Orientierungshilfe
zu
Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet

erstellt von den
Arbeitskreisen „Technik“ und „Medien“
der
Konferenz der Datenschutzbeauftragten
des Bundes und der Länder

Überarbeitete Fassung vom November 2008

Inhalt

1. Einleitung

Der weltweite Internet-Boom hat auch vor den öffentlichen Verwaltungen nicht Halt gemacht. Beginnend mit der Möglichkeit, das Internet als Informationsmedium für eigene Zwecke zu nutzen bis zu der Notwendigkeit, sich dort mit Informationen und Dienstleistungen zu präsentieren, wird das Thema Internet von der öffentlichen Hand heute nicht wesentlich anders behandelt als von Privaten[1].

Dabei ist der Anschluss an das Internet mit erheblichen Gefährdungen des Datenschutzes und der Datensicherheit verbunden. Die Rechner und Übertragungswege dieses weltweiten Computernetzes sind nicht kontrollierbar. Welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist für den Endnutzer nicht transparent, geschweige denn beeinflussbar. Den damit verbundenen Risiken für Vertraulichkeit, Integrität und Zurechenbarkeit wird vielfach nicht in der gebotenen Weise begegnet. Je stärker die öffentliche Verwaltung auf die Vorteile des Internet setzt, umso mehr schlagen Schwächen in Protokollen, Software und Design auf eigene Netze, Prozesse und Daten durch. Ohne ausreichende Schutzmaßnahmen kann sich ein Angreifer oft mit wenig Aufwand unter Ausnutzung der Sicherheitslücken unberechtigten Zugang zu Rechnern mit Internetanschluss verschaffen und dort Daten ausspähen oder sogar manipulieren oder zerstören. Dies stellt allein aufgrund der Zahl der potenziellen Angreifer[2] ein erhebliches Problem dar.

Die vorliegende Orientierungshilfe wurde vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erstellt. Sie soll den für den Betrieb und die Konzeption von Netzen der öffentlichen Verwaltung Verantwortlichen deutlich machen, mit welchen Risiken für die Sicherheit der „internen“ Netze bei einem Anschluss an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können.

Die Frage, in welchen Fällen und unter welchen Bedingungen es zulässig ist, dass Verwaltungen personenbezogene Daten mit Hilfe des Internet übertragen oder veröffentlichen, ist nicht Gegenstand der Orientierungshilfe.

---

[1] Aufgrund der Zuständigkeit der Mitglieder dieses Gremiums vor allem für den Datenschutz im öffentlichen Bereich richtet sich diese Orientierungshilfe in erster Linie an öffentliche Verwaltungen. Die Aussagen lassen sich aber auch auf Unternehmen und andere Bereiche übertragen.

[2] Im Jahr 2006 ca. 1 Milliarde Internet-Nutzer weltweit; die Erreichung der Zwei-Milliarden-Grenze wird für 2011 prognostiziert (http://www.c-i-a.com/pr0207.htm).

2. Planung einer sicheren Internetanbindung

Grundlage für eine datenschutzgerechte Nutzung des Internet ist eine genaue Planung der Internet-Aktivitäten einer Verwaltung. Je nach dem Informations- und Kommunikations-Bedarf ist eine der möglichen Nutzungsarten unter Berücksichtigung einer der Anschlussmöglichkeiten vorzusehen. Es bedarf einer genauen Analyse sowohl dieses Bedarfs als auch der mit der jeweiligen Anschlussart verbundenen Risiken.

2.1 Nutzungs- und Anschlussmöglichkeiten

2.1.1 Nutzungsarten

Grundsätzlich sind zwei Konstellationen der Internet-Nutzung einer Behörde zu unterscheiden:

1. Eine Behörde nutzt einen Internet-Zugang, um Informationen im Internet zu nutzen bzw. zu suchen und nutzt Möglichkeiten der elektronischen Kommunikation mit Behörden, Firmen und ggf. Bürgerinnen und Bürgern, z.B. per E-Mail, und/oder
2. eine Behörde stellt eigene Informationen im Internet zum (potentiell weltweiten) Abruf zur Verfügung und bietet zusätzlich die Interaktion mit Bürgerinnen und Bürgern, z.B. per E-Mail bzw. Web-Formulare, an.

Die vorliegende Orientierungshilfe befasst sich vorwiegend mit der ersten Konstellation. Die zweite Konstellation, das Informationsangebot im Internet, wird i.d.R. von einem externen Dienstleister realisiert, der die notwendigen Web-Server in einem Rechenzentrum betreibt. Für Fragestellungen, die sich aus der zweiten Konstellation ergeben, verweisen wir auf die „Orientierungshilfe Datenschutzgerechtes eGovernment“ [OH eGov] des Arbeitskreises Technik.

2.1.2 Anschlussarten

Prinzipiell können die Anschlussarten an das Internet in drei verschiedene Szenarien unterteilt werden, die unterschiedliche Sicherheitsrisiken mit sich bringen. Das erste Szenario ist in der Praxis in Behörden kaum noch gebräuchlich und wird hier nur noch der Vollständigkeit halber aufgeführt. Die möglichen Anschlussarten werden in diesem Abschnitt nur informativ vorgestellt. Für grundsätzliche Betrachtungen verweisen wir auf den vom Bundesamt für Sicherheit in der Informationstechnik herausgegebenen Leitfaden „Integration und IT-Revision von Netzübergängen“ [BSI 2006].

2.1.2.1 Direktanschluss eines Rechners an das Internet

Hier wird ein einzelner, nicht lokal vernetzter Rechner per Modem, ISDN oder DSL über einen Provider (dies kann ein verwaltungsinterner oder ein externer sein) an das Internet angeschlossen (Abbildung 2.1). Selbst bei kleinen Behörden spielt diese Variante keine größere Rolle mehr, da in aller Regel mehrere Arbeitsplatzrechner miteinander und mit dem Internet verbunden werden müssen. Bei eventuellen Angriffen besteht ein Sicherheitsrisiko nur für den einzelnen Rechner. Da der Schutz dieses Rechners nur eingeschränkt möglich ist, kann diese Konfiguration nur empfohlen werden, wenn der Rechner **ausschließlich** für den Zugang zum Internet verwendet wird.

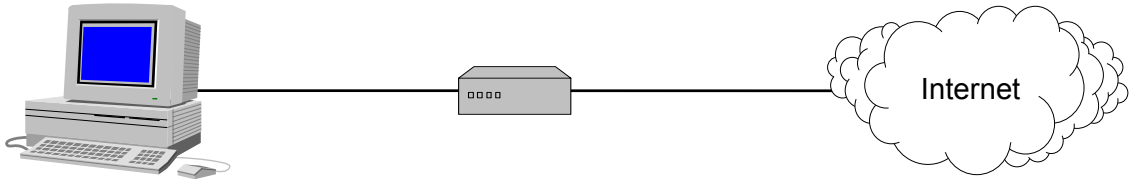

Abbildung 2.1: Direktanschluss eines Rechners an das Internet

2.1.2.2 Zentrale Kopplung eines lokalen Netzes an das Internet

Hier hat der Rechner (i.d.R. über ein LAN) einen Zugang zum Intranet der Verwaltung. Von dort besteht ein einziger zentraler Zugang zum Internet (Abbildung 2.2). Eventuelle Angriffe aus dem Internet können bereits an der zentralen Übergangsstelle vom Internet zum Intranet zum großen Teil abgefangen werden. Für die Planung muss beachtet werden, dass der Rechner bzw. das LAN zusätzlich aus dem Intranet heraus angreifbar ist.

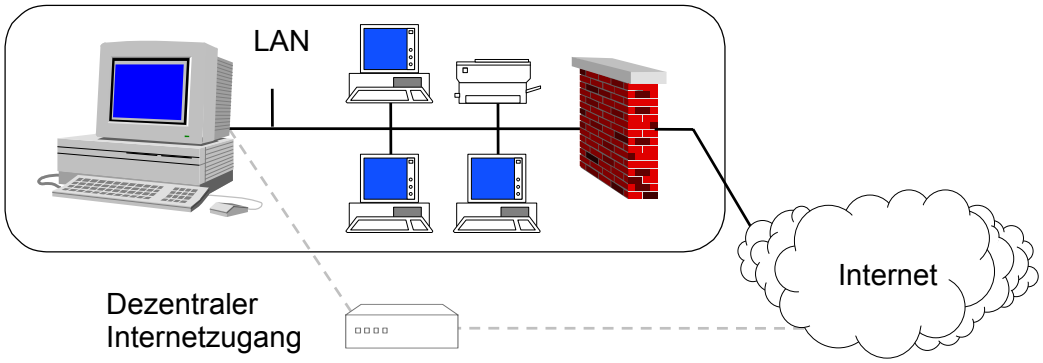

Abbildung 2.2: Zentrale Kopplung eines lokalen Netzes an das Internet

In Abbildung 2.2 ist zudem (in grau) ein dezentraler Internetzugang eingezeichnet. Solche Konfigurationen findet man vereinzelt noch immer. Bei eventuellen Angriffen besteht nicht nur ein

Sicherheitsrisiko für den dezentral an das Internet angeschlossenen Rechner, sondern auch für das LAN, in dem sich der Rechner befindet, und das Intranet. **Daher ist von dieser Konstellation generell abzuraten.**

Die zentrale Übergangsstelle zum Internet kann so gestaltet sein, dass mehrere getrennte Bereiche (Teilnetze mit verschieden hohen Sicherheitsanforderungen) miteinander verbunden werden. So kann beispielsweise der E-Mail-Server in einem weniger sicherheitskritischen Bereich untergebracht werden oder im Intranet nur ein graphischer Zugang zum Internet (z.B. per VNC oder Citrix, siehe 5.4.3) angeboten werden.

2.2 Kommunikations- und Risikoanalyse

Die Art des zu realisierenden Zugangs hängt wesentlich davon ab, welche Dienste des Internet genutzt werden müssen. Vor einem Anschluss an das Internet ist daher eine Analyse des Kommunikationsbedarfs durchzuführen. Diese Kommunikationsanforderungen müssen aufgrund der unterschiedlichen Aufgaben sowohl für den zentralen Zugang zum Internet als auch für jeden einzelnen Rechner analysiert werden.

Ausgangspunkte einer derartigen Analyse sind der Schutzbedarf der zu verarbeitenden Daten und die Sicherheitsziele der öffentlichen Stelle sowie die Risiken der unterschiedlichen Dienste.

In Anlehnung an die Empfehlungen der BSI-Grundschutzkataloge [BSI GS] sind im Rahmen einer Risikoanalyse zur Feststellung des Schutzbedarfs folgende Fragen zu beantworten:

- 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 interne Netzstruktur und Benutzernamen nach außen unsichtbar gemacht werden? (z.B. durch Nutzung eines HTTP-Proxy-Servers)
- Welche (benutzerspezifischen) Authentisierungsverfahren sollen benutzt werden?
- 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?
- Welche Einschränkungen würden Benutzer durch den Einsatz von Schutzmaßnahmen akzeptieren?

Um im Rahmen der empfohlenen Kommunikationsanalyse beurteilen zu können, welche Dienste von welchem Nutzer an welchem Rechner tatsächlich benötigt werden, sollten die jeweiligen Stellen zunächst versuchen, genaue Kenntnisse über die Möglichkeiten und Gefährdungen der angebotenen Kommunikationsmöglichkeiten zu erlangen.

Verwaltungsnetze dürfen an das Internet nur angeschlossen werden, wenn und soweit dies erforderlich ist. Die Kommunikationsmöglichkeiten haben sich am Kommunikationsbedarf zu orientieren. Dabei ist auch zu prüfen, inwieweit das Behördennetz in anschließbare, nicht anschließbare und bedingt anschließbare Teile (beispielsweise über einen graphischen Zugang) segmentiert werden muss. Bei einem unvertretbaren Restrisiko muss auf einen Anschluss des jeweiligen Netzes an das Internet verzichtet werden. Der Zugriff auf Internet-Dienste kann in diesem Fall nur über solche Systeme erfolgen, die nicht mit dem Verwaltungsnetz verbunden sind und auf denen ansonsten keine sensiblen Daten verarbeitet werden.

2.3 Sicherheitsrisiken und Schutzmaßnahmen

Mit dem Zugang zum Internet sind Risiken verbunden, die großenteils daraus resultieren, dass das Datennetz nicht unter Sicherheitsaspekten entwickelt wurde. Schwächen finden sich in den Protokollen für die Datenübertragung, in den Implementierungen und Installationen der Programme für die Internet-Dienste und in den angeschlossenen Rechnersystemen. So stellt das dem Internet zugrunde liegende IP-Protokoll beispielsweise keine sicheren Mechanismen zur Identifikation und Authentisierung bereit.

Die nachfolgend dargestellten Sicherheitsrisiken spiegeln lediglich einen kleinen Ausschnitt der möglichen Angriffe auf Rechnersysteme mit Internet-Anschluss wider. Selbst wenn Maßnahmen gegen die bekannten Gefährdungen getroffen werden, lässt sich ein hundertprozentiger Schutz ohne Verzicht auf die Internet-Anbindung nicht realisieren. Sobald ein Computer Zugang zu einem Datennetz hat, ist er von anderen angeschlossenen Rechnern aus erreichbar. Damit wird das eigene System der Gefahr eines unberechtigten Gebrauches ausgesetzt. Es gibt jedoch eine Reihe von Schutzvorkehrungen, um das Sicherheitsrisiko zu minimieren.

2.3.1 Protokollimmanente Sicherheitsrisiken

Bei vielen gängigen Diensten werden die Inhaltsdaten im Klartext über das lokale Netz (z.B. Ethernet) und über das Internet übertragen. Mit Programmen, die unter der Bezeichnung LAN-Analyzer bekannt sind (z.B. Packet Sniffer), kann der Datenverkehr im Netz bzw. auf den Netzknoten belauscht und nach interessanten Informationen durchsucht werden.

Gegenmaßnahmen:

Verschlüsselung der Daten

Datenpakete können nicht nur abgehört, sondern auch manipuliert werden. Beispielsweise lässt sich der Dateninhalt und die Sender bzw. Empfängeradresse fälschen. Auch 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 Nachrichteninhalten 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-Adresse 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 Paket-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.**) Identifizierung und Authentifizierung ausschließlich an Hand der IP-Adresse vermeiden!

*) definiert im RFC 1597

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

Zudem werden immer wieder Fehler in Protokollen und noch wesentlich häufiger in den dazugehörigen Implementierungen gefunden. Infolge solcher Fehler ergeben sich Angriffmöglichkeiten, die eigentlich durch bereits umgesetzte Sicherheitsmaßnahmen ausgeschlossen sein sollten.

Gegenmaßnahmen:

Sämtliche genutzte Soft- und Hardware sollte u.a. durch Installation von Patches immer auf dem neuesten Stand gehalten werden. **Zudem sind alle nicht notwendigen Dienste unbedingt zu deaktivieren**. Idealerweise sollte so häufig wie möglich mit starker Authentisierung gearbeitet werden.

2.3.2 Dienstespezifische Sicherheitsrisiken

2.3.2.1 E-Mail

Elektronische Post (E-Mail) kann mitgelesen werden, sofern sie nicht verschlüsselt ist. E-Mails ohne eine digitale Signatur lassen sich leicht verändern oder fälschen. Über den elektronischen Postweg können – wie bei einem Transfer per physischen Datenträger – Computerviren und Trojaner ins System gelangen. Selbst ein automatisches Durchsuchen der Nachrichten nach Viren bietet keinen vollständigen Schutz.

Gegenmaßnahmen:

Verschlüsselung und digitale Signatur,

Virenschutzsysteme

Das E-Mail-Programm und auch Server-Software zum Verschicken elektronischer Post sollte regelmäßig aktualisiert werden, um sicherheitsrelevante Fehler schnellstmöglich zu korrigieren.

2.3.2.2 Telnet

Telnet ist ein Dienst, mit dem berechtigte Nutzer und insbesondere der System-Administrator sich auf der Text-Konsole eines entfernten UNIX-Rechners einloggen können. Telnet bietet keine Verschlüsselung. Ein Angreifer kann daher absolut sicherheitskritische Zugangsdaten leicht abhören, in bestehende 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), einem Software-Paket, mit dem man durch anerkannte kryptographische Verfahren eine zuverlässige gegenseitige Authentisierung und eine transparente Verschlüsselung des gesamten Datenstroms erreichen kann.

2.3.2.3 FTP

Besondere Vorsicht ist bei der Konfiguration von FTP-Servern geboten, insbesondere wenn der FTP-Server Daten uneingeschränkt (Anonymous-FTP) zum Download bereitstellen soll. Bei Fehlkonfigurationen kann es einem Angreifer gelingen, auf eigentlich zu schützende Bereiche zuzugreifen. Beispielsweise könnte er versuchen, 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:

Ersatz des FTP-Dienstes (incl. rcp) durch Programme aus dem SSH-Paket (scp) oder Konfiguration eines SSH-Kanals mit Verschlüsselung und Authentisierung, Beschränkung durch Vergabe von entsprechenden Zugriffsrechten

2.3.2.4 WWW

Gefährdungen entstehen bei der Nutzung des WWW insbesondere durch fehlerhafte Software. Ohne den Einsatz von SSL (Secure Socket Layer) oder anderen Verschlüsselungsmechanismen lässt sich die Kommunikation leicht abhören. Zudem werden Angriffsmethoden wie **Web-Spoofing** vereinfacht, 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:

SSL-Verschlüsselung der Kommunikation und Authentisierung der Web-Server, gegenseitige Authentisierung von Nutzer und Web-Server.

Eine besondere Gefahr stellen aktive Inhalte in Webseiten da. Diese werden daher in Abschnitt 2.3.3 ausführlich behandelt.

2.3.2.5 DNS

Mit Hilfe des Domain Name Service (**DNS**) lassen sich Rechnernamen in IP-Adressen umsetzen und umgekehrt. Dabei besteht die Gefahr, dass Informationen über die Struktur des internen Netzes nach außen gelangen. Auch beim DNS gibt es 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:

Verbergen der Struktur des internen Netzes durch geeignete Anordnung von DNS-Servern, Adressierung durch die numerische IP-Adresse, soweit praktikabel, Einsatz eigener Domain Name Server

2.3.2.6 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

2.3.2.7 Instant-Messaging

Als Instant-Messaging werden Dienste wie z.B. ICQ und die dazugehörige Client-Programme bezeichnet, mit denen Benutzer über das Internet miteinander chatten oder zeitverschoben Nachrichten versenden können. Die hohe Attraktivität besteht darin, dass sichtbar ist, welcher der Bekannten/Freunde (Buddies) gerade „Online“ ist, man also eine schnelle Antwort erwarten kann.

Ein Sicherheitsrisiko stellen derartige Dienste in mehrfacher Hinsicht dar. Einerseits wurden in den Client-Programmen immer wieder Sicherheitslücken gefunden, die beispielsweise das Einschleusen von Viren oder Trojanern ermöglichte. Zudem ist es für die Nutzung der Dienste oft erforderlich, einige Einschränkungen des Internetzugangs zu lockern (z.B. bestimmte Ports in der Firewall freizugeben), wodurch neue Angriffmöglichkeiten entstehen können. Ein weiteres Risiko geht von den Nutzenden selbst aus: Viele Instant-Messaging-Dienste bieten die Möglichkeit, Dateien zu übertragen. Dies umgeht möglicherweise Einschränkungen und Vorkehrungen wie z.B. den Nichteinbau von Diskettenlaufwerken oder das Scannen aller E-Mails auf Viren. Soll Instant-Messaging für dienstliche Zwecke eingesetzt werden, ist zu beachten, dass die Datenübertragung oft unverschlüsselt erfolgt und daher abgehört werden könnte. Zudem werden die Nachrichten (wie auch bei E-Mail) über den zentralen Server des Anbieters übertragen. Dieser könnte daher das Kommunikationsverhalten uns sogar die Nachrichteninhalte protokollieren und missbräuchlich verwenden.

> Die dienstliche oder private Nutzung von Instant-Messaging-Diensten externer Anbieter sollte in der Verwaltung nicht erlaubt werden.

2.3.2.8 Internet-Telefonie / Voice over IP

Bei der Internet-Telefonie, auch als Voice over IP (VoIP) bezeichnet, muss unterschieden werden zwischen Softwarelösungen externer Anbieter und Lösungen, die die bisherige ISDN-

Telefonanlage ersetzen soll. Erstere Lösungen werden insbesondere im privaten Bereich eingesetzt, um z.B. bei Auslandsgesprächen hohe Telefonkosten zu vermeiden. Dazu wird eine Telefonie-Software (z.B. Skype) auf dem Rechner jedes Nutzenden installiert und die Gesprächsdaten werden über bestehende Internetverbindungen ohne Zusatzkosten übertragen. Gegen den Einsatz von Telefonier-Software im Intranet der Verwaltung bestehen die gleichen Bedenken wie gegen den Einsatz von Instant-Messaging-Programmen (vgl. vorherigen Abschnitt). Auch bei VoIP-Programmen werden immer wieder Sicherheitslücken bekannt. Zudem bieten auch VoIP-Programme oft die Möglichkeit, Dateien zu übertragen. Für den dienstlichen Einsatz sind derartige Softwarelösungen (auch zusätzlich) wegen der unsicheren Verfügbarkeit und der Abhängigkeit von einem externen Anbieter nicht zu empfehlen. Die Gesprächsdaten werden normalerweise direkt zwischen den Telefonierenden übertragen und zudem bei einigen Diensten verschlüsselt, aber der Anbieter kennt normalerweise den eingesetzten Schlüssel, so dass Gesprächsinhalte prinzipiell entschlüsselt werden könnten.

Für den Einsatz von VoIP als Ersatz für die bisherige ISDN-Telefonanlage verweisen wir auf die Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik [BSI GS], insbesondere auf Baustein B 4.7. Grundsätzlich sollte sowohl die Signalisierung von Gesprächswünschen sowie die Sprachübertragung verschlüsselt erfolgen, da das IP-Datennetz wesentlich verwundbarer gegenüber (internen) Angreifern ist. Daher sollte auch eine logische Trennung des Sprachnetzes vom Datennetz realisiert werden. Dazu bietet sich der Einsatz von Virtuellen Netzwerken (VPN) an, beispielsweise auf Basis des Routingprotokolls „Multiprotocol Label Switching (MPLS)“.

2.3.3 Aktive Inhalte/Aktive Elemente

Neben E-Mail ist das WWW eine der Hauptanwendungen des Internet. Innerhalb der für das WWW genutzten Protokolle HTTP und HTML existieren weitere Dienste, deren Sicherheits- und Datenschutzrisiken in diesem Abschnitt aufgezeigt werden.

2.3.3.1 ActiveX

ActiveX ist eine **Entwicklung der Firma Microsoft**. Es 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 ausführbare 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 in einer WWW-Seite eingebettet 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 Scrip-

ting 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 herunter geladenen Codes durch Codesignierung mittels digitaler Signatur. Dies erlaubt neben der sicheren Identifikation des Programm-Autors 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.

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.** Aus Sicherheitsgründen empfiehlt es sich daher, die ActiveX-Unterstützung gänzlich abzuschalten.

Gegenmaßnahmen:

Abschalten der ActiveX-Unterstützung,
Aktivieren einer hohen Sicherheitsstufe im Internet-Explorer,
Einsatz von ActiveX-Filtern und des Internet-Explorer-Administration-Kits in Netzwerken

Abschließend sei noch auf die **unzureichenden Sicherheitsmechanismen der Betriebssystemplattformen** hingewiesen. Erst ab Windows Vista laufen Webbrowser und damit auch ActiveX-Controls und andere aktive Inhalte in einem eingeschränkten Rechteraum.

2.3.3.2 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-Applications) 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 (Java Virtual Machine) auf der Plattform. Java verfügt über ein integriertes Sicherheitssystem **(Sandbox-System):**

Im Browser ausgeführte Java-Applets unterliegen sehr strengen Sicherheitskontrollen. Applets, die über das Netz geladen werden, haben auf dem Client keine Lese- und Schreibrechte, können keine fremden Programme starten, keine Systemfunktionen aufrufen, keine Netzwerkverbindung zu anderen Rechnern aufbauen, keine zusätzlichen Bibliotheken laden und kennzeichnen Fenster besonders, die durch Applets gestartet wurden.

Applets können im Standardfall auch nur definierte Systemeigenschaften (z.B. die Version des Betriebssystems) lesen. SUN bietet zudem die Möglichkeit, mit **signierten Applets** zu arbeiten. Somit kann der Client die Authentizität und die Herkunft prüfen. Die Signierung sagt jedoch nichts über die Funktionalität des Programms. Die Java-Spezifikation bietet mit ihren durchdachten Mechanismen eine ausreichende Sicherheit, aber durch Implementierungsfehler wurden Angriffe durch Java-Applets möglich.

Um sich zusätzlich zu schützen, bieten sich mehrere Optionen an. Man kann z. B. im Browser **die Java-Funktionalität abschalten** oder auf **signierte Applets** beschränken. Einen weiteren Schutz bieten **Java-Filter**, die Listen mit Servern definieren, von denen Java-Applets akzeptiert werden.

Gegenmaßnahmen:

Abschalten der Java-Funktionalität, Einsatz von Java-Filtern, Arbeiten mit signierten Applets, Verwendung von Browsern, bei denen JVM fehlerfrei implementiert ist.

2.3.3.3 JavaScript

JavaScript ist eine plattformunabhängige **Skriptsprache**. Sie wird direkt in die HTML-Seiten eingebettet und über einen Interpreter interpretiert und ausgeführt. Durch den Einsatz von JavaScript kann die Anzahl von notwendigen Verbindungen zum Server verringert werden, indem beispielsweise Eingaben überprüft oder auch Berechnungen lokal durchgeführt werden. Außer-

dem lassen sich wichtige Funktionen des Browsers, wie Öffnen und Schließen von Fenstern, Manipulieren von Formularelementen oder das Anpassen von Browser-Einstellungen verwirklichen. Ein Zugriff auf Dateisysteme auf anderen Rechnern ist nicht möglich. Sicherheitsprobleme gibt es jedoch in zwei Bereichen: 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 Implementierungsfehler in den Ablaufumgebungen modifizieren oder eine weitere Nutzung des Systems – vorsätzlich erzeugt oder ungewollt durch Programmierfehler – verhindern, und Angriffen die das Lesen von fremden Nachrichten, Ändern von Nachrichten und Verschicken von Texten ermöglichen. Die meisten Sicherheitslöcher sind implementierungsabhängig.

Gegenmaßnahmen:

> Verwendung von Browsern, bei denen die Anwendung korrekt implementiert ist, regelmäßiges Einspielen von Patches. Aktivieren der JavaScript-Funktionalität nur für vertrauenswürdige Webseiten.

2.3.3.4 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. Weit verbreitet ist beispielsweise der **Flash-Player**, welcher als Browser-Plug-In für alle Plattformen verfügbar ist. Flash ist ein auf Vektorgrafiken basierendes Grafik- und Animationsformat. Eingesetzt wird es beispielsweise für animierte Filme, für Werbebanner und gelegentlich zur gesamten Gestaltung eines Webangebotes. Ein Abschalten von Flash bzw. Nichtinstallieren des Plug-Ins kann daher i.d.R. nicht empfohlen werden.

Der Flash-Player kann kleine Binärdateien, so genannte Local Shared Objects (LSOs), auf dem Rechner des Anwenders abspeichern. Diese können die gleichen Zwecke erfüllen, wie die im nächsten Abschnitt vorgestellten HTTP-Cookies. Allerdings entziehen sich die **Flash-Cookies** den Cookie-Verwaltungsmechanismen des Browsers und müssten über ein Interface des Flash-Players gelöscht bzw. deaktiviert werden.

Gegenmaßnahmen:

> Schulung der Benutzer, um unbeabsichtigtes Installieren der Software zu verhindern. Deaktivierung der lokalen Datenspeicherung des Flash-Players.

2.3.3.5 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. Die Anwendungsmöglichkeiten gehen jedoch weit darüber hinaus.

Typischerweise werden Cookies eingesetzt, damit der Nutzer das Angebot des angewählten Webservers auf seine persönlichen 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. Eine Manipulation des Computers über die Speicherung und Abfrage der Cookie-Daten hinaus ist mit dem Cookie-Mechanismus selbst nicht möglich. Da die Cookie-Informationen, die auch Zugangsberechtigungen für Web-Seiten umfassen können, jedoch in einer Datei im Dateisystem auf dem Rechner gespeichert werden, kann ein Unberechtigter beispielsweise mit Hilfe von ActiveX-Controls (siehe 2.3.3.1) darauf zugreifen.

Problematisch sind Cookies trotzt dieses vergleichsweise geringen Gefährdungspotentials für die Computersicherheit aufgrund ihrer geringen Transparenz für den Benutzer. Der Datenaustausch mittels Cookies erfolgt zwischen den beteiligten Computern vollkommen im Hintergrund, ohne dass der Benutzer über Inhalte, Zweck, Umfang, Speicherdauer oder Zugriffsmöglichkeiten auf die Cookie-Daten informiert wird, sofern er keine besonderen Maßnahmen ergreift. Insbesondere von den Betreibern der allgegenwärtigen Internet-Werbung werden Cookies missbräuchlich verwendet, um Interessensprofile der Nutzenden zu erstellen. 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. Moderne Browser bieten mittlerweile ausgefeilte Möglichkeiten der Verwaltung von Cookies. Empfehlenswert ist die Einstellung, sämtliche Cookies nur bis zum Ende der aktuellen Sitzung / bis zum Schließen des Browsers zu speichern und für einzelne Webseiten Ausnahmen zu definieren, falls der Einsatz von Cookies wirklich einen Vorteil bedeutet.

Gegenmaßnahmen:

> Konfiguration des Browsers, so dass Cookies nicht oder nur auf Nachfrage akzeptiert werden. Empfehlenswert ist es, Cookies nur bis zum Schließen des Browsers zu speichern.

Löschen bereits gespeicherter Cookies, Einsatz von Cookie- und Werbefiltern (z.B. Adblock Plus für Mozilla)

3. Sicherheitsgateways und modulare Erweiterungen

Um ein lokales Verwaltungsnetz an das Internet anzuschließen, ist der Einsatz eines Sicherheitsgateways erforderlich.

Die Verwendung des Begriffs „Sicherheitsgateways“ wurde bewusst gewählt. Er wurde anstatt des üblicherweise genannten Begriffes „Firewall“ verwendet und soll verdeutlichen, dass zur Absicherung von lokalen Netzen und Netzübergängen heute nicht mehr ein einzelnes Gerät verwendet wird, sondern eine Menge von Rechnern und deren Konzeption, die unterschiedliche Aufgaben übernehmen, z. B. Schutz vor Viren, Spam oder die Überwachung des Netzverkehrs.

3.1 Grundkonzepte Sicherheitsgateways

Ein Sicherheitsgateway ist ein System aus soft- und hardewaretechnischen Komponenten zur Gewährleistung einer sicheren Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsleitlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei vor allem die ausschließliche Zulassung erwünschter Zugriffe oder Datenströme zwischen verschiedenen Netzen und die Kontrolle der übertragenden Daten.

Ein Sicherheitsgateway kann durch verschiedene Grundkomponenten realisiert werden. Im Wesentlichen unterscheidet man folgende Komponenten:

- Paketfilter
- Application-Level-Gateway
- DMZ

3.1.1 Paketfilter

Paketfilter sind IT-Systeme mit spezieller Software, die den ein- und ausgehenden Datenverkehr anhand spezieller Regeln filtern. Ihre Aufgabe ist es, Datenpakete anhand der Informationen in den Header-Daten der IP- und Transportschicht (z. B. Quell- und Ziel-Adresse, -Portnummer, TCP-Flags) weiterzuleiten oder zu verwerfen. Der Inhalt des Pakets bleibt dabei unberücksichtigt.

Vielfach bieten Paketfilter auch eine Möglichkeit zur Adressumsetzung (Network Address Translation, NAT), bei der zum Beispiel die Absender-Adresse im IP-Paket-Header durch eine IP-Adresse des Paketfilters ersetzt wird. Dadurch wird die Netzstruktur des zu schützenden Netzes gegenüber externen Kommunikationspartnern verborgen.

Paketfilter, die eine Filterentscheidung allein anhand der Header-Daten des Datenpakets treffen, werden *zustandslose Paketfilter* genannt. *Zustandsbehaftete Paketfilter* erweitern dagegen die zustandslose Filterung um die Möglichkeit zur Betrachtung des Kommunikationskontexts (sogenannte Stateful Inspection). Die Filterung erfolgt hierbei zum Beispiel abhängig davon, ob die Kommunikationsverbindung von innen nach außen oder von außen nach innen aufgebaut wurde, oder zeitabhängig in einem vorgegebenen Freigabeintervall. Darüber hinaus können zustandsbehaftete Filter oft auch einfache Anwendungsattribute oberhalb der Transportschicht in die Betrachtung einbeziehen.

Einfache Paketfilter lassen sich als Software-Lösung auf PC-Basis unter einem Standardbetriebssystem (z. B. Linux) realisieren. Reine Software-Realisierungen weisen jedoch eine Reihe gravierender Nachteile auf:

- Ihr Durchsatz ist gering, nicht zuletzt wegen der beschränkten Leistungsfähigkeit des Kommunikationsbusses gewöhnlicher PC-Architekturen.
- Aufgrund beweglicher Teile (Festplatte, Lüfter) haben PCs im Dauerbetrieb eine höhere Ausfallwahrscheinlichkeit als Hardware-Lösungen ohne solche mechanischen Komponenten.
- Der Bedienkomfort ist in der Regel geringer als bei spezialisierten Geräten.

Für höhere Ansprüche wird daher normalerweise der Einsatz von Paketfiltern mit maßgeschneiderter Hardware und angepasstem Betriebssystem empfohlen, zum Beispiel eine Appliance, ein Router oder ein kommerzielles Firewall-Produkt.

3.1.2 Application-Level Gateway (Sicherheits-Proxy)

Filterfunktionen oberhalb der Transportschicht werden von einem sogenannten Application-Level Gateway (ALG) übernommen, auch Sicherheits-Proxy genannt. Ein Proxy ist eine Art Stellvertreter für Dienste in Netzen. Er nimmt Daten an seinem Eingang entgegen und leitet sie nach einer Prüfung an den eigentlichen Dienst weiter. Mittels eines Proxys lassen sich Datenströme auf der Anwendungsschicht verwerfen, modifizieren oder gezielt weiterleiten.

Implizit nehmen ALGs auch Funktionen auf den darunter liegenden Schichten des TCP/IP-Modells wahr. ALGs unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über das ALG hinweg nimmt das ALG die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt das ALG analog.

Diese Kommunikationsform ermöglicht es dem ALG beispielsweise, bestimmte Protokollbefehle auf der Anwendungsschicht zu filtern. Das ALG kann zudem die strikte Einhaltung von Anwen-

dungsprotokollen erzwingen, unerwünschte Anwendungsdaten aus den Datenpaketen entfernen (bzw. austauschen) oder Verbindungen anwendungsspezifisch protokollieren.

Verglichen mit einem (meist vorgeschalteten) Paketfilter ermöglicht ein ALG in der Regel nur einen geringeren Durchsatz bei der Datenübermittlung. Um das ALG zu entlasten und seinen Durchsatz zu verbessern, können ALG-Proxy-Funktionen auf separate Proxy-Server ausgelagert werden, die parallel zum ALG betrieben werden (z. B. für das rechenintensive Auftrennen verschlüsselter Verbindungen). Dies verringert bei komplexen Anwendungsprotokollen (z. B. SOAP mit WSS-Erweiterungen) die Angriffsfläche des ALGs und beschleunigt die Übermittlung größerer Datenströme. Das Auskoppeln einzelner Protokolle und deren Umlenken auf einen unabhängigen Proxy-Server verursacht unter Umständen allerdings zusätzliche Paketlaufzeiten (Latenz) für die betroffenen Kommunikationsverbindungen, was sich vor allem bei interaktiven Kommunikationsmustern störend bemerkbar machen kann.

Sicherheits-Proxys können nur unverschlüsselte Daten filtern. Um auch bei verschlüsselter Kommunikation einen Sicherheitsgewinn zu erzielen, ist es daher erforderlich, die Verschlüsselung im Proxy aufzubrechen und gegebenenfalls die Daten für das interne Netz erneut zu verschlüsseln. Das Aufbrechen der Kommunikationsbeziehung zerstört jedoch die Ende-zu-Ende-Sicherheitsgarantien, was nicht in allen Anwendungen tolerierbar ist.

3.1.3 Demilitarisierte Zone

Eine Demilitiarisierte Zone (DMZ) ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen, noch zu dem anderen Netz gehört. Sie stellt ein Netz dar, das weniger stark gesichert, aber vom äußeren Netz aus besser erreichbar ist als das eigentlich zu schützende interne Netz. Die DMZ dient der Schaffung eines zusätzlichen Sicherheitsbereichs für Dienste (z. B. E-Mail, Web) oder Proxys, die von externen Netzen aus nutzbar sein sollen, aber aus Sicherheitsgründen nicht im internen Netz platziert werden dürfen.

Bei einem dreistufigen Sicherheits-Gateway (Paketfilter − ALG − Paketfilter, siehe Abbildung 3.1) dient in der Regel eine weitere Schnittstelle des ALGs als DMZ-Schnittstelle. Verfügt das ALG über mehr als drei Schnittstellen, können weitere derartige Zonen gebildet werden.

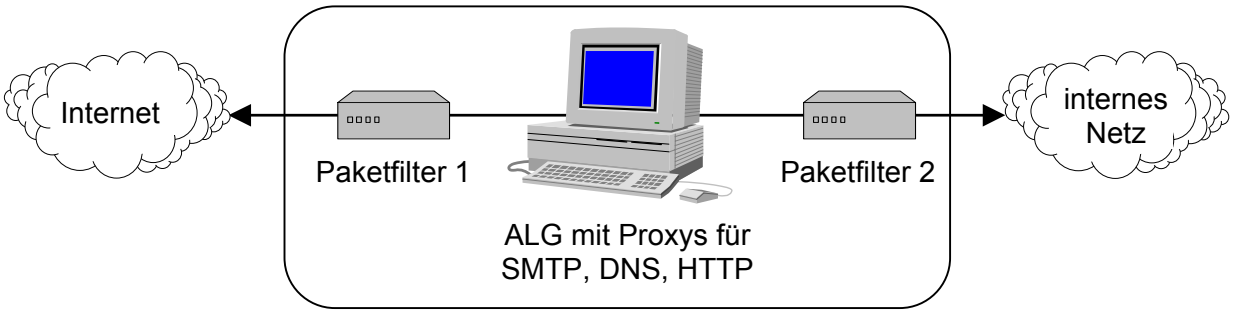

Abbildung 3.1: Dreistufiges Sicherheitsgateway

3.2 Modulare Erweiterungen

Sichere Netzkopplung auf der Anwendungsschicht erfordert die individuelle Anpassung des Sicherheits-Gateways an die spezifischen Anwendungen im LAN. Daher sind Erweiterungen des Sicherheits-Gateways in der Regel unumgänglich. Dazu werden die betroffenen Anwendungsprotokolle im Gateway ausgekoppelt und gesonderten Erweiterungsmodulen zugeführt.

Grundlegende Empfehlungen zu modularen Erweiterungen eines Sicherheits-Gateways bietet [BSI-SGW 2007]. Die wichtigsten modularen Erweiterungen betreffen vor allem die im Folgenden genannten Punkte.

3.2.1.1 Terminieren sicherer Fernzugänge

Fernzugänge ermöglichen Mitarbeitern im Außendienst einen LAN-Zugriff über unsichere öffentliche Kommunikationsverbindungen (Client-to-Site), oder sie dienen dazu, entfernte LAN-Segmente über das Internet sicher anzubinden (Site-to-Site). Einen Client-to-Site-Zugriff bezeichnet man auch als Fernzugriff (Remote Access). Dazu bietet die ISi-Reihe ein eigenes Modul mit detaillierten Empfehlungen [ISi-Fern].

Sichere Site-to-Site-Verbindungen werden in der Regel als VPN realisiert (siehe 3.2.2). Das Sicherheits-Gateway stellt dazu ein VPN-Gateway bereit, das als Eintritts- und Austrittspunkt für VPN-Verbindungen dient. Genauere Sicherheitsempfehlungen zur Realisierung sicherer VPNs bietet die ISi-Reihe in [ISi-VPN].

3.2.1.2 Funktionsüberwachung der Internet-Anbindung

Die Internet-Anbindung − speziell das Sicherheits-Gateway − bedarf der kontinuierlichen Überwachung, um schnell auf Anzeichen für Fehlfunktion, mangelnde Verfügbarkeit oder äußere Bedrohungen durch Angriffsversuche reagieren zu können. Die Überwachung umfasst das Messen des Kommunikationsaufkommens und der Systemauslastung, das Erkennen verdächtiger Kommunikationsmuster (sogenannte Intrusion Detection) sowie eine geeignete Protokollie-

rung der erfassten Merkmale zur weiteren Analyse und zur Beweissicherung im Falle von Sicherheitszwischenfällen (siehe 3.2.3).

Da jegliche externe Kommunikation über das Sicherheits-Gateway geführt wird, ist dieses gut dazu geeignet, die Wechselwirkungen zwischen dem Internet und dem LAN zu überwachen. Die Funktionsüberwachung im Sicherheits-Gateway und entsprechende Maßnahmen im LAN-Inneren ergänzen sich wechselseitig, um die Verfügbarkeit und Integrität der lokalen IT-Infrastruktur zu gewährleisten.

3.2.1.3 Zentrales Erkennen und Löschen schädlicher Daten

Das Sicherheits-Gateway trägt entscheidend dazu bei, schädliche Daten (z. B. Computer-Viren, Spam, unerlaubte E-Mail-Dateianhänge) von den LAN-Anwendungen fernzuhalten. Viren- und Spam-Filterung ist zwar auch client-seitig möglich (siehe dazu [ISi-Client], [DSK-OHA]). Solche dezentralen Maßnahmen ersetzen jedoch nicht eine zentrale Filterung gemäß einer einheitlichen, LAN-übergreifenden Sicherheitsleitlinie. Sie dienen vielmehr als zusätzliche Verteidigungslinie bei einem Versagen der vorgelagerten zentralen Viren-Prüfung (siehe 3.2.4 und 3.2.5).

3.2.2 Virtuelle Private Netze

Ein Virtuelles Privates Netz ist ein Netz, das physisch innerhalb eines anderen Netzes (meist des Internets) betrieben wird, jedoch logisch von diesem Netz getrennt ist. VPNs können unter Zuhilfenahme kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten schützen und die Kommunikationspartner sicher authentisieren, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

Der Begriff VPN wird oft als Synonym für verschlüsselte Verbindungen verwendet. Zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls. Man unterscheidet zwei grundlegende VPN-Varianten: Trusted VPN und Secure VPN.

3.2.2.1 Trusted VPN

VPNs werden als *Trusted* VPN bezeichnet, wenn die vertrauliche Verbindung verschiedener Standorte durch externe VPN-Dienstleister gewährleistet wird. Dabei werden die Daten aus dem vertrauenswürdigen Netz in der Regel unverschlüsselt über einen dedizierten Kommunikationskanal zu einem Gateway-Router des Anbieters geleitet. Die Bildung des VPNs erfolgt dann durch logische Abschottung des VPN-Datenverkehrs vom übrigen Datenverkehr (z. B. mittels Multiprotocol Label Switching, MPLS [RFC 3031]). Für mobile Nutzer stellen Dienstleister zu-

dem VPNs über Gateway-Router bereit, die nur über spezielle Einwahl-Knoten erreicht werden können. Diese Einwahlknoten müssen vor unberechtigtem Zugriff geschützt werden.

Für vertrauliche Daten sind Trusted VPNs ohne zusätzliche Verschlüsselung auf der Anwendungsschicht nicht geeignet, da die Sicherheit solcher Verbindungen ausschließlich in Händen des Internet-Diensteanbieters liegt. So bietet ein Trusted VPN zum Beispiel keinen Schutz gegen Innentäter des Anbieters. Für vertrauliche Datenkommunikation empfiehlt sich daher ein Secure VPN.

3.2.2.2 Secure VPN

Die Abhängigkeit von Dritten kann vermieden werden, wenn die Vertraulichkeit der Kommunikationsverbindung an den Endpunkten der Verbindung durch Verschlüsselung gewährleistet wird, die im eigenen Verantwortungsbereich des VPN-Nutzers liegt. Man bezeichnet diese Lösung auch als *Secure* VPN.

Die am weitesten verbreiteten Technologien zur Erzeugung von Secure VPNs sind zurzeit IPSec und SSL-VPNs. Während IPSec eigens zur Realisierung von VPNs entworfen wurde, wird bei SSL-VPNs die SSL-Erweiterung des TCP/IP-Stacks zum Aufbau sicherer Transportverbindungen für alle Protokolle auf Anwendungsschicht verwendet.

3.2.3 Intrusion Detection System/Intrusion Prevention System

Ein Intrusion Detection System (IDS) ist ein System zum Erkennen von Angriffen auf ein Rechnersystem oder ein Rechnernetz. Richtig eingesetzt, ergänzen sich Sicherheits-Gateway und IDS und erhöhen so die Sicherheit von Netzen. Man unterscheidet zwischen folgenden IDS-Varianten:

- **Host-basierte Systeme** sind auf den zu überwachenden Komponenten installiert. Sie prüfen in regelmäßigen Abständen die Systemdateien und melden verdächtige Veränderungen, die auf Angriffsversuche hindeuten.
- **Netzwerk-basierte Systeme** analysieren den Netzwerkverkehr und melden Kommunikationsereignisse, die auf Missbrauchsversuche oder Sicherheitsverletzungen schließen lassen.
- **Hybrid-Systeme** verbinden beide Prinzipien, um eine höhere Abdeckung bei der Angriffserkennung zu erzielen. Man spricht in diesem Zusammenhang von netz- und hostbasierten Sensortypen, die an ein zentrales Managementsystem angeschlossen sind. Es ist heute üblich, dass ein IDS über eine solche hybride Funktionsweise verfügt.

IDS senden ihre Meldungen an ein zentrales Analysesystem. Dort können die eintreffende Befunde gesammelt, verdichtet und protokolliert werden. Zudem erfolgt bei Bedarf eine Alarmierung des Sicherheitsadministrators. In den meisten Fällen kann auf eine manuelle Analyse des Angriffs nicht verzichtet werden, da IDS einerseits Fehlalarme auslösen und andererseits nicht alle Auswirkungen eines Angriffs verlässlich erfassen können.

Ein Intrusion Prevention System (IPS) ist eine Erweiterung eines IDS. Ein IPS erkennt und meldet Angriffe nicht nur, sondern verwirft die zu einem erkannten Angriff gehörenden IP-Pakete und verschärft zu diesem Zweck gegebenenfalls dynamisch die Filtereinstellungen am Sicherheits-Gateway.

IDS oder IPS sind komplexe Erweiterungen von Sicherheits-Gateways und können hier nicht ausführlich behandelt werden. Genauere Hinweise zur Konzeption und Integration solcher Systeme, finden sich in verschiedenen IDS-Studien des BSI (siehe dazu das Verzeichnis [BSI 2002] im Internet) sowie in einem gesonderten Modul der ISi-Reihe [ISi-IDS]. Anforderungsprofile von IDS/IPS sowie rechtliche Aspekte, die aus Datenschutzgründen bei deren Einsatz zu beachten sind, finden Sie in dieser OH in Kapitel 6.

Das grundlegende Realisierungskonzept für die Erweiterung der Grundarchitektur um IDS-Funktionen ist wie folgt:

- **Hostbasierte IDS-Informationen** werden durch Out-of-Band-Zugriffe über das Management-Netz ausgelesen. Relevante Komponenten für eine hostbasierte Überwachung sind vor allem die ALG-Komponenten sowie die Server in der DMZ. Zum Schutz gegen Innentäter können bedarfsweise weitere Rechner im Server-Segment des internen Netzes in die Überwachung einbezogen werden.

- **Netzbasierte IDS-Informationen** werden mittels zusätzlicher Sensoren auf Kommunikationsverbindungen des Sicherheits-Gateways erhoben und ebenfalls über das Management-Netz sicher zur zentralen Auswertung weitergeleitet. Bei der netzbasierten Überwachung ist zu bedenken, dass IDS-Komponenten unter Umständen hohe Übertragungsbandbreiten verarbeiten müssen. Dies stellt besondere Anforderungen an die Sensoren, die den Durchsatz der Nutzdatenverbindung möglichst nicht mindern sollten und anfallende IDS-Daten gegebenenfalls geeignet verdichten müssen, um das Management-System nicht zu überlasten.

Bei allen Überwachungsmaßnahmen sind allerdings die geltenden datenschutzrechtlichen Bestimmungen (siehe Kapitel 6) genau einzuhalten, da die erfassten Daten potenziell die Privatsphäre lokaler Netzteilnehmer oder externer Kooperationspartner berühren. Daher sind die Grundsätze des Datenschutzes − zum Beispiel das Wesentlichkeitsprinzip (Datensparsamkeit)

und die Zweckbindung − schon bei der Planung und Durchführung von Überwachungsmaßnahmen umfassend zu berücksichtigen.

3.2.4 Virenschutz

Für das Ausfiltern schädlicher Daten auf der Anwendungsschicht werden Virenschutzprogramme eingesetzt, die als Sicherheits-Proxys im ALG betrieben werden. Solche Virenschutz-Programme sind nach zwei Funktionsprinzipien realisierbar.

3.2.4.1 Signaturerkennung

Dieses Verfahren beruht auf dem Abgleich der Daten mit hinterlegten Erkennungsmerkmalen („Signaturen“) bekannter Schadprogramme. Eine Stärke der Signaturerkennung ist die geringe Anzahl von Fehlalarmen (False Positives) und das sichere Erkennen der geläufigen Schädlinge. Der Nachteil des Verfahrens besteht darin, dass eine ständige Auffrischung der Signaturen erforderlich ist und dass die Signaturerkennung blind gegenüber neuem Schadecode ist, für die noch keine Signaturen verfügbar sind.

3.2.4.2 Anomalie-Erkennung

Anomalie-Erkennung vergleicht den beobachteten typischen Systemzustand mit den aktuell erfassten Beobachtungsdaten und schlägt Alarm, wenn „unübliche“ Daten oder Kommunikationsmuster erkannt werden, deren Abweichung ein vorgegebenes Toleranzintervall überschreitet. Anders als bei der Signaturerkennung lässt sich so unter Umständen auch Schadcode erkennen, der bisher unbekannt war. Eine stetige Signatur-Aktualisierung ist nicht erforderlich, denn Anomalie-Erkennung bietet das Potenzial für selbstlernende, adaptive Filter. Die Schwäche des Verfahrens ist die vergleichsweise geringe Erkennungswahrscheinlichkeit (False Negatives), die derzeit nur auf Kosten einer höherer Quote von Fehlalarmen (False Positives) gesteigert werden kann.

Kommerzielle Virenschutzprogramme arbeiten derzeit vor allem mit Signaturerkennung. Selbstlernende Sicherheits-Proxys nach dem Prinzip der Anomalie-Erkennung befinden sich noch im Forschungsstadium.

3.2.5 Antispam-Strategien

Der Begriff Spam bezeichnet unverlangt zugesandte Massen-E-Mail. Unverlangt ist eine E-Mail dann, wenn das Einverständnis des Empfängers zum Empfang der Nachricht nicht vorliegt und nicht zu erwarten ist. Massen-E-Mail bedeutet, dass der Empfänger die Nachricht nur als einer von vielen erhält.

Das Medium E-Mail wird jeden Tag von Millionen Menschen in der ganzen Welt genutzt. Kein Internet-Dienst ist erfolgreicher. E-Mail ist aus der privaten Kommunikation und dem Geschäftsleben nicht mehr wegzudenken.

Mit dem Siegeszug der E-Mail in den letzten zehn Jahren ging aber eine steigende Zahl von Missbrauchsfällen einher. Was als kleines Ärgernis begann, ist heute ein großes und sehr teures Problem, das die Verfügbarkeit dieses Dienstes gefährdet. Werbemail und andere unerwünschte E-Mails, kurz „Spam“, kosten jeden einzelnen Zeit und die Gesellschaft jedes Jahr viele Milliarden Euro. Das tägliche Spam-Aufkommen hat die Zahl der erwünschten E-Mails bei weitem überschritten; manche Studien schätzen bereits, dass 90% des Mailaufkommens im Internet aus Spam besteht. Zum Versand von Spam werden Hunderttausende infizierter Rechner missbraucht was für sich genommen bereits ein gigantisches Sicherheitsproblem darstellt.

In den letzten Jahren hat die Internet-Gemeinde viele Verfahren entwickelt, die helfen, Spam zu vermeiden oder zumindest den Empfänger davor zu schützen. Umfangreiche Filtersysteme untersuchen eingehende E-Mails und trennen Unerwünschtes von Erwünschtem. Die Kosten dafür sind enorm, aber ohne Maßnahmen gegen Spam wäre E-Mail für viele nicht mehr nutzbar.

Wegen der Komplexität des weltweiten Mailsystems und der immer neuen Tricks der Spammer gibt es eine große Anzahl sehr verschiedener Antispam-Maßnahmen. Es ist daher nicht leicht, die Funktion und Effizienz der Verfahren und ihre Vor- und Nachteile einzuschätzen. Die Studie „Antispam-Strategie“ des BSI [Anti-SPAM] hat vor allem das Ziel, technische Maßnahmen gegen Spam in ihrer ganzen Bandbreite ausführlich zu beschreiben, um eine Entscheidungshilfe für Auswahl und Einsatz eines oder mehrerer Verfahren zu geben.

Im Folgenden werden die gebräuchlichsten Antispam-Maßnahmen kurz beschrieben.

3.2.5.1 Whitelist

Liste mit Mailadressen oder IP-Adressen, von denen auf jeden Fall E-Mail angenommen werden soll. Im weiteren Sinne kann eine Whitelist auch Einträge enthalten, für die eine weniger strikte Filterung notwendig ist. Gegenteil: Blacklist.

3.2.5.2 Blacklist

Unter Blacklisting wird ein Verfahren zur Ausgrenzung bestimmter Objekte aus einer Gruppe unter Nutzung einer Datenbank verstanden. Dazu werden die Objekte anhand eines Identifizierungsmerkmals mit einer Liste von Objekten auf Übereinstimmung verglichen. Verwendung findet diese Technik bei der Ausgrenzung nicht gewünschter Teilnehmer im Rahmen der Bereitstellung von Diensten wie beispielsweise der E-Mail Kommunikation. Blacklists werden in der Regel zusammen mit einer sogen. Whitelist verwendet. Eine Whitelist ist die logische Umkeh-

rung einer Blacklist und ermöglicht eine Positiv-Auswahl von Objekten einer Gruppe. Das Verfahren des Blacklistings findet in vielen verschiedenen Bereichen Verwendung, z.B. bei der Bonitätsprüfung im Kreditwesen oder zur Sperrung von gestohlenen Mobiltelefonen im Mobilfunkbereich. Im Anti-Spam Sektor findet das Blacklisting Verfahren vor allem als IP-Blacklisting Verwendung. Desweiteren existieren u.a. Hash-Blacklists, URI-Blacklist und Right-Hand-Side Blackhole Lists.

3.2.5.3 URI-Blacklist

Eine URI-Blacklist (URIBL) dient der Speicherung von in Spam-Nachrichten vorkommenden Uniform Resource Identifier (URI). Kommerzieller Spam enthält in vielen Fällen einen Link auf eine Webseite, um dem Empfänger die Möglichkeit zu bieten, die beworbenen Produkte bestellen zu können. Diese, auch Uniform Resource Identifier genannten Links werden in URI-Blacklists zur Identifizierung von Spam gespeichert. Enthält eine E-Mail einen in der Blacklist aufgeführten URI, kann dies auf Spam hinweisen.

3.2.5.4 IP-Blacklist

Unter dem Begriff IP-Blacklisting wird der Abgleich von IP-Adressen E-Mail versendender MTAs (Message Transfer Agents) mit in Datenbanken gespeicherten IP-Adressen von Spam-Versendern und nicht für den Mail-Versand vorgesehenen Systemen verstanden. Ziel dabei ist es, potentielle Spam-versendende Mail-Server als solche vor der Übermittlung der E-Mail zu erkennen und somit eine Annahme zu verweigern. Zur Ermittlung der in einer IP-Blacklist aufgeführten IP-Adressen werden u.a. Erfahrungswerte bezüglich des Sendeverhaltens verschiedener Mail-Lieferanten sowie selbst bereitgestellte Informationen von Internet Service Providern über ihre Netzstruktur herangezogen. Gespeichert werden diese IP-Adressen in Datenbanken bzw. Listen in der Regel als einzelne IP-Adressen in punktiert dezimaler Schreibweise und/oder Netzbereichen im CIDR-Format.

3.2.5.5 Hash-Blacklist

In einer Hash-Blacklist werden Hash-Werte von Spam-Nachrichten aufgeführt. Zu als Spam identifizierten E-Mail Nachrichten wird unter Verwendung einer Hashfunktion ein der E-Mail zuzuordnender Hash-Wert berechnet. Inhaltsbasierte Spam-Analysen verwenden solche entsprechenden Hash-Werte zur Identifizierung von Spam. Hash-Blacklists ermöglichen daher die Verbreitung von Identifikationswerten zu bekanntem Spam.

3.2.5.6 Right-Hand-Side-Blacklist

Right-Hand-Side-Blacklists (RHSBL) dienen der Speicherung des Domain-Teils von im Envelope einer E-Mail enthaltenen Absender- und Empfängeradressen. Der Name dieser Blacklist-Variante lässt sich darauf zurück führen, dass der Domain-Teil einer Adresse rechts vom „@"-Zeichen steht. Ziel ist es, Spam-Nachrichten durch den Vergleich dieser Domain Angaben mit Angaben von in der Vergangenheit als Spam identifzierter E-Mail Nachrichten als solche zu erkennen, um somit den Empfang der E-Mail zu verweigern.

3.2.5.7 DNSBL

Für einen schnellen und einfachen Zugriff auf die Listen wurde das Domain Name System zweckentfremdet. Über eine bestimmte DNS-Anfrage kann man feststellen, ob eine IP-Adresse unter Spamverdacht steht oder nicht. Mit der Zeit haben sich immer mehr Listen etabliert, die alle die gleiche zugrunde liegende DNS-Technik benutzen, sich aber darin unterscheiden, welche IP-Adressen sie aufnehmen. Als Oberbegriff für all diese Listen dient der Name DNSBL (Domain Name System Blacklist / Blackhole List / Blocklist / Blocking List).

3.2.5.8 SPF/DKIM

Es gibt verschiedene Ansätze, um zu erkennen, dass eine E-Mail von einem legitimen Mail Server versendet wurde. Das Sender Policy Framework (SPF) ermöglicht dies an Hand eines zusätzlichen DNS-Eintrags fuer die Absenderdomäne, der angibt, welche Server E-Mails fuer diese Domäne versenden düerfen. DomainKeys Identified Mail (DKIM) versieht die ausgehenden E-Mails mit einer Signatur des Absendeservers, die mit Hilfe entsprechender DNS-Einträge verifiziert werden kann.

Beide Verfahren können verwendet werden, um mit ihnen korrekt gekennzeichnete E-Mails als Nicht-Spam zu erkennen (White-List). Da SPF und DKIM nicht verpflichtend sind, sind in der Regel aber nicht alle ungekennzeichneten E-Mails als Spam zu sehen.

3.2.5.9 Greylisting

Beim Greylisting weist der Mailserver des Empfängers eine eingehende E-Mail mit einer temporären Fehlermeldung versehen zunächst zurück. Gleichzeitig vermerkt er in einer Datenbank Absenderadresse, Empfängeradresse und IP-Adresse des absendenden Rechners und versieht den Eintrag mit einem Zeitstempel und einer Gültigkeitsdauer. Auf die temporäre Zurückweisung reagiert der Mailserver des Absenders innerhalb eines definierten Zeitraumes mit einem erneuten Zustellversuch. Geht dieselbe E-Mail innerhalb der in der Datenbank des Mailservers des Empfängers eingetragenen Gültigkeitsdauer erneut ein, wird sie nunmehr dem Empfänger zugestellt. Die Eintragung in der Datenbank wird dann als „zulässige Kommunikati-

onsbeziehung“ markiert und mit einem Gültigkeitsstempel/Ablaufdatum versehen. Während dieser Zeit werden E-Mails mit den gleichen Merkmalen als zulässig angesehen und ohne Zeitverzögerung zugestellt. Dabei wird der Gültigkeitszeitraum jeweils verlängert. Eine Zeitverzögerung tritt also nur am Beginn der Kommunikationsbeziehung auf. Da die Spam-Software in der Regel nach einer temporären Zurückweisung keinen erneuten Zustellungsversuch veranlasst, kann auf diese Weise Spam-Mail abgewehrt werden.

4. Grundschutzmaßnahmen

Zur Bewertung der erforderlichen Schutzmaßnahmen wird hier auf das Grundschutz-Modell des BSI [BSI GS] zurückgegriffen. Dieses Modell bietet auch aus Sicht des Datenschutzes eine Reihe von Vorteilen:

- Es spiegelt die gesetzliche Anforderung wider, nur solche Maßnahmen treffen zu müssen, deren Aufwand in einem angemessenen Verhältnis zum Schutzzweck steht. Die über den Grundschutz hinausgehenden Anforderungen werden in Kapitel 5 erörtert.
- Es handelt sich um einen mittlerweile auch international anerkannten Maßstab für IT-Sicherheit, der eine aufwändige Diskussion über die Erforderlichkeit einzelner Maßnahmen erübrigt.
- Durch die stetige Fortschreibung seitens des BSI ist sichergestellt, dass auch neue Erkenntnisse und aktuelle technische Entwicklungen berücksichtigt werden.

Auch wenn sich diese Orientierungshilfe auf die Absicherung der Internetverbindung konzentriert, soll an dieser Stelle betont werden, dass ein Grundschutzniveau für diesen Aspekt nicht sinnvoll isoliert von einer Gesamtbetrachtung erreicht werden kann. Hierzu sei auf den BSI-Standard 100-2 [BSI 100-2] verweisen.

4.1 Schutzbedarf

Die IT-Grundschutz-Kataloge sind für Situationen mit normalem Schutzbedarf in den Kategorien Vertraulichkeit, Integrität und Verfügbarkeit konzipiert. Bezogen auf personenbezogene Daten bedeutet dies, dass das Überwinden oder Versagen technisch-organisatorischer Maßnahmen nur zu geringfügigen Beeinträchtigungen des informationellen Selbstbestimmungsrechts führen darf. Im Gegensatz hierzu steht die Verarbeitung sensibler Daten (siehe 5.1), die regelmäßig Maßnahmen erfordert, die über das Grundschutzniveau hinausgehen.

4.2 Empfehlungen

4.2.1 Virenschutz

Um den Grundbedrohungen der Internetnutzung am Arbeitsplatz begegnen zu können, ist der Einsatz eines Virenschutzprogramms unverzichtbar. Dabei sind folgende Aspekte besonders relevant:

- Erkennungsspektrum – Die Software sollte möglichst alle bekannte Formen von Schadsoftware bekämpfen können, seien es Viren, Würmer, Trojanische Pferde oder andere unliebsame Programme.
- Flexibilität – Eine Anpassung auf die spezifischen Schutzbedürfnisse sollte durch entsprechende Einstellungen möglich sein. Dabei sollte auch festgelegt werden können, welche Einstellungen nur Administratoren zugänglich sind, um eine (versehentliche) Veränderung durch den Nutzer zu verhindern.
- Stand der Technik – Das Programm sollte regelmäßig fortentwickelt werden, um auch mit Bedrohungen durch neue Schadsoftware umgehen zu können.
- Aktualität – Neue Programm- und Signaturstände sollten ohne Zeitverlust eingepflegt werden. Hierfür sind ein automatischer Updatedienst sowie eine zentrale Updatekontrolle entscheidende Faktoren.

Mindestens ebenso wichtig ist die Frage der mit dem Virenschutz verbundenen Prozesse. Ein Virenvorfall muss zu einer möglichst automatischen Meldung bei einer dafür verantwortlichen Stelle führen. Diese muss den Vorfall bewerten und ggf. weitere Maßnahmen einleiten. Um aus einzelnen Ereignissen Muster größerer Attacken erkennen zu können, sollte diese Stelle möglichst zentral in einer Organisation eingebunden sein.

Weitere Hinweise können den Grundschutzkatalogen entnommen werden ([BSI GS], „M 4.3 Regelmäßiger Einsatz eines Anti-Viren-Programms“).

4.2.2 Patchmanagement

Bekannte und vom Softwarehersteller behobene Softwarefehler, insbesondere Sicherheitslücken, sollten umgehend und einheitlich beseitigt werden, indem entsprechende Updates oder Patches installiert werden. Viele Sicherheitsvorfälle gehen auf nicht ausreichend gepatchte Software zurück, wobei Angriffsmöglichkeiten ausgenutzt werden, die in aktualisierten Versionen nicht mehr zur Verfügung stehen.

4.2.3 Personal Firewall

Eine Firewall auf Clientebene kann als Grundschutzmaßnahme gegen eine Reihe von Risiken schützen. Neben die Kontrolle der Zugriffe von außen tritt dabei wesentlich auch die Begrenzung der Zugriffe vom Client ins Internet bzw. das vorgelagerte Intranet. Solche Zugriffe können schlicht unerwünscht sein, etwa wenn Programme ungefragt Kontakt mit Servern des Herstellers aufnehmen (sog. „nach Hause telefonieren“), oder sie resultieren von Schadprogrammen wie Trojanischen Pferden oder Bots, die ein Sicherheitsproblem darstellen.

Weitere Informationen enthalten die Grundschutzkataloge ([BSI GS], „M 5.91 Einsatz von Personal Firewalls für Internet-PCs“).

4.3 Anforderungen an Service-Provider

Im Zuge der voranschreitenden Zentralisierung von IT-Dienstleistungen auch im öffentlichen Sektor wird der Internet-Zugang zunehmend nicht mehr von einzelnen Dienststellen eigenständig organisiert und administriert, sondern durch einen Service-Provider auf kommunaler oder Landesebene realisiert.

Gerade Sicherheitserwägungen spielen bei dieser Entscheidung eine wichtige Rolle. Denn der Aufwand für eine sichere Internetanbindung kann an einer Stelle gebündelt besser getragen, Spezialwissen kann leichter verfügbar gehalten und auf Sicherheitsvorfälle schneller reagiert werden. Dennoch bleibt auch beim Outsourcing aus Datenschutz- ebenso wie aus Grundschutzsicht die einzelne verantwortliche Stelle für die Gewährleistung der Datensicherheit zuständig. Diese Zuständigkeit schlägt sich vor allem in organisatorischen Maßnahmen nieder, wie etwa die sorgfältige Auswahl und Kontrolle des Dienstleisters und die schriftliche Auftragsvergabe.

Diese Orientierungshilfe kann daher auch dazu dienen, Anforderungen an zentrale Dienstleister zu formulieren und diese z.B. in Form eines Grundschutzzertifikats oder anderer belegbarer Sicherheitsmaßnahmen abzufragen.

Zum Thema Outsourcing aus Grundschutzsicht siehe auch [BSI GS], „B 1.11 Outsourcing“.

5. Zusatzmaßnahmen bei der Verarbeitung sensibler Daten

5.1 Sensible Daten

Die steigende Attraktivität des Internet führt in zunehmendem Maße dazu, dass auch solche Bereiche einen Internet-Anschluss erhalten, in denen sensible personenbezogene Daten verarbeitet werden (z.B. Gesundheits- oder Personaldaten). Dies kann entweder im Zuge einer Strategie erfolgen, bei der das Internet als allgemeines Informationsmedium bedarfsunabhängig jedem Mitarbeiter zur Verfügung gestellt wird oder aber aus einer konkreten Bedarfsermittlung, die etwa im Gesundheitsbereich die Erforderlichkeit einer medizinisch-fachlichen Recherche ergibt. Ggf. kommen auch Systeme zum Einsatz, auf denen sehr sensible oder aber dem Geheimschutz unterliegende Daten gespeichert und verarbeitet werden. Hierbei ist je nach Schutzbedarf zu entscheiden, ob diese Daten nur auf einem Stand-Alone System ohne jeglichen Netzzugang verarbeitet werden oder aber ob hier etwa besondere Techniken zur Absicherung, wie etwa der terminalbasierte Zugang zum Internet, zum Einsatz kommen darf. In diesem Kapitel wird erläutert, inwieweit die in den vorangehenden Kapiteln dargestellten Maßnahmen ausreichen, um auch in solchen Fällen einen datenschutzgerechten Betrieb zu gewährleisten, welche konkreten Risiken bei Betrieb einer Firewall weiterhin bestehen und welche Zusatzmaßnahmen getroffen werden sollten, um diesen Risiken zu begegnen.

5.2 Schutzniveau von Firewalls

Einzelne Firewalls wie auch sogenannte Personal- oder Desktop-Firewalls, die den Datenverkehr einzelner PCs auf dem sie läuft und dem Netz filtern, bieten eine Reihe von Möglichkeiten, um den Datenverkehr in das und aus dem Internet zu kontrollieren und damit das Schutzniveau gegenüber einem direkten Anschluss wesentlich zu erhöhen. Dazu gehören:

- Begrenzung des Zugangs zum Internet auf einen einzigen kontrollierbaren Punkt
- Begrenzung der zugelassenen Dienste auf das Erforderliche
- Begrenzung der Internet-Nutzung auf bestimmte Stationen oder Benutzer
- Verbergen der lokalen IP-Adressen
- Verhindern eines Verbindungsaufbaus aus dem Internet nach innen
- Ausschluss bestimmter Internet-Server oder -Domains
- Ausschluss aktiver Inhalte wie Java oder ActiveX
- Kontrolle auf schädliche Inhalte wie Viren oder Trojanische Pferde

- Protokollierung von Angriffsversuchen

Ein gut konfiguriertes und administriertes Firewall-System kann daher die Gefahren, die beispielsweise durch Trojanische Pferde wie „Back Orifice“ oder „NetBus“ entstehen, wirkungsvoll begrenzen. Dennoch können auch große und mit erheblichem Aufwand betriebene Firewall-Installationen nicht gegen sämtliche Gefahren aus dem Internet schützen; dies zeigen Vorfälle wie die Verbreitung der E-Mail-Würmer „Iloveyou“ oder „Melissa“. Diese Ereignisse belegen grundsätzliche Aspekte von Firewalls:

- Jeder Kommunikationskanal, der eröffnet wird, um einen gewünschten Datenaustausch zu ermöglichen, kann auch missbraucht werden. Ein Firewall-System hat im Rahmen des Zugelassenen keine Möglichkeit, zwischen Gebrauch und Missbrauch eines Kommunikationskanals zu unterscheiden. Dies können sich Angreifer zunutze machen.
- Die zunehmende Tendenz, Daten (passive Inhalte) und Programme (aktive Inhalte) zu koppeln, indem Standardanwendungen oder das ganze Betriebssystem skriptfähig gemacht werden, führt zu immer weiteren Schwierigkeiten, den lokalen Betrieb eines PC zu kontrollieren. Neben Makros und Skripten führen auch Browser-basierte Technologien wie Java oder ActiveX immer wieder zu Problemen.
- Virenscanner, zentral oder dezentral, können nur auf bereits bekannte Schadenssoftware reagieren. Bei den rapiden Ausbreitungsgeschwindigkeiten, die das Internet für Schadenssoftware bietet, kommen Updates mitunter zu spät, um den Schaden wirkungsvoll zu begrenzen.

5.3 Kommunikationsverbindungen als verdeckte Kanäle

Da die Anbindung an das Internet zum Ziel hat, eine Kommunikation mit anderen Rechnern außerhalb des internen Netzes zu ermöglichen, muss selbst eine sehr restriktiv konfigurierte Firewall eine bestimmte Menge von Datenaustausch zwischen dem internen und dem externen Bereich zulassen. Sowohl der Kommunikationsbedarf als auch die zugrunde liegende Technik des Internet machen es dabei unumgänglich, dass Daten nicht nur in den internen Bereich hineinfließen, sondern auch aus diesem herausgelangen – und sei es nur in Form von Steuerungsinformationen an einen Web-Server.

Dies kann bereits genügen, um einen weitgehenden Angriff auf den geschützten Bereich hinter einer Firewall durchzuführen. So kann etwa das HTTP-Protokoll, das zum Zugriff auf das WWW verwendet wird, missbraucht werden, um – mittels eines entsprechenden Trojanischen Pferdes auf dem betroffenen PC – gespeicherte Daten auf einen Rechner im Internet zu übertragen, ohne dass der Benutzer dies merkt und ohne dass die Firewall dies als unzulässig erkennt. Ins-

besondere im Rahmen von sog. Web-2.0- oder Ajax-Anwendungen sind Techniken entwickelt worden, die diese Gefahren mit sich bringen (siehe [XMLHttpRequest]).

Auch der Kommunikationskanal für E-Mail könnte auf diese Weise missbraucht werden. Die erwähnten E-Mail-Würmer waren – aus Datenschutzsicht – insofern vergleichsweise harmlos, als keine schützenswerten Daten nach außen versandt wurden. Dies hätte jedoch problemlos in die entsprechenden Programme integriert werden können.

Für die Firewall ist diese Kommunikation von normalen, berechtigten Zugriffen durch den Benutzer mittels seines Browsers oder E-Mail-Programms nicht zu unterscheiden. Auch sog. Intrusion Detection Systeme (IDS), die als Zusatzkomponente von besonders aufwändigen Firewalls den laufenden Betrieb auf Unregelmäßigkeiten hin überwachen, sind kaum in der Lage, eine solche „Nutzung“ von der normalen zu unterscheiden.

Das geschilderte Angriffsszenario setzt vier Komponenten voraus:

- eine aktive lokale Komponente, d.h. ein Schadprogramm auf dem betroffenen PC,
- ein Kommunikationskanal, der auf geeignete Weise missbraucht wird,
- ein oder mehrere Kommunikationspartner im externen Netz, d.h. im Internet,
- ein lokales Schadenspotenzial, z.B. in Form gespeicherter personenbezogener Daten.

Dabei müssen alle vier Bestandteile *zur gleichen Zeit* vorliegen. Sofern es gelingt, eine dieser Voraussetzungen zu unterbinden, wird das Risiko eines Datenmissbrauchs erheblich reduziert. Zwar sind prinzipiell auch Angriffe denkbar, die diese Beschränkungen umgehen, z.B. indem die schützenswerten Daten zwischengespeichert werden und damit dauerhaft zugreifbar sind. Dies setzt jedoch eine weitgehende Kenntnis der internen Systemlandschaft voraus, über die ein externer Angreifer in der Regel nicht verfügt.

5.3.1 Beschränkung der aktiven lokalen Komponenten

Die Risiken, von trojanischen Pferden oder anderer Schadsoftware befallen zu werden, sind hinreichend bekannt. Das Internet bildet dabei heute das Hauptverbreitungsmedium, indem entweder ausführbare Programme direkt oder als Bestandteil von Dokumenten (dazu gehören z.B. auch Java-Applets) von dort aktiv oder aber per E-Mail passiv bezogen werden.

Die Schutzmechanismen dagegen sind ebenfalls vergleichsweise gut entwickelt; dazu gehören Virenscanner (zentral und dezentral), Verhindern des Downloads zumindest bestimmter Dateitypen, Begrenzung der lokal ausführbaren Programme auf bekannte Software, lokales Ausschalten von Skript- und Makrokomponenten.

Allerdings schränken diese Maßnahmen den Benutzer relativ stark ein und werden daher nach Möglichkeit umgangen. Zudem kann damit in der Regel nur bereits bekannte Schadsoftware kontrolliert werden.

5.3.2 Eingeschränkte Kommunikationskanäle

Die Risiken bestehender Kommunikationskanäle wurden bereits beschrieben. Zunächst einmal sollte die Internetanbindung daher auf die erforderlichen Dienste begrenzt werden; dies ist Bestandteil und Aufgabe jeder Firewall-Installation.

Darüber hinaus können die Risiken dadurch begrenzt werden, dass die Kommunikationskanäle nicht dauerhaft zur Verfügung stehen, sondern nur unter bestimmten Bedingungen. Beispielsweise könnte die Verbindung nur für bestimmte Benutzer zugelassen werden oder sichergestellt werden, dass die Verbindung zu einem Server mit schützenswerten Daten zuvor unterbrochen wurde. Schließlich besteht die Möglichkeit, statt den Standard-Kommunikationskanälen andere, weniger bekannte oder proprietäre Protokolle zu verwenden, die den Aufwand für einen Angriff erhöhen.

5.3.3 Begrenzung der Kommunikationspartner

Wird die Verbindung zu jedem Rechner im Internet sowie von und zu jeder E-Mail-Adresse zugelassen, besteht das Risiko, von jedem Internet-Rechner weltweit attackiert zu werden.

In vielen Fällen ist jedoch aus fachlicher Sicht nur ein begrenzter Internetzugang erforderlich. Dabei kann mit einer überschaubaren (und administrierbaren) Liste zugelassener Kommunikationspartner gearbeitet werden. Diese können daraufhin überprüft werden, ob von dort Angriffe zu erwarten sind.

Demgegenüber kann auch eine Negativliste implementiert werden, die bekannte oder vermutete Angreifer ausschließt. Dies ist jedoch in der Regel wenig effektiv, da nicht einmal annähernd bekannt ist, von welchen Stellen aus Angriffe stattfinden oder zu erwarten sind. Zudem macht die Dynamik des Internet eine sehr aufwändige Pflege erforderlich.

Zu beachten ist in jedem Fall, dass die Überprüfung auf gute oder schlechte Kommunikationspartner nur dann hilfreich ist, wenn deren Identität zweifelsfrei feststeht. Allerdings lassen sich sowohl E-Mail- als auch IP-Adressen bzw. Domainnamen fälschen. Zudem können Angriffe durchaus auch von bekannten (und ansonsten harmlosen) Kommunikationspartnern ausgehen, wie die Beispiele der E-Mail-Würmer „Melissa“ und „Iloveyou“ zeigen.

5.3.4 Verminderung des lokalen Schadenspotenzials

Der Schaden, der auf Seite des angegriffenen Systems entstehen kann, hängt aus Datenschutzsicht vor allem damit zusammen, welche personenbezogenen Daten von dort aus direkt oder indirekt zugreifbar sind.

Maßnahmen sollten daher daran ansetzen, diesen Zugriff zu begrenzen. Dies kann durch die Möglichkeiten des Betriebssystems (Dateirechte) geschehen, durch Verschlüsselung, durch die Vermeidung einer lokalen Datenhaltung, durch eine anwendungsbezogene Authentisierung etc..

5.4 Vorgeschlagene Systemkonfigurationen

Die genannten Einzelmaßnahmen müssen zu sinnvollen Gesamtkonfigurationen zusammengefasst werden. Im Folgenden werden praxiserprobte Lösungen für jeweils unterschiedliche Nutzungsprofile des Internet vorgestellt. Dabei ist teilweise auch eine Kombination der Modelle möglich, um die Sicherheit weiter zu erhöhen.

5.4.1 Proxy mit Positivliste (inhaltliche Begrenzung)

Dieses Konzept ist für solche Benutzer gedacht, die für die Erledigung ihrer fachlichen Aufgaben den Zugriff auf lediglich einen klar definierbaren und überschaubaren Ausschnitt des Internet benötigen, z.B. Arbeitsvermittlungsangebote lokaler oder regionaler Anbieter. Ein solches Nutzungsprofil ermöglicht es, die risikobehafteten Bereiche des Internet pauschal auszublenden, ohne sie im Einzelnen definieren oder bewerten zu müssen.

Technisch kann dies durch eine Kontrolle der zugelassenen Internet-Adressen oder Domainnamen auf der Firewall geschehen. Sollen mehrere verschiedene solcher Ausschnitte des Internet verwaltet werden, ist es zweckmäßig, jeweils eigene Proxys vorzusehen, die lediglich dieser Adressfilterung dienen. Dabei ist darauf zu achten, dass die Benutzer dann nur noch über den zugehörigen Proxy und nicht mehr über die Firewall auf das Internet zugreifen können, z.B. indem nur die IP-Adressen der Proxys auf der Firewall eingetragen werden.

Diese Lösung eignet sich auch für solche Fälle, bei denen ein zeitgleicher Zugriff auf personenbezogene Daten und das Internet aus fachlichen Gründen erforderlich ist.

Der Mehraufwand liegt in der Erstellung und Pflege der Positivliste sowie in der Beschaffung und dem Betrieb des Proxys.

5.4.2 Virtuelle Surf-Lösungen

Dieses Konzept kommt für solche Benutzer in Betracht, die einen hohen Schutzbedarf haben und inhaltlich unbegrenzten Zugang zum Internet benötigen. Die Idee beruht darauf, die Gleichzeitigkeit des Zugriffs auf schützenswerte Daten und auf das Internet innerhalb verschiedener virtueller Umgebungen auf einem System oder aber den Internetzugriff innerhalb eines Sandbox-Systems zu realisieren.

Solche virtuellen Systeme bildet man z.B. mit VM-Ware oder der Virtual Box ab. Dabei sollte man grundsätzlich schon aus Sicherheitserwägungen verschiedene Gast- und Host-Betriebssysteme nehmen. Empfehlenswert ist die Kombination Linux als Host-System und Windows als Gast-System. Wegen seiner guten Netzwerkeigenschaften lässt sich das Linux-System durch entsprechende Einstellungen gut gegen Angriffe aus dem Netzwerk schützen. Das Windows-System wird als virtuelles System aufgesetzt und kann bei einer Zerstörung leicht und schnell aus einer Kopie wieder betriebsbereit hergestellt werden. Damit erspart man sich eine Menge an Zeit, die typischerweise mit einer vollständigen Systeminstallation verbunden ist. (Auf handelsüblichen Maschinen beträgt die Zeit zur Wiederherstellung zwischen 5 und 10 Minuten). Im Falle der Virtual-Box kann man das Windows-System z.B. über NAT an die Host-Schnittstelle ankoppeln. Dadurch kann man das Netzwerk des Gast-Systems fast vollständig von dem des Host-Systems trennen. Ein Übergang von Daten aus dem Host-Netz zum Gast-Netz wird damit verhindert. Das Gast-System mit NAT-Anschluss arbeitet wie ein normales System, dass über einen Router angeschlossen ist. Der Router wird jedoch vom Host-System gebildet. In der vorgeschlagenen Konfiguration hat man damit ein mächtiges Werkzeug in der Hand, um den Internet-Trafic zum Gast-System hin zu kontrollieren. Für das Gast-System stehen jedoch alle Funktionen zur Verfügung. Wegen seiner schnellen Wiederherstellbarkeit kann es sogar als „Opfersystem“ betrieben werden (Honey-Pot-Technik). Die Virtualisierung geht im Falle der Virtual Box sehr weit. So werden beispielsweise auch CD/DVD-Laufwerke, USB-Anschlüsse und Sound-Karte des Host-Systems durch das Gast-System gesteuert. Damit sind dann z.B. auch geschützt Downloads und Speichern der Daten auch auf externen Datenträgern möglich. Schwierigkeiten bei virtuellen Lösungen bereiten eigentlich nur hochauflösende Grafikkarten. Diese werden zurzeit nicht unterstützt, da die Virtualisierung auf einem „normierten“ Hardwaremodell aufsetzt. Daher ist es z.B. auch möglich, eine installierte virtuelle Maschine von einer Hardware auf eine andere zu kopieren und zu betreiben.

5.4.3 Grafischer Internetzugang (logische Systemtrennung)

Diese Lösung ist für solche Benutzer geeignet, die eine weder inhaltlich noch zeitlich begrenzbare Internet-Nutzung benötigen. Die Idee beruht darauf, den PC lediglich als Fenster ins Internet zu nutzen. Per Terminal-Emulation wird auf einen Browser oder ein E-Mail-System auf ei-

nem anderen Gerät (Terminal-Server) zugegriffen, auf dem keine schützenswerten Daten verarbeitet werden. Nur der Terminal-Server benötigt einen Internet-Zugang, während der Arbeitsplatz-PC, obwohl in das interne Netz integriert, keinen direkten Kontakt zum Internet oder zur Firewall benötigt. Schadenssoftware kann daher nur an dem Terminal-Server ansetzen, wovon jedoch keine schützenswerten Daten betroffen sind. Beispielprodukte sind VNC [VNC] oder der Windows Terminal Server.

Der Mehraufwand für diese Lösung besteht zum einen in dem zusätzlichen Gerät für den Internet-Zugang und zum anderen in der erhöhten Netzlast und Reaktionszeit, die die Übertragung der Bildschirminhalte zwischen Terminal-Server und Arbeitsplatz-PC mit sich bringt. Zudem kann der Benutzer heruntergeladene Dokumente oder empfangene E-Mails zwar öffnen und betrachten sowie ggf. drucken, jedoch nicht auf seinen eigenen PC übertragen. Dies erfordert einen Austausch über Datenträger oder andere gesicherte Wege.

Prinzipiell kann auf diesem Weg auch Schadenssoftware importiert werden, die sich anschließend sowohl den Kommunikationskanal für die Terminalverbindung als auch den Kommunikationskanal für die Internet-Verbindung zunutze macht. Hierzu müssten allerdings lokale Komponenten auf dem Internet-Gerät und auf dem Terminal-PC installiert werden sowie das verwendete Protokoll für die Terminalverbindung missbraucht werden. Dies stellt eine erheblich höhere Hürde für einen Angreifer dar, insbesondere wenn die interne Systemkonfiguration nicht bekannt ist.

5.4.4 Stand-alone-System (physikalische Systemtrennung)

Diese rigideste Lösung ist für all die Fälle geeignet, in denen die verbleibenden Restrisiken der vorgenannten Modelle als zu hoch eingeschätzt werden.

Eine vollständige Systemtrennung zwischen Internet und der Verarbeitung schützenswerter Daten schützt die Vertraulichkeit dieser Daten optimal. Allerdings ist der Aufwand sowohl finanzieller als auch organisatorischer Art u.U. erheblich. Bei einer nur sporadischen Internet-Nutzung genügt ein einzelner Internet-PC für mehrere Mitarbeiter. Eine extensive Nutzung setzt jedoch jeweils ein Zweitgerät am Arbeitsplatz voraus.

Zu beachten ist dabei, dass auch bei einer vollständigen systemischen Trennung durch verschiedene Geräte bzw. Netze häufig gleichwohl der Bedarf besteht, Daten zwischen diesen Bereichen auszutauschen, z.B. ein Dokument, das im geschützten Netz erstellt wurde, per E-Mail zu versenden. Dies kann per Datenträger (USB-Stick o.ä.) geschehen. Auch auf diesem Weg kann Schadsoftware importiert werden, diese kann jedoch ausschließlich Effekte im lokalen Bereich erzielen.

5.5 Virtuelle Poststelle (VPS) als weitere Maßnahme

Die sogenannte virtuelle Poststelle ermöglicht durch serverbasierte Bereitstellung kryptografischer Funktionen das transparente Versenden verschlüsselter E-Mail. Sie übernimmt hierbei die Aufgaben des Verschlüsselns und Signierens abgehender sowie das Entschlüsseln und die Signaturüberprüfung eingehender E-Mail als zentraler Server-Dienst. Es können auch interne Zeitstempel erstellt und externe eingeholt werden um Ein- und Ausgang von E-Mail revisionssicher zu protokollieren. Der auf einem zentralen Server bereitgestellte Dienst kann Authentifizierungsverfahren und die Weiterleitung mit Vertretungsregelung (auch bei Verschlüsselung) durchführen. Entschlüsselte Inhalte können an einen zentralen Virenscanner zur Contentprüfung weitergegeben werden. Erste Versionen einer virtuellen Poststelle sind aus dem Projekt BundOnline 2005 hervorgegangen. Diese bietet Komponenten für zentrale Dienste basierend auf dem Produkt Governikus und der Mail-Komponenten JULIA MailOffice. Wird eine virtuelle Poststelle eingesetzt, so ist der Austausch verschlüsselter E-Mail unabhängig vom verwendeten Mailclient und Betriebssystem sichergestellt. Weitere Informationen hierzu siehe [BSI VP].

6. Zulässigkeit von Protokollierung und Inhaltskontrolle mittels einer Firewall

6.1 Allgemeines

Firewalls sind selbst keine eigenständigen Telekommunikationsdienste oder Telemedien, sondern als unselbständiger Bestandteil eines solchen Dienstes zu betrachten. Daher kommt für den Betrieb einer Firewall das Datenschutzrecht zur Anwendung, das auch für den zu Grunde liegenden Dienst gilt. Deshalb sollen im Folgenden kurz die Anwendungsbereiche der für die Dienste einschlägigen Datenschutzvorschriften erläutert werden.

Das Verhältnis zwischen Telekommunikationsdiensten einerseits und Telemedien andererseits wird grundsätzlich durch die in § 1 Abs. 1 Telemediengesetz (TMG) enthaltene Begriffsabgrenzung beschrieben. Danach sind Telemedien alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht

- Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen,
- telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder
- Rundfunk nach § 2 des Rundfunkstaatsvertrages sind.

Telemedien liegt in der Regel eine **Übermittlung mittels Telekommunikation** zu Grunde. Telekommunikation ist hingegen nach der Definition des Telekommunikationsgesetzes (§ 3 Nr. 22 TKG) der reine Übertragungsvorgang, d. h. der technische Vorgang des Aussendens, Übermitteln und Empfangens von Signalen mittels Telekommunikationsanlagen.

Ausgehend von diesen gesetzgeberischen Vorgaben kann die Beziehung zwischen Telekommunikationsdiensten und Telemedien durch ein Schichtenmodell beschrieben werden. Dabei stellt die Telekommunikation die Transportebene dar, auf deren technischer Basis die jeweiligen Telemedien erbracht werden. Das hierfür maßgebliche datenschutzrechtliche Rechtsregime wird durch die einschlägigen Vorschriften des Telekommunikationsgesetzes (TKG) bestimmt. Soweit es nicht die Datenverarbeitungsbefugnisse im Verhältnis zwischen Anbieter und Nutzer betrifft, können zusätzlich die Regelungen des allgemeinen Datenschutzrechts (Bundesdatenschutzgesetz, Landesdatenschutzgesetze) greifen.

Um im Bild zu bleiben, handelt es sich bei den Telemedien demgegenüber um die Transportbehälter. Für diesen Bereich sind das Telemediengesetz (TMG) sowie der Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag – RStV) einschlägig. Zu beachten ist, dass ge-

mäß § 11 Abs. 3 TMG für Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, überwiegend die datenschutzrechtlichen Regelungen des TKG und zusätzlich die §§ 12 Abs. 3, 15 Abs. 8 und 16 Abs. 2 Nr. 2 und 5 TMG gelten. Unter die Regelung des § 11 Abs. 3 TMG fallen nach der Gesetzesbegründung z. B. der Zugang zum Internet, das Angebot von E-Mail-Kommunikation oder die Internet-Telefonie (Voice over IP).

Schließlich muss noch eine dritte Ebene betrachtet werden, nämlich die durch bzw. mit den Telemedien vermittelten – also in diesen Transportbehältern befindlichen – Inhalte. Die rechtliche Bewertung der Inhalte richtet sich nach den jeweiligen Gesetzen, die auch offline anzuwenden wären, also etwa den Verwaltungsverfahrensgesetzen, dem Strafgesetzbuch, dem Gesetz gegen den unlauteren Wettbewerb, dem BDSG oder den Landesdatenschutzgesetzen.

Die Verarbeitung und Nutzung personenbezogener Daten auf der Transportebene wird in Umfang und Grenzen maßgeblich durch das Fernmeldegeheimnis (Art. 10 GG, § 88 TKG) geprägt, das die dabei anfallenden Verkehrsdaten und die Kommunikationsinhalte schützt. Nach § 88 Abs. 2 TKG sind alle Diensteanbieter zur Wahrung des Fernmeldegeheimnisses verpflichtet. Entsprechend den einschlägigen Begriffsbestimmungen in § 3 TKG ist es dabei unerheblich, ob diese Dienste für die Allgemeinheit bestimmt sind oder nur einem bestimmten Kreis von Berechtigten, z. B. in einer geschlossenen Benutzergruppe angeboten werden. Ohne Bedeutung ist auch, ob Telekommunikationsdienste mit oder ohne Gewinnerzielungsabsicht erbracht werden. Durch diesen weiten Anwendungsbereich soll ein umfassender Schutz des Fernmeldegeheimnisses gewährleistet werden. Vor diesem Hintergrund muss beispielsweise auch eine Behörde, die ihren Mitarbeitern die private Nutzung der vorhandenen Telekommunikationsanlage erlaubt, als Telekommunikationsdiensteanbieter mit all den sich daraus ergebenden Verpflichtungen beurteilt werden.

Auch die bei Telemedien entstehenden Nutzungsdaten unterliegen dem Schutz durch das Fernmeldegeheimnis, weil diese Dienste definitionsgemäß auf Grundlage der Telekommunikation abgewickelt werden und ihrerseits Inhalt der Telekommunikation sind.

Bei der Protokollierung sind deshalb sowohl die Bestimmungen des TKG und des TMG bzw. des RStV, als auch das Fernmeldegeheimnis und ggf. einschlägige Bestimmungen über kommunizierte Inhalte (z. B. Arzt- oder Sozialgeheimnis) zu beachten.

Betroffen von einer Protokollierung durch Firewalls sind in erster Linie die Bediensteten oder Arbeitnehmer der Stelle, deren Datenverarbeitungsanlage von der Firewall geschützt werden soll, im Fall der E-Mail-Kommunikation und bei interaktiven Angeboten aber auch die externen Kommunikationspartner. Bei Angriffen auf die Firewall können zudem personenbezogene Daten der Angreifer registriert werden.

Hinsichtlich des Umfangs und der Zulässigkeit der Protokollierung von Zugriffen, die über eine Firewall erfolgen, und der Kontrolle von Inhaltsdaten lassen sich folgende Fallkonstellationen unterscheiden:

6.2 Kontrolle von Inhaltsdaten bei E-Mail-Kommunikation

Die Frage nach der Zulässigkeit der Kontrolle von Inhaltsdaten wird insbesondere relevant bei eingehenden E-Mails, die nicht an die Mail-Adresse einer zentralen Poststelle, sondern an die Mail-Accounts einzelner Arbeitnehmer der betreffenden Dienststelle gerichtet sind. Hierbei können folgende Fallkonstellationen unterschieden werden:

6.2.1 Kontrolle auf Virenbefall mittels automatischem Virencheck

Sowohl bei dienstlicher als auch bei privater Nutzung bestehen grundsätzlich gegen eine Kontrolle auf Virenbefall mittels automatischem Virencheck keine Bedenken, soweit die Kontrolle ausschließlich automatisch erfolgt und die Kenntnisnahme von den Inhalten privater E-Mails durch Vertreter der Dienststelle (z. B. den Systemadministrator) nicht ohne Einwilligung des Benutzers erfolgt.

Dadurch kann allerdings eine dezentrale Überprüfung der Dateien auf Viren nicht bzw. nicht vollständig ersetzt werden, da Virencheckprogramme Viren, die in verschlüsselten E-Mails enthalten sind, nicht erkennen können. Mindestens für diese E-Mails muss daher nach der Entschlüsselung eine Virenüberprüfung beim Benutzer selbst erfolgen.

6.2.2 Kontrolle eingehender dienstlicher E-Mails

Wie bei herkömmlicher Post können Vorgesetzte sich auch eingegangene dienstliche E-Mails von den betreffenden Mitarbeitern vorlegen lassen. Der Arbeitnehmer hat auf Verlangen dem Arbeitgeber Ausdrucke der E-Mails auszuhändigen bzw. diesem den Zugang zu den E-Mails zu ermöglichen.

6.2.3 Kontrolle eingehender privater E-Mails

Soweit die private Nutzung des E-Mail-Dienstes gestattet ist, ist der Arbeitgeber als Anbieter von Telekommunikationsdiensten einzuordnen bzw. gemäß § 11 Abs. 3 TMG als solcher zu behandeln und unterliegt damit in Bezug auf die Protokollierung den Vorschriften des Telekommunikationsgesetzes (TKG) über die Verarbeitung personenbezogener Daten. Im Hinblick auf den Inhalt der privaten E-Mails der Beschäftigten hat er auch das Fernmeldegeheimnis nach § 88 TKG zu wahren. Daraus folgt insbesondere, dass es ihm untersagt ist, sich oder anderen über das für die Erbringung des Dienstes erforderliche Maß hinaus Kenntnis vom Inhalt oder

den näheren Umständen der Telekommunikation zu verschaffen. Die Weitergabe von Informationen, die dem Fernmeldegeheimnis unterliegen, ist strafbewehrt.

Wenn die private Nutzung von E-Mail zugelassen wird, ergibt sich die Notwendigkeit, dienstliche und private E-Mails zu trennen. Hat der Mitarbeiter eine personalisierte E-Mail-Adresse nach dem Muster „Vorname.Name@Behörde.de“, so kann nicht ausgeschlossen werden, dass eingehende Mails nicht an die Behörde, sondern an den Mitarbeiter privat gerichtet sind. Dieses Problem kann dadurch gelöst werden, dass den Beschäftigten für die dienstliche und die private Benutzung von E-Mail verschiedene E-Mail-Adressen zugewiesen werden. Denkbar ist auch, die private Nutzung des dienstlichen E-Mail-Kontos zu untersagen und die Bediensteten bei erlaubter privater Nutzung des WWW auf die Nutzung von Webmail-Angeboten zu verweisen, siehe [DSK-OHA].

Unabhängig vom Aufbau und der Differenzierung der E-Mail-Adressen einer Behörde gilt, dass private E-Mails, die beim Posteingang fälschlich zunächst als dienstliche E-Mails angesehen wurden, so zu behandeln sind, wie bei der Behörde eingegangene, für einen Mitarbeiter bestimmte private Schreiben, deren privater Charakter nicht besonders, etwa durch den Zusatz „persönlich“ gekennzeichnet ist. Sobald der private Charakter dieser E-Mails erkannt wurde, sind sie unverzüglich dem betreffenden Mitarbeiter zur alleinigen Kenntnis zu geben.

6.2.4 Kontrolle ausgehender E-Mails

Auch bei ausgehenden E-Mails kann die automatische Kontrolle auf Virenbefall sinnvoll sein. Zwar träfe der Schaden hier den Empfänger, dies kann allerdings eine Rufschädigung der absendenden Stelle zur Folge haben. Ausgehende private E-Mails sind genauso vom Fernmeldegeheimnis geschützt wie die eingehenden, so dass die inhaltliche Überprüfung ausscheidet.

Hinsichtlich ausgehender dienstlicher E-Mails gilt grundsätzlich das oben zu den eingehenden dienstlichen E-Mails Gesagte entsprechend. Die Vertreter der Dienststelle müssen feststellen können, welche Inhalte in dienstlichen E-Mails nach außen gelangt sind. Die Kontrolle der Inhalte durch die Vorgesetzten ist daher ohne weiteres zulässig. Darüber hinausgehend wäre es technisch durch den Einsatz entsprechender Auswertungsprogramme auch möglich, z. B. anhand der Absendezeiten und Länge der E-Mails oder mit der gezielten automatischen Suche nach darin verwendeten Begriffen eine umfassende Leistungs- und Verhaltenskontrolle zu bewirken. Der Einsatz derartiger Programme stellt allerdings einen weitgehenden Eingriff in das Persönlichkeitsrecht der Beschäftigten dar und ist daher lediglich in Ausnahmefällen und auch dann nur aufgrund einer Dienstvereinbarung zulässig.

6.3 Protokollierung von Internet-Zugriffen mittels einer Firewall

Für Art und Umfang der Protokollierung lassen sich vor allem zwei Szenarien unterscheiden:

- Die Firewall dient lediglich der Abschottung des internen Netzes gegen das Internet, Zugriffe von außen sind grundsätzlich nicht zugelassen. In diesem Szenario kommt die Protokollierung der zulässigerweise von innen erfolgenden Zugriffe der Mitarbeiter auf das Internet in Betracht. Dabei ist zwischen den Zugriffen bei dienstlicher und bei privater Nutzung zu unterscheiden. Außerdem kann die Protokollierung dazu dienen, den Versuch eines unzulässigen Zugriffs von außen rechtzeitig zu erkennen.
- In einem anderen Szenario geht es um Zugriffe von außen auf Komponenten des internen Netzes, die dafür grundsätzlich vorgesehen sind (z. B. Web-Server). Die selbstverständlich möglichen Mischformen bleiben der Einfachheit halber außer Betracht.

Ordnet man die Maßnahmen nach ihrer Zielrichtung, ergibt sich daraus folgendes Schema:

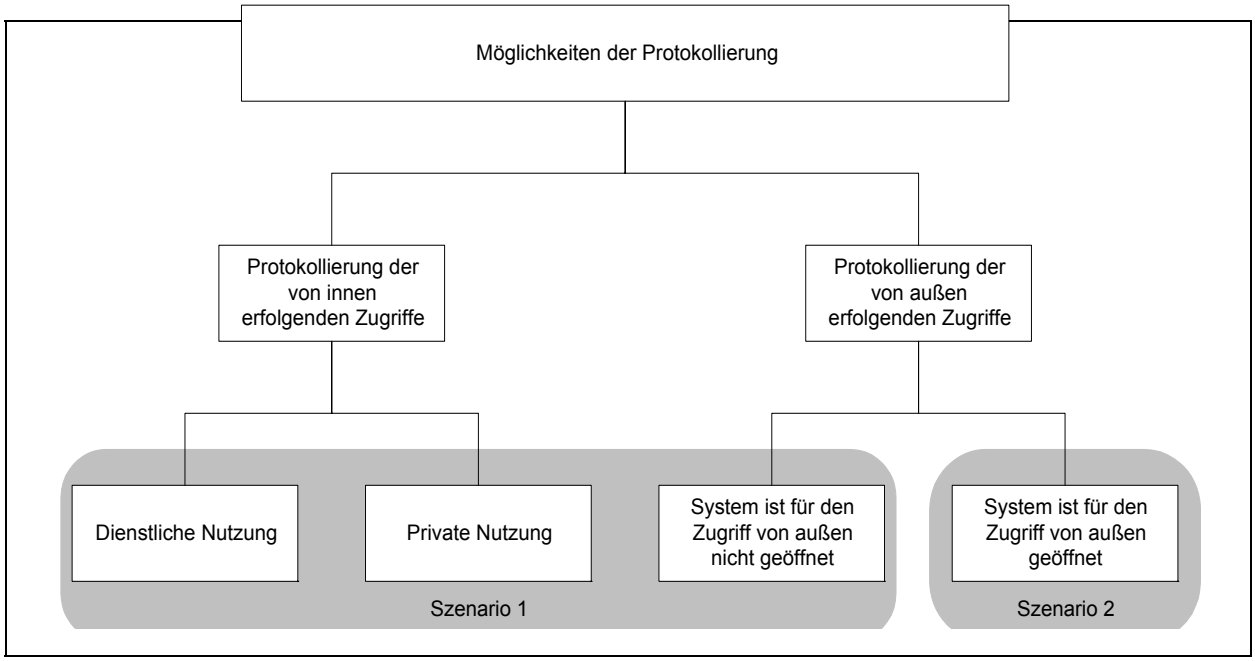

Abbildung 6.1: Protokollierung von Internetzugriffen

Soweit zur Aufrechterhaltung der Datensicherheit die Protokollierung erforderlich ist, stellt sich die Frage, wie lange die dabei erzeugten Logfiles aufbewahrt werden dürfen. Dies muss für den Einzelfall entschieden werden. Die Daten sind zu löschen, sobald sie für Zwecke der Datensicherheit nicht mehr erforderlich sind.

6.3.1 Protokollierung der von innen erfolgenden Zugriffe (Protokollierung von Mitarbeiterdaten)

Sämtliche Maßnahmen der Inhaltskontrolle und Protokollierung sind geeignet, die Beschäftigten einer Organisation zu überwachen und ihre Leistung und ihr Verhalten zu kontrollieren. In jedem Fall muss für die Betroffenen transparent sein, welche potenziell zur Überwachung ihres Verhaltens geeigneten Maßnahmen aktiviert sind. Derartige Maßnahmen unterliegen außerdem ohne Ausnahme der Mitbestimmung der gewählten Mitarbeitervertretungen (Personalrat bzw. Betriebsrat). Da – wie im Folgenden dargelegt wird – eine Reihe von Einzelfragen zu klären ist, bietet es sich an, zu diesen Themen eine Dienst- bzw. Betriebsvereinbarung abzuschließen.

Vorab ist festzuhalten, dass die Protokolldaten in allen Fällen den besonderen Zweckbindungsvorschriften des § 14 Abs. 4 BDSG bzw. der entsprechenden Vorschriften der Landesdatenschutzgesetze (z. B. § 11 Abs. 5 BlnDSG) unterliegen, soweit die Protokollierung der Aufrechterhaltung der Datensicherheit dient.

Grundsätzlich ist eine pauschale, flächendeckende und „vorbeugende“ Protokollierung aller Internet-Zugriffe der Mitarbeiter zur Verhaltens- und Leistungskontrolle nicht erforderlich und damit unzulässig. Gleiches gilt auch bei der Nutzung eines Intranet. Hier sollte regelmäßig der Sperrung unerwünschter Angebote bzw. der Beschränkung des Zugriffs auf dienstlich erforderliche Angebote der Vorzug gegeben werden.

Für alle Kontrollmaßnahmen ergibt sich eine grundsätzliche Weichenstellung bei der Frage, ob den Nutzern die private Verwendung des dienstlichen Internetanschlusses erlaubt ist. Für den Dienstherrn bzw. Arbeitgeber besteht keine Pflicht, die private Nutzung zuzulassen. Ist die private Nutzung gestattet, so greift das Fernmeldegeheimnis nach § 88 TKG. Dieses umfasst den Inhalt der Telekommunikation und deren nähere Umstände (wer hat wann mit wem kommuniziert oder dies versucht?). Sämtliche Kontrollmaßnahmen sind dann nur noch unter sehr engen Voraussetzungen zulässig.

6.3.1.1 Dienstliche Nutzung

Beim Bereitstellen eines Internet-Zugangs für die ausschließlich dienstliche Nutzung handelt es sich nicht um einen Telekommunikationsdienst im Sinne des Telekommunikationsgesetzes (TKG). Der Arbeitgeber bietet dem Arbeitnehmer keinen Dienst an, sondern stellt ihm lediglich ein Arbeitsmittel zur Verfügung; bei diesem „In-Sich-Verhältnis“ fehlt das vom Telekommunikationsgesetz vorausgesetzte Merkmal, dass es sich bei Diensteanbieter und Nutzer um zwei unterschiedliche Rechtssubjekte handelt (vgl. § 3 Nr.6 und Nr. 14 TKG). Damit finden die Vorschriften des Telekommunikationsgesetzes auf die Protokollierung der ausschließlich dienstlichen Nutzung von Telekommunikationsdiensten keine Anwendung.

Zulässigkeit und Umfang der Protokollierung richtet sich in diesen Fällen vielmehr nach den Vorschriften, die auf die Verarbeitung von Daten im jeweiligen Beschäftigungsverhältnis Anwendung finden, also z. B. nach dem jeweiligen allgemeinen Datenschutz- bzw. dem Beamtenrecht. Art und Umfang einer Protokollierung sollte durch eine Dienstvereinbarung geregelt werden.

Dagegen sollte die Protokollierung der dienstlichen Nutzung nicht auf die Einwilligung der Arbeitnehmer gestützt werden, da es auf Grund der Abhängigkeit im Beschäftigungsverhältnis häufig an der erforderlichen Freiwilligkeit der Einwilligung fehlt.

Bei der dienstlichen Nutzung hat der Arbeitgeber grundsätzlich auch das Recht zu prüfen, ob das Surfen der Mitarbeiter im WWW tatsächlich vollständig dienstlich motiviert war. Allerdings gilt hier, wie bei der Kontrolle der ausgehenden dienstlichen E-Mails, dass eine automatisierte Vollkontrolle im Hinblick auf das Persönlichkeitsrecht der Beschäftigten auf erhebliche Bedenken stößt. In jedem Fall müssen die Beschäftigten auf die geplanten Überwachungsmaßnahmen und die drohenden Sanktionen ausdrücklich hingewiesen werden.

In der Regel geht es darum zu vermeiden, dass Mitarbeiter in der Arbeitszeit und unter Nutzung dienstlicher Ressourcen aus rein privatem Interesse auf Informationen zugreifen. Daher sollten nach Möglichkeit die bekanntesten Angebote (z. B. erotische Angebote, Spiele oder Börsenkurse) bereits gesperrt sein, sofern nicht eine dienstliche Notwendigkeit für die Inanspruchnahme solcher Angebote besteht. Umgekehrt wäre es auch denkbar, die Zugriffe auf dienstlich erforderliche Angebote zu beschränken (Positivliste). Um weiteren Missbrauch zu verhindern, bietet es sich an, in einer Dienstvereinbarung datenschutzfreundliche Verfahren (z. B. stufenweise, zunächst nicht personenbezogene, oder stichprobenartige Protokollierung der Zugriffe) festzulegen.

6.3.1.2 Private Nutzung

Bei der privaten Nutzung eines vom Dienstherren zur Verfügung gestellten Internet-Zuganges handelt es sich um die Nutzung eines Telekommunikationsdienstes im Sinne des Telekommunikationsgesetzes bzw. um ein Telemedium im Sinne von § 11 Abs. 3 TMG, für den im Wesentlichen die datenschutzrechtlichen Vorschriften des TKG anzuwenden sind. Wenn der Arbeitgeber die private Nutzung gestattet, ist er als Diensteanbieter im Sinne des § 3 Nr. 6 TKG anzusehen. Art und Umfang der Protokollierung von Nutzungs- und Abrechnungsdaten richten sich nach § 96 des TKG bzw. durch die Verweisung in § 11 Abs. 3 TMG zusätzlich nach § 12 Abs. 3 und § 15 Abs. 8 TMG. Außerdem gilt das Fernmeldegeheimnis aus § 88 TKG. Sind bestimmte Protokollierungen aus technischer Sicht für die Aufrechterhaltung eines regelgerechten Firewall-Betriebs unabdingbar, können sie ergänzend auf § 100 Abs. 1 sowie § 109 TKG gestützt werden. § 100 Abs. 1 TKG konkretisiert für die Störungserkennung, -eingrenzung und -beseitigung

§ 88 Abs. 3 TKG, wonach es den Diensteanbietern erlaubt ist, sich in dem zum Schutz der technischen Systeme erforderlichen Maß Kenntnis von den näheren Umständen der Telekommunikation zu verschaffen und diese Daten zu diesem Zweck auch zu verwenden.

Zudem kann die private Nutzung des Internet-Zugangs auch von bestimmten einschränkenden Bedingungen (z. B. einer maßvollen Protokollierung zum Zwecke der Kontrolle der Nutzungsbedingungen) abhängig gemacht werden. Unabhängig davon sind die Bediensteten über Art und Umfang der Protokollierung zu informieren (Näheres dazu vgl. [DSK-OHA]).

6.3.2 Protokollierung der von außen erfolgenden Zugriffe

6.3.2.1 Nur Anschluss des internen Netzes an das Internet; keine Angebote der öffentlichen Stelle nach außen

In diesen Fällen ist die Firewall nicht Bestandteil eines Telemediums. Die Vorschriften des Telemediengesetzes finden daher keine Anwendung.

Zulässigkeit und Umfang der Protokollierung richten sich nach § 9 BDSG und Anlage bzw. den entsprechenden Vorschriften der Landesdatenschutzgesetze. Für öffentliche Stellen des Bundes kommt als Rechtsgrundlage für eine erforderliche Verarbeitung personenbezogener Daten § 14 BDSG in Betracht; in den Ländern entsprechende Vorschriften der Landesdatenschutzgesetze.

6.3.2.2 Angebot nach außen (Web-Server)

Soll über eine Firewall der Zugriff auf einen Web-Server einer öffentlichen Stelle aus dem Internet reguliert werden, so dient sie in erster Linie dem Schutz der „hinter“ dem Webserver liegenden technischen Systeme und weniger dem auf dem Webserver gespeicherten Internet-Angebot der Stelle selbst. Insbesondere wenn das Internet-Angebot nicht ausschließlich der Information, sondern auch der Kommunikation oder Transaktion zwischen öffentlicher Stelle und Nutzer dient, soll die Firewall vor allem den Zugriff auf die eigenen Systeme aus dem Internet verhindern und damit Vertraulichkeit, Verfügbarkeit und Integrität der hinter dem Webserver gespeicherten Daten sichern. Die Firewall ist damit nicht unmittelbar selbst Bestandteil des Telemediums, das die öffentliche Stelle auf dem betreffenden Web-Server anbietet.

Für Zwecke der Datensicherheit kommt daher eine Protokollierung auf der Grundlage von § 9 BDSG und Anlage bzw. der entsprechenden Vorschriften der Landesdatenschutzgesetze in Betracht. Da die Firewall weniger der Identifizierung von Angreifern als vielmehr deren Abwehr dient, ist die Abwehr von Zugriffen der Protokollierung vorzuziehen.

Die für das eigentliche Internet-Angebot einer öffentlichen Stelle geltenden inhaltlichen und datenschutzrechtlichen Anforderungen ergeben sich hingegen aus dem TMG, das in der Bundesverwaltung unmittelbar gilt und bei öffentlichen Stellen der Länder durch § 60 Abs. 2 RStV für anwendbar erklärt wird. Zulässigkeit und Umfang der Protokollierung von Nutzungsdaten richten sich ausschließlich nach § 15 TMG. Die Vorschrift lässt eine Speicherung personenbezogener Daten über das Ende des Nutzungsvorgangs hinaus nur zu Abrechnungszwecken zu. Auch für diesen Zweck sind IP-Adressen der Nutzer regelmäßig nicht erforderlich. Eine Verarbeitung von Nutzungsdaten zu Zwecken der Datensicherheit ist nach dem TMG nicht erlaubt; ein Rückgriff auf andere Rechtsvorschriften ist nicht möglich. Deshalb dürfen auf dem Webserver selbst die IP-Adressen bei unproblematischen Zugriffen auf das Angebot nicht gespeichert werden.

Soweit eine Protokollierung auf der Firewall personenbezogen erfolgen darf, ist sie dabei entsprechend den Firewall-Regeln auf das zur Abwehr von Angriffen unabdingbar Notwendige zu begrenzen; der Anbieter unterliegt hier gem. § 3a BDSG bzw. den entsprechenden Bestimmungen der Landesdatenschutzgesetze den Verpflichtungen zur datenarmen Gestaltung seiner Systeme. Für Anbieter von Telemedien ergibt sich diese Verpflichtung bei der Verarbeitung von Bestands- und Nutzungsdaten speziell aus § 13 Abs. 6 TMG. Der Anbieter muss darüber hinaus die Informationspflichten nach § 13 Abs. 1 TMG auch hinsichtlich der Protokollierung personenbezogener Daten beachten.

Soweit unter den genannten Bedingungen personenbezogene Daten zur Gewährleistung der Datensicherheit oder des Datenschutzes gespeichert werden, unterliegen sie der besonderen Zweckbindung nach § 14 Abs. 4 BDSG bzw. den entsprechenden Vorschriften der Landesdatenschutzgesetze (z. B. § 11 Abs. 5 BlnDSG).

In dieser Konstellation kann die Protokollierung an der Firewall nicht auf die Einwilligung des bzw. der Betroffenen gestützt werden, da eine rechtswirksame Einholung der Einwilligung von Betroffenen auf Grund der technischen Gegebenheiten im Internet praktisch nicht möglich ist.

Weitere datenschutzrechtliche Empfehlungen zur Nutzung von Internetdiensten am Arbeitsplatz können der von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder herausgegebenen „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“ [DSK-OHA] entnommen werden.

7. Anhänge

7.1 Literatur

[Anti-Spam] Antispam-Strategien
http://www.bsi.bund.de/literat/studien/antispam/antispam.pdf

[BSI 100-2] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-2, IT-Grundschutz-Vorgehensweise, Version 1.0
http://www.bsi.de/literat/bsi_standard/standard_1002.pdf

[BSI 2002] Bundesamt für Sicherheit in der Informationstechnik: BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen
http://www.bsi.bund.de/literat/studien/ids02/index.htm

[BSI 2006] Bundesamt für Sicherheit in der Informationstechnik (Hg.): Integration und IT-Revision von Netzübergängen, Bonn, 2006
http://www.bsi.de/fachthem/sinet/ablaufplan/itrevision/Teil_I_LeitfadenRevision.pdf

[BSI GS] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge
http://www.bsi.de/gshb/

[BSI VP] Bundesamt für Sicherheit in der Informationstechnik: Die Virtuelle Poststelle
http://www.bsi.bund.de/fachthem/vps/index.htm

[BSI-SGW 2007] Bundesamt für Sicherheit in der Informationstechnik: Konzeption von Sicherheitsgateways
http://www.bsi.de/fachthem/sinet/loesungen_netze/Konz_SiGw.pdf

[DSK-OHA] Datenschutzgerechte Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, 2007
http://www.lfd.m-v.de/dschutz/informat/nutzuint/nutzuint.pdf

[HDSB] Der Hessische Datenschutzbeauftragte, 28. TB, Zf. 10.3: Intrusion Detection Systeme
http://www.datenschutz.hessen.de/_old_content/tb28/k10p3.htm

[ISi-Client] Bundesamt für Sicherheit in der Informationstechnik: Sichere Anbindung von lokalen Netzen an das Internet: Absicherung von Clients in lokalen Netzen
http://www.bsi.bund.de/literat/studien/ISILana/ISi-S-LANA.pdf

[ISi-Fern] Bundesamt für Sicherheit in der Informationstechnik: BSI-Reihe zur Internet-Sicherheit, Sicherer Fernzugriff auf das interne Netz
http://www.bsi.bund.de/fachthem/sinet/

[ISi-IDS] Bundesamt für Sicherheit in der Informationstechnik: BSI-Reihe zur Internet-Sicherheit, Einsatz von Intrusion-Detection-Systemen zum Schutz von lokalen Netzen

http://www.bsi.bund.de/fachthem/sinet/

[ISi-VPN] Bundesamt für Sicherheit in der Informationstechnik: BSI-Reihe zur Internet-Sicherheit, Einsatz von Virtual Privat Networks zur sicheren Verbindung von Netzen
http://www.bsi.bund.de/fachthem/sinet/

[OH eGov] Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Orientierungshilfe Datenschutzgerechtes eGovernment, Nov 2002
http://www.datenschutz-berlin.de/attachments/7/oh_egovern.pdf

[RFC 3031] Multiprotocol Label Switching Architecture
http://tools.ietf.org/html/rfc3031
siehe auch http://de.wikipedia.org/wiki/Multiprotocol_Label_Switching

[VNC] Wikipedia: Virtual Network Computing
http://de.wikipedia.org/wiki/Virtual_Network_Computing

[XMLHttpRequest] Wikipedia: XMLHttpRequest
http://de.wikipedia.org/wiki/XMLHttpRequest

7.2 Abkürzungsverzeichnis

ALG	Application-Level Gateway
ARP	Address Resolution Protocol
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CGI	Common Gateway Interface
CIDR	Classless Inter-Domain Routing
DKIM	DomainKeys Identified Mail
DMZ	Demilitarisierte Zone
DNS	Domain Name Service
DNSBL	DNS-based Blackhole List
DSL	Digital Subscriber Line
FTP	File Transfer Protocol
GG	Grundgesetz
HIDS	Host Intrusion Detection System
HTML	HyperText Markup Language
HTTP	HyperText Transport Protocol
ICMP	Internet Control Message Protocol
ICQ	„I seek you“
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
JVM	Java Virtual Machine
LAN	Local Area Network
LSO	Local Shared Object
MPLS	Multiprotocol Label Switching

MTA	Message Transfer Agent
NAT	Network Address Translation
NFS	Network File System
NID	Network Intrusion Detection
NIDS	Network Intrusion Detection System
OH	Orientierungshilfe
RFC	Request for Comment
RHSBL	Right Hand Side Blocking List
RStV	Rundfunkstaatsvertrag
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TMG	Telemediengesetz
TKG	Telekommunikationsgesetz
URI	Universal Ressource Identifier
URIBL	URI Blacklist
USB	Universal Serial Bus
VM	Virtual Machine
VNC	Virtual Network Computing
VoIP	Voice over IP
VPN	Virtual Private Network
VPS	Virtuelle Poststelle
WSS	Web Services Security
WWW	Word Wide Web