-Befehle ist eine gesonderte Rechteverwaltung eingerichtet.				
4.9	Die mittels FTP übertragenen Daten werden verschlüsselt.				
4.10	Eingehende Telnet Daten werden auf den Port 23 gefiltert.				
4.11	S-HTTP-Daten werden vom HTTP-Proxy abgewiesen.				
4.12	Die Netzobjekte (wie Host, Domain, Subnet, Group, IP-Range, VPN-Objekte) werden für die Filterung definiert.				
4.13	Der Paket-Filter Kontext wird gespeichert.				
4.14	Ggf. Zusatzfrage:				

Beachten Sie bitte:

Eine beantwortete Checkliste deckt möglicherweise vorhandene Sicherheitslücken des Systems auf. Daher sollten Sie die ausgefüllte Checkliste bis zur vollständigen Beseitigung dieser Mängel entsprechend vertraulich behandeln!

Anlage 1

Sicherheitsrisiken im Internet[3]

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 Bezeichung 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 Passworten 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

[3] Akr. Technik, Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

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, rup, 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 (IEAK) 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 Rechteraum (mit den Zugriffsrechten) des gerade angemeldeten Benutzers.

Java

Java ist eine ojektorientierte Programmiersprache, die unabhängig von der jeweiligen Systemplattform nutzbar ist. Sie wurde von Sun Microsystems entwickelt. Java bietet die Möglichkeit, Stand-Alone-Anwendungen (Java-Applikations) 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 HMTL-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[4]

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 geeignet 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 trotzt 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

[4] Forschungsinstitut für anwendungsorientierte Wissensverarbeitung Ulm, Sicherheit für Benutzer der Internet-Technologie

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*

Anlage 2

Firewall-Systeme[5]

Firewall-Technologien

Eine Firewall kann durch verschiedene Konzepte realisiert werden, im Wesentlichen unterscheidet man folgende Grundkonzepte:

- Packet Filter (Packet Screen, Screening Router)
- Application Level Gateway (Dual-homed Gateway)
- Stateful Inspection (Stateful Packet Filter, Dynamic Packet Filter)

Ein **Packet Filter** ist ein Router, der IP-Pakete zur Unterscheidung zwischen der erlaubten und unerlaubten Nutzung von Kommunikationsdiensten filtert. Packet Filter können nach Quell- und Zieladresse sowie nach Quell- und Zielport filtern. Damit ist einschränkbar, welche Rechner im zu schützenden und welche im unsicheren Netz an der Kommunikation beteiligt sein dürfen, sowie welche Kommunikationsdienste erlaubt sind.

Ein **Application Level Gateway** ist ein speziell konfigurierbarer Rechner, über den die gesamte Kommunikation zwischen dem zu schützenden und dem unsicheren Netz stattfindet. Ein Application Level Gateway arbeitet im Gegensatz zum Packet Filter auf der Anwendungsschicht, d.h. die Kontrolle der Kommunikationsbeziehungen findet auf Anwendungsebene statt. Für jeden Dienst (Telnet, FTP usw.) werden Security Proxys eingeführt, die den direkten Zugriff darauf verhindern. Hierbei bestehen z.B. die Möglichkeiten einer ausführlichen Protokollierung (Audit) und einer benutzerbezogenen Authentisierung für die unterschiedlichen Dienste. Die meisten Application Level Gateways sind nicht in der Lage, zu unterscheiden, über welche Netzschnittstelle ein Paket hereinkommt. Ein Application Level Gateway mit zwei Netzschnittstellen wird Dual-homed Gateway genannt.

Die Kombination von Packet Filter und Application Level Gateway wird als **Screened Gateway**, Transparent Application Gateway oder Sandwich-System bezeichnet und erhöht die Sicherheit der Firewall gegenüber den beiden Einzelkomponenten erheblich. Die Anordnung der beteiligten Komponenten kann variieren und erlaubt die individuelle Realisierung eines Firewall-Konzeptes.

Stateful Inspection (auch Stateful Packet Filter oder Dynamic Packet Filter) ist eine recht neue Firewall-Technologie und arbeitet sowohl auf der Netz- als auch auf der Anwendungsschicht. Die IP-Pakete werden auf der Netzschicht entgegengenommen, von einem Analysemodul, das dynamisch im Betriebssystemkern geladen ist, zustandsabhängig inspiziert und gegenüber einer Zustandstabelle abgeglichen. Die Regeln, nach denen das Modul agiert, können sehr differenziert vorgegeben werden. Für die Kommunikationspartner stellt sich eine Firewall mit Stateful Inspection als eine direkte Leitung dar, die nur für eine den Regeln entsprechende Kommunikation durchlässig ist. Im Out-Of-Band-Betrieb erfolgt die Wartung und Konfiguration nicht über TCP/IP. Die Firewall besitzt dann keine eigene IP-Adresse, so dass keine Möglichkeit besteht, sie über TCP/IP direkt aus den angeschlossenen Netzen anzusprechen oder auf diesem Wege anzugreifen. Optional führt die Firewall ein Rewriting durch, d.h. Pakete werden vor dem Weitersenden nach vorgegebenen Regeln transformiert. Stateful Inspection vereinigt bereits konzeptuell die Schutzmöglichkeiten von Packet Filter und Application Level Gateway, so dass diese beiden Funktionen nicht in getrennten Komponenten realisiert werden müssen.

Firewall	Vorteile	Nachteile
Packet Filter	• *leicht realisierbar, da von vielen Routern angeboten*	• *es ist bei den meisten Produkten nicht möglich, Dienste nur für bestimmte Benutzer zuzulassen*

[5] Akr. Technik, Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

Firewall	Vorteile	Nachteile
Router oder Rechner mit spezieller Software	• *leicht erweiterbar für neue Dienste* • *Router auf dem Markt verfügbar* • *Transparenz für den Benutzer* • *Arbeitsgeschwindigkeit*	• *alle Dienste, die erlaubt und erreicht werden können, müssen sicher sein* • *Protokollierung nur auf unteren Netzschichten möglich* • *Keine Authentisierung möglich*
Dual-homed Gateway Application Level Gateway mit zwei Netzschnittstellen	• *kein Paket kann ungefiltert passieren, aussagekräftige Protokollierung auf höheren Schichten möglich* • *interne Netzstruktur wird verborgen durch den Einsatz von Network Address Translation (NAT)*	• *Übernahme des Application Level Gateways durch einen Angreifer führt zu einem vollständigen Verlust der Sicherheit, keine Transparenz für den Benutzer, Probleme bei neuen Diensten, schlechte Skalierbarkeit*
Screened Gateway Anordnung aus Application Level Gateway mit einem oder zwei Packet Filtern (Teilnetz-Bildung)	• *kein direkter Zugang zum Gateway möglich, interne Netzstruktur wird verborgen, Network Address Translation (NAT), vereinfachte Regeln durch 2. Filter, durch Einsatz mehrerer Gateways lässt sich die Verfügbarkeit steigern, aussagekräftige Protokollierung möglich*	• *keine Transparenz für den Benutzer* • *bei Realisation mit mehreren Rechnern und Routern: erhöhter Platzbedarf* • *Probleme bei neuen Diensten, schlechte Skalierbarkeit*
Stateful Inspection Firewall-Rechner mit zustandsabhängiger Analyse und Reaktion	• *gute Skalierbarkeit, arbeitet auf Netz- und Anwendungsschicht* • *Out-Of-Band-Betrieb: keine Angriffsmöglichkeit über TCP/IP* • *interne Netzstruktur wird verborgen* • *Rewriting möglich (über NAT hinaus), umfangreiche Authentisierungsvarianten*	• *keine Zwischenspeicherung, daher nicht volle Gateway-Funktionalität und kein Caching* • *schneller Rechner erforderlich, da wegen der umfangreichen Analyse und Aktionsmöglichkeiten sonst Performance-Einbussen*

Firewall-Architekturen

Neben den im folgenden dargestellten Architekturen von Firewalls sind auch Abwandlungen der Kombinationen der Anordnungen möglich.

Zentrale Firewall

Rein zentrale Firewall-Lösungen sind durch folgende Aspekte charakterisiert:

- Die zentrale Firewall bildet die einzige Schnittstelle (Choke Point) zwischen dem kompletten zu schützenden Verwaltungsnetz und dem übrigen Internet.
- Innerhalb des gesamten Verwaltungsnetzes besteht ein einheitliches Sicherheitsniveau, eine weitere Differenzierung nach Sicherheitsstufen erfolgt nicht.
- Eine Kontrolle der internen Verbindungen durch die Firewall ist nicht möglich.
- Die zentrale Firewall setzt eine definierte Sicherheitspolitik für das gesamte Verwaltungsnetz voraus. Abweichende Sicherheitspolitiken 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.

Da eine zentrale 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 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 gerade von diesen Stellen zusätzli-

che Internet-Zugänge mit geringeren Restriktionen geschaffen werden, wodurch der gesamte Zweck der Firewall ad absurdum geführt wird. Ein weiterer Nachteil zentraler Firewalls besteht in dem – auch aus dem Grossrechnerbereich bekannten – Problem, dass eine Benutzerverwaltung, die fernab von dem jeweiligen Fachbereich erfolgt, häufig zu Abweichungen zwischen der Realität von Benutzerrechten und deren Abbildung in Form von Accounts führt.

Da eine Firewall Zugriffe innerhalb des internen Netzes nicht kontrolliert, 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 restringiert werden. Dieser Aspekt ist zwar nur mittelbar Teil des Themas „Internet-Anbindung", muss bei einer Gesamtbetrachtung von Netzsicherheit jedoch unbedingt einbezogen werden. Der Einsatz einer alleinigen zentralen Firewall ist allenfalls dann vertretbar, wenn alle angeschlossenen Teilnetze über ein gleiches Sicherheitsbedürfnis bzw. -niveau verfügen und zudem nicht die Gefahr des internen Missbrauchs besteht. Davon kann in behördenübergreifenden Verwaltungsnetzen mit einer Vielzahl angeschlossener Rechner jedoch nicht ausgegangen werden.

Gestaffelte Firewall

Gestaffelte Firewall-Lösungen sind durch folgende Aspekte charakterisiert:

- Es handelt sich um eine Kombination zentraler und dezentraler Komponenten, wobei durch eine zentrale 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 Sicherheitpolitik für das Gesamtnetz voraus. Bei ihrer Definition müssen insbesondere die Anforderungen an einen zu garantierenden Grundschutz 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 die zentrale Firewall mit Systemen im Internet in Verbindung zu treten.
- Auch die dezentralen Firewalls müssen qualifiziert administriert werden.

Für die dezentralen Firewalls bieten sich prinzipiell die gleichen Technologien wie bei einer 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 die zentrale Firewall durch einen Eindringling überwunden wurde.
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 können sowohl gegen Angriffe von außen – aus dem Internet – als auch untereinander abgeschottet werden.
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" Internet-Zugänge geringer. Zudem würden sich die Folgen derartiger Verstöße gegen die festgelegte Sicherheitspolitik besser isolieren lassen.
Auch gestaffelte Firewalls sind mit einem insgesamt hohen Administrations- und Pflegeaufwand verbunden, der jedoch auf die zentrale Firewall und die dezentralen Firewalls verteilt ist. Die Festlegung der individuellen Benutzerrechte kann dabei im Wesentlichen den anwendernäheren dezentralen Firewalls zugeordnet werden.

Entmilitarisierte Zone

Server, die Dienste für Internet-Nutzer zur Verfügung stellen wie WWW oder Mail, werden häufig hinter einer Firewall in der sogenannten entmilitarisierten Zone (DMZ, Demilitarized Zone, auch Screened Subnet) eingerichtet, von der das interne Netz durch eine (weitere) Firewall abgeschottet ist. Dies hat den Vorteil, dass das lokale Netz auch dann noch geschützt ist, wenn ein Angreifer bis zum WWW-Server gelangt.
Die entmilitarisierte Zone kann beispielsweise zwischen zwei Firewalls realisiert werden. Durch Verwendung unterschiedlicher Firewall-Produkte lässt sich dabei eine höhere Sicherheit erreichen, da mögliche Fehlfunktionen bei unabhängiger Entwicklung der Produkte wahrscheinlich nicht gleichzeitig auftreten. Allerdings entstehen höhere Kosten für die Anschaffung und Wartung der Systeme, so dass diese Lösung meist nur für größere Netze in Frage kommt.
Die Aufgaben der beiden Firewalls können auch von nur einer Firewall mit mehreren Schnittstellen übernommen werden, mit denen sich mehrere Netze mit unterschiedlicher Sicherheit bilden lassen. So können auch eine oder mehrere entmilitarisierte Zonen eingerichtet werden. Diese Lösung ist kostengünstiger, verzichtet aber auf die erhöhte Sicherheit.

Screened Gateway

Zumeist werden neben der Firewall Router eingesetzt, die oft die Funktion von Packet Filtern übernehmen können. Damit lässt sich eine „Sandwich-Lösung“ realisieren, die durch Verwendung unterschiedlicher Systeme eine erhöhte Sicherheit gewährleisten kann. Auch hier ist die Einrichtung einer entmilitarisierten Zone möglich.

So erreichen Sie den Landesbeauftragten für den Datenschutz Niedersachsen:

Schreiben Postfach 221, 30002 Hannover
Anrufen 0511 / 120-4552
Faxen 0511 / 120-4591
E-Mailen poststelle@lfd.niedersachsen.de
Surfen www.lfd.niedersachsen.de
Persönlich Brühlstraße 9, Hannover