Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Leitfaden

Bedrohung der Informationssicherheit durch den gezielten Einsatz von Schadprogrammen

Teil 2: IT-Sicherheitsmaßnahmen gegen spezialisierte Schadprogramme

Änderungshistorie

Datum	Änderung
22.01.2007	Version 1
03.04.2007	Version 1.1: Aktualisierung der Literaturhinweise

Ansprechpartner

Referat 113 - VS- und IT-Sicherheitsberatung

E-Mail: Referat113@bsi.bund.de

Tel.: +49 (0) 22899-9582-5220

Referat 125 - IT-Penetrationszentrum, Abwehr von Internetangriffen

E-Mail: Referat125@bsi.bund.de

Tel.: +49 (0) 22899-9582-5304

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: http://www.bsi.bund.de

Thema und Zielgruppe

Die Bedrohung von schützenswerten Informationen hat durch die Weiterentwicklung von Schadsoftware eine neue Dimension erreicht. Dieser Leitfaden beschäftigt sich in erster Linie mit Schadprogrammen, die individuell für ein bestimmtes Opfer geschrieben werden und maßgeschneiderte Funktionen bieten. Sie sind besonders gefährlich, da sie von klassischen Viren-Schutzprogrammen und Firewalls nicht mehr zuverlässig erkannt werden können.

Da Spionageprogramme zunehmend aus kriminellen oder nachrichtendienstlichen Motiven gegen Behörden und Unternehmen eingesetzt werden, ist eine Anpassung und Erweiterung bestehender Sicherheitskonzepte notwendig.

Der Leitfaden besteht aus drei Teilen:

1. Der erste Teil erläutert die Wirkungsweise moderner Schadprogramme, stellt das Gefahrenpotential dar und gibt einen Überblick über mögliche Sicherheitsmaßnahmen. Er richtet sich an **Führungskräfte** mit Zuständigkeit für Informationstechnik und Informationssicherheit, **IT-Sicherheitsbeauftragte** und interessierte **IT-Anwender.** Zum Verständnis ist allgemeines IT-Wissen von Vorteil.

2. Der zweite Teil beschreibt konkrete Maßnahmen und richtet sich an **IT-Sicherheitsbeauftragte** und **IT-Personal** mit guten technischen Kenntnissen. An vielen Stellen werden weitere Informationsquellen wie Studien, Best-Practice-Ratgeber oder Standards angegeben, die bei der praktischen Umsetzung der Maßnahmen hilfreich sind.

   Es gibt zurzeit *kein einzelnes* Sicherheitsprodukt, das einen ausreichenden Schutz gegen individuell angepasste Schadprogramme bietet. Es wird auch jeder Versuch scheitern, *die wichtigste* Maßnahme zu benennen. Einem Angreifer stehen vielfältige Techniken und Informationen zur Verfügung, um in fremde Rechner einzudringen. Ihm genügt eine einzige Schwachstelle im Programmcode einer Anwendung, in Konfigurationsdateien oder im Design einer IT-Landschaft. Sicherheitsmaßnahmen müssen daher ein breites Spektrum abdecken - vom Schutz einzelner Rechner über organisatorische Maßnahmen, die Ausbildung der Mitarbeiter bis zur Netzsicherheit. Dieser Leitfaden hilft bei der Auswahl wirksamer Sicherheitsmaßnahmen und gibt Hinweise, wo Standardmaßnahmen durch höherwertige ergänzt werden müssen.

3. Den dritten Teil bildet ein Kurztest zur Einschätzung der eigenen Bedrohungslage durch gezielte Angriffe mit Schadprogrammen. Das Ergebnis gibt **Führungskräften** einen ersten Anhaltspunkt, wie gut vertrauliche Informationen geschützt sind und wie wahrscheinlich es ist, durch Spionage oder Sabotage Schaden zu nehmen.

Redaktionelle Leerseite

Inhaltsverzeichnis

1 Einleitung

Im Folgenden werden die wichtigsten Maßnahmen zusammengefasst, die zum Schutz vor Angriffen mit Spionageprogrammen notwendig sind. Die vorgestellten Maßnahmen gehen teilweise über das IT-Grundschutz-Niveau hinaus oder beschreiben ausgewählte Sachverhalte detaillierter.

Der Maßnahmenkatalog ist keine Einführung in Grundbegriffe der IT-Sicherheit und setzt entsprechendes Wissen voraus. Er stellt die Maßnahmen möglichst kurz und prägnant dar und ist so auch als Checkliste nutzbar. Bestehende BSI-Standards, IT-Grundschutzkataloge oder BSI-Studien werden daher nicht unnötig reproduziert. Stattdessen finden sich Verweise, wenn ein Thema an anderer Stelle bereits ausführlich dargestellt ist. Beispielsweise gibt es keine Maßnahme, die abermals die Notwendigkeit von angemessenen Backup-Verfahren darstellt.

→ Literaturhinweise

In vielen Maßnahmen wird auf weiterführende Literatur verwiesen. In Kapitel 10 werden die verwendeten Abkürzungen erklärt und die wichtigsten Informationsquellen noch einmal abschließend zusammengestellt.

Nicht immer werden sich die empfohlenen Maßnahmen ohne Anpassung an die eigenen Gegebenheiten sofort übernehmen lassen. Der Erfolg von Schutzmaßnahmen gegen individuell erstellte Schadprogramme beruht auch darauf, einen Angreifer durch ungewöhnliche und kreative Methoden zu überraschen und zu verwirren. Keine Maßnahme ist so ausgefeilt, dass sie alleine einen vollständigen Schutz gewährleistet. Einem Außentäter stehen nur beschränkte Möglichkeiten zur Verfügung, ein fremdes Netz auszukundschaften. Jede ungewöhnliche Maßnahme, jede Abweichung von Standardinstallationen und jede Eigenentwicklung erhöht den Aufwand für einen Angreifer. Selbst einfache Maßnahmen können daher die Sicherheit verbessern. Das Dokument enthält deswegen an einigen Stellen auch Vorschläge, die nicht durch Standardsoftware realisiert werden können. Administratoren sollen dazu angeregt werden, eigene Ideen zu entwickeln und „um die Ecke zu denken“.

Bewertung einzelner Maßnahmen

In den Kapiteln 7 „Sichere Vernetzung und Internetnutzung“ und 8 „Detektion und Abwehr von Schadprogrammen“ werden auch Maßnahmen vorgestellt, die sich nur mit erheblichem Aufwand umsetzen lassen. Andere Maßnahmen schränken den Komfort und die Funktionalität von Anwendungen stark ein. Es ist daher nicht sinnvoll, jede der vorgestellten Maßnahmen in das eigene IT-Sicherheitskonzept zu übernehmen. Ob eine Maßnahme sinnvoll ist, hängt vom Schutzbedarf der verarbeiteten Informationen und der individuellen Bedrohungslage ab. Diese aufwendigeren, optionalen Maßnahmen enthalten zur besseren Orientierung für Sicherheitsbeauftragte jeweils eine kurze Bewertung des Sicherheitsgewinns. Zusätzlich werden je nach Zusammenhang weitere Kategorien wie Funktionseinbußen oder Realisierungsaufwand angesprochen.

Alle Maßnahmen ohne Bewertungstabelle hält das BSI jedoch in jeder Einsatzumgebung für erforderlich.

2 IT-Sicherheitsmanagement und Organisation

Der Schutz gegen spezialisierte Schadprogramme ist nicht ohne Aufwand möglich und erfordert eine vollständige und konsequente Umsetzung von Sicherheitsmaßnahmen. Die Behörden- oder Unternehmensleitung sollte klare strategische Vorgaben machen, ein systematisches Sicherheitsmanagement betreiben und für geeignete organisatorische Rahmenbedingungen sorgen. Der IT-Sicherheitsbeauftragte und die weiteren Personen mit IT-Sicherheitsaufgaben sind auf den Rückhalt im Management angewiesen - besonders wenn im Alltag oder bei Projekten Sicherheit, Komfort und Funktionalität ausbalanciert werden müssen.

Systematisches IT-Sicherheitsmanagement nach anerkannten Methoden

Sicherheitsmanagement und technische Maßnahmen sollten sich an anerkannten Standards, Best-Practices und Herstellerdokumentationen orientieren. Das BSI empfiehlt, mindestens IT-Grundschutz umzusetzen und bei hohen Sicherheitsanforderungen weitergehende Maßnahmen zu prüfen.

→ BSI Standards zum IT-Sicherheitsmanagement:

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
- BSI-Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz

→ Weitere Literatur zum IT-Sicherheitsmanagement:

- ISO/IEC 17799:2005 „Information technology - Code of practice for information security management“, ISO/IEC JTC1/SC27
- ISO/IEC 27001:2005 „Information technology - Security techniques - Information security management systems requirements specification“, ISO/IEC JTC1/SC27
- Information Security Forum (ISF): Im ISF haben sich einige große Unternehmen zusammengeschlossen, um gemeinsam an Themen der IT-Sicherheit zu arbeiten. Öffentlich verfügbar ist ein Leitfaden zur Erstellung eines IT-Sicherheitskonzeptes: „The Forum’s Standard of Good Practice“, http://www.isfsecuritystandard.com

→ Erstellung eines IT-Sicherheitskonzeptes (technische Informationen):

- BSI IT-Grundschutz: http://www.bsi.bund.de/gshb
- NIST: http://csrc.nist.gov/publications/nistpubs/index.html
- NSA: http://www.nsa.gov/snac/
- CPNI: Current Advice - Mitigating the risk of Malicious Software, http://www.cpni.gov.uk/docs/currentAdvice.pdf

Risikobetrachtung für bedrohte Informationen und IT-Komponenten

Eine Risikobetrachtung dient der Auswahl *angemessener* Maßnahmen. Es sollen zu aufwendige Maßnahmen vermieden werden, ohne jedoch Gefährdungen zu vernachlässigen. Wichtig ist dabei eine individuelle Betrachtung der Bedrohungslage: Gibt es Konkurrenten oder andere Interessensgruppen, die möglicherweise aggressive Methoden zur Ausspähung von vertraulichen Informationen oder zur Sabotage einsetzen? Ist man in einem politisch oder ideologisch heiklen Umfeld tätig?

1. Zu jedem Geschäftsprozess und jeder Fachanwendung muss es einen Ansprechpartner geben, der für Fragen der Informationssicherheit zuständig ist. Zu jedem Geschäftsprozess und jeder Fachaufgabe muss festgelegt werden, wie kritisch, also wie schutzbedürftig die verarbeiteten Informationen sind und welche Maßnahmen zu ihrem Schutz getroffen werden.

2. Es muss eine Übersicht mit allen relevanten Schutzobjekten - wie Informationen, IT-Anwendungen, IT-Systeme oder Netze - erstellt werden. Damit muss nachvollziehbar sein, welche Beziehungen und Abhängigkeiten zwischen den Schutzobjekten bestehen. Beispielsweise muss dokumentiert sein, welche Geschäftsprozesse bzw. Informationen besonders vertraulich sind, auf welchen IT-Systemen die betroffenen Daten verarbeitet werden und wie diese Rechner vernetzt sind.

3. Mögliche Schäden durch IT-Sicherheitsvorfälle müssen analysiert und bewertet werden. Um ein Risiko bestimmen zu können, müssen die Bedrohungen ermittelt und deren Schadenspotential und Eintrittswahrscheinlichkeit eingeschätzt werden.

→ Weitere Informationen:

- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, Kapitel 4 Erstellung einer IT-Sicherheitskonzeption nach IT-Grundschutz
- GS-K, M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
- GS-K, M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten
- ISO/IEC 13335 „Management of information and communications technology security“, ISO/IEC JTC1/SC27
- NISCC Technical Note 04/04: Organisational Vulnerability Management Process, Issued 25 March 2004, http://www.cpni.gov.uk/docs/re-20040325-00157.pdf

Regelmäßige Erfolgskontrolle

Es muss regelmäßig durch interne und externe Audits untersucht werden, ob Sicherheitsvorgaben und Regeln eingehalten werden. Social Engineering-Tests sollten dabei ebenso durchgeführt werden wie Penetrationstests zur Verifikation der Sicherheit von Netzübergängen. Darüber hinaus muss geprüft werden, ob mit den einmal umgesetzten Maßnahmen die gesetzten IT-Sicherheitsziele immer noch zu erreichen sind. Dieser Leitfaden könnte z. B. ein Anlass sein, die eigene Bedrohungslage neu zu bewerten und das Sicherheitskonzept anzupassen.

→ Weitere Informationen:

- BSI-Studie „Durchführungskonzept für Penetrationstests“, http://www.bsi.bund.de/literat/studien/pentest/index.htm
- BSI-Studie „Revision von Netzübergängen“, http://www.bsi.bund.de/fachthem/sinet/ablaufplan/itrevision/index.htm
- IT-Grundschutz-Zertifikat, http://www.bsi.bund.de/gshb/zert/index.htm

Auswahl von Dienstleistern und Herstellern

Bei der Auswahl von Geschäftspartnern (Dienstleister, Outsourcing-Partner, Hersteller, Lieferanten) müssen Sicherheitsgesichtspunkte mit berücksichtigt werden. In Bereichen mit besonders hohen Vertraulichkeitsanforderungen spielen die Beziehungen des Geschäftspartners zu Konkurrenten oder das Herkunftsland des Auftragnehmers eine Rolle. Externen Dienstleistern oder Beratern sollte nur nach sorgfältiger Sicherheitsüberprüfung Zugang zu Systemen ermöglicht werden, mit denen auf vertrauliche Daten zugegriffen werden kann. Besonders bei der Beschaffung von Sicherheitssoftware und -tools muss der Hersteller sehr sorgfältig ausgewählt werden.

3 Integration der Mitarbeiter in den Sicherheitsprozess

Ausarbeitung von Sicherheitsrichtlinien

In Sicherheitsrichtlinien sollten den Mitarbeitern die wichtigsten Spielregeln für die IT-Nutzung begründet und erläutert werden. Folgende Punkte sollten thematisiert werden:

- Sicherheitsleitlinie („Policy“): Sinn und Zweck der IT-Nutzung sowie Grundregeln der IT-Sicherheit
- Internet- und E-Mail-Nutzung
- Verhalten bei Sicherheitsvorfällen und in Notfällen
- IT-Nutzung: z. B. Umgang mit externen Datenträgern und privaten Geräten, Einspielen von Software, Nutzung mobiler Geräte, Backup

→ Weitere Informationen:

Muster und Beispiele zum IT-Grundschutz,
http://www.bsi.bund.de/gshb/deutsch/hilfmi/muster.htm

Schulung und Sensibilisierung

Folgende Themen sollten Teil eines Schulungs- und Sensibilisierungskonzeptes sein:

1. Technische Inhalte für verschiedene Zielgruppen
   (z. B. Administration, Softwareentwicklung, Entwicklung von Web-Applikationen)
2. Sicherheitsspezifische Themen
   (u. a. Internetnutzung, Schutz vor Schadprogrammen, Backup, Nutzung mobiler Geräte)
3. Sicherheitsmanagement und Organisation
   - Welche Sicherheitsrichtlinien müssen beachtet werden?
   - Welche Abläufe und Prozesse sind einzuhalten?
   - Wie werden vertrauliche Informationen eingestuft und geschützt? Welche Informationen dürfen an Externe weitergegeben werden? Welche Daten dürfen über E-Mail ausgetauscht werden?
   - In welcher Form wird intern und extern mit Geschäftspartnern kommuniziert? Wer sind die Ansprechpartner? Welche Kompetenzen haben sie? Wie findet eine Authentisierung statt?
4. Methoden des Social Engineerings, Angriffsvektoren von Nachrichtendiensten und Spionen

Schulungs- und Sensibilisierungsveranstaltungen müssen regelmäßig wiederholt werden. Besonders wichtig ist es, die Aufmerksamkeit im Alltag wach zu halten und Mitarbeiter auf Fehler und Nachlässigkeiten hinzuweisen. Die Durchführung von Audits oder kleineren Social Engineering-Tests durch externe Fachleute ist daher sehr zu empfehlen: Werden Besucher tatsächlich kontrolliert? Lassen sich Mitarbeiter vertrauliche Informationen am Telefon entlocken? Werden Verschlusssachen sicher aufbewahrt?

→ **Weitere Informationen:**

- GS-K, B 1.13 IT-Sicherheitssensibilisierung und -schulung
- „Faktor Mensch - Die Kunst des Hackens oder warum Firewalls nichts nützen“ von SAP für die Initiative „Deutschland sicher im Netz“ https://www.sicher-im-netz.de/?sicherheit/ihre/software/leitfaeden

4 Verhinderung unberechtigter Nutzung von IT-Systemen

Zugang zu IT-Systemen

Es ist zu verhindern, dass IT-Systeme durch Unbefugte (z. B. Mitarbeiter ohne die notwendigen Berechtigungen, Besucher, Fremdpersonal, Handwerker, Servicetechniker) genutzt oder manipuliert werden.

1. Der Zutritt zu Gebäuden und Räumen ist angemessen zu sichern.

2. Personen ohne die notwendigen Befugnisse müssen in Sicherheitsbereichen begleitet werden.

3. Unbefugte dürfen keine Möglichkeit haben, mitgebrachte IT an das Netz anzuschließen (z. B. über ungenutzte Netzwerkdosen).

4. Über IT-Systeme, die für externe Personen zugänglich sind (z. B. in Warteräumen, im Empfangsbereich oder in Besprechungsräumen), darf kein ungesicherter Zugang ins Intranet möglich sein.

5. Alle Mitarbeiter müssen den Zugang zu ihrem Rechner sperren, wenn sie den Arbeitsplatz verlassen.

→ Weitere Informationen:

- GS-K, Bausteine der Schicht 2 (Infrastruktur)
- GS-K, M 2.4 Regelungen für Wartungs- und Reparaturarbeiten
- GS-K, M 2.6 Vergabe von Zutrittsberechtigungen
- GS-K, M 2.7 Vergabe von Zugangsberechtigungen
- GS-K, M 2.8 Vergabe von Zugriffsrechten

Schutz vor nicht zugelassener Hard- und Software

Angreifer können nicht nur *vorhandene* Hardware manipulieren, sondern auch *zusätzliche* Hardware installieren. Aus der Praxis sind z. B. Fälle bekannt, in denen heimlich ein Router für eine ungesicherte Außenverbindung installiert wurde. Einer Bank entstand ein Schaden durch Einbrecher, die einen WLAN-Access-Point zurückgelassen hatten, über den sie Zugang zum Intranet erhielten. Aber auch eigene Mitarbeiter können unabsichtlich Schadprogramme einschleppen oder Schnittstellen öffnen, wenn sie private oder ungeprüfte Hard- oder Software verwenden.

Einspielen bzw. Benutzen nicht freigegebener Hard- und Software muss daher verboten und außerdem durch technische Verfahren verhindert werden. Bei der Auswahl von Produkten (z. B. USB-Sticks), die zugelassen werden sollen, müssen die Sicherheitseigenschaften sorgfältig recherchiert werden. Beispielsweise besitzen so genannte U3-USB-Sticks eine Logik zur Codeausführung und ermöglichen an vielen Rechnern den Start von speziell an die U3-Software angepassten Applikationen. Sie sind daher besonders gefährlich, zumal in Sicherheitskreisen verschiedene Schadprogramme vorgestellt wurden, die die U3-Autostart-Funktionalitäten nutzen.

Die Schnittstellen von Rechnern müssen durch spezielle Sicherheitsprodukte vor der unberechtigten Nutzung geschützt werden. Die Konfigurationsmöglichkeiten des Betriebssystems sind zum Schutz von Schnittstellen nicht ausreichend. Spezielle Tools sorgen beispielsweise dafür, dass nur registrierte USB-Sticks an einen Desktop-Rechner angeschlossen werden können.

In Hochsicherheitsbereichen muss zusätzlich die Manipulation von Hardware und Verkabelung erschwert werden (Verschluss, Siegel, Sicherung von Switch-Ports). Es ist auch sinnvoll, nur Geräte mit registrierter MAC-Adresse im Intranet zuzulassen.

→ Weitere Informationen:

- „Eingeschleppte Gefahr - Risiko durch mobile Datenträger“, iX 02/2006, Heise Verlag
- GS-K, M 4.206 Sicherung von Switch-Ports

Schutz mobil genutzter Datenträger (z. B. USB-Sticks) und IT-Systeme (z. B. Mobiltelefone)

Angreifer können sich bei Veranstaltungen oder Besprechungen in einem unbeobachteten Moment Zugang zu einem fremden Gerät (Notebook, PDA, Mobiltelefon) verschaffen, um Spionagesoftware aufzuspielen oder Daten zu kopieren. Diese Angriffe sind sogar gefährlicher als ein Diebstahl, da sie häufig unbemerkt bleiben. Bei Dienstreisen und bei Veranstaltungen, in deren Verlauf z. B. ein eingesetztes Notebook nicht immer unter Kontrolle gehalten werden kann, sollten daher nach Möglichkeit nur Geräte ohne vertrauliche Daten mitgenommen werden. Nach der Veranstaltung sollte das Notebook neu aufgesetzt werden. Ist dies nicht möglich, muss das Notebook zumindest über wirksame Maßnahmen zum Zugangsschutz verfügen und zudem komplett verschlüsselt sein. Eine Authentisierung sollte dabei aus zwei Komponenten (Passwort und Hardware wie Chipkarte oder Token) bestehen. Wenn das Notebook unbeaufsichtigt zurückgelassen wird, muss der Zugang während der Abwesenheit sicher gesperrt werden. Maßnahmen zur Verschlüsselung und zum Zugangsschutz müssen auch für andere mobilen Geräte umgesetzt werden, wenn vertrauliche Daten oder E-Mails auf ihnen gespeichert sind. Maßnahmen zum physischen Schutz reichen jedoch nicht aus, da die meisten Geräte auch über drahtlose Kommunikationsmöglichkeiten verfügen (siehe dazu Kapitel 7.4).

Besondere Beachtung verdient der Datenaustausch über Medien und Geräte mit USB-Anschluss. So ist es übliche Praxis, dass bei Veranstaltungen Daten über USB-Sticks ausgetauscht werden. Dieser Umstand kann für gezielte Spionageangriffe genutzt werden, indem mehr als die gewünschte Datei (wie eine Präsentation im PDF-Format) auf den überreichten USB-Stick kopiert wird. Bei hohem Schutzbedarf darf der eigene USB-Stick daher nicht aus der Hand gegeben werden. Ist ein Datenaustausch dennoch notwendig, sollte der USB-Stick zunächst an einem gehärteten Testrechner angeschlossen werden, um die gewünschten Dateien umzukopieren. Anschließend muss der USB-Stick formatiert werden.

→ Weitere Informationen:

BSI-Broschüre „Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen“,
http://www.bsi.bund.de/literat/doc/mobile/index.htm

5 Umgang mit schützenswerten Dateien und Anwendungen

Maßnahmen zum Schutz einzelner Dateien und Informationen können einem Angreifer auch dann noch das Leben schwer machen, wenn er bereits heimlich ein Schadprogramm installieren und starten konnte. Dateien und Programme, die ein IT-Anwender gerade verwendet, liegen einem Angreifer schutzlos offen. Er kann z. B. Tastatureingaben aufzeichnen oder Programme starten. Durch geeignete Maßnahmen kann aber zumindest verhindert werden, dass ein Angreifer Zugriff auf weitere Informationen, Dateien oder Programme erhält. Ein weiterer Baustein zum Schutz von Dateien ist die richtige Netzsegmentierung, die in Kapitel 7 „Sichere Vernetzung und Internetnutzung“ besprochen wird. Auf Netzebene kann der Zugriff auf bestimmte Dateien zuverlässiger verhindert werden als über Berechtigungen. Wenn möglich, sollten daher immer beide Mechanismen angewendet werden.

Verschlüsselung von hoch vertraulichen Daten

Um zu verhindern, dass ein Spionageprogramm sehr einfach große Datenmengen durchsuchen und entwenden kann, dürfen hoch vertrauliche Informationen nur verschlüsselt gespeichert werden. Je nach Vertraulichkeitsgrad sind Verzeichnisse oder Einzeldateien individuell zu verschlüsseln. Eine Komplettverschlüsselung eines Notebooks ist dazu z. B. nicht ausreichend, da nach einem Login zu jeder Zeit auf alle Dateien zugegriffen werden kann.

Verwendung von Rollen und Profilen

1. Jeder IT-Anwender sollte nur auf die Datenbestände zugreifen und die Programme ausführen dürfen, die er für seine tägliche Arbeit auch wirklich benötigt. Aufgaben- oder projektbezogene Verzeichnisse erleichtern daher die Verwaltung von Berechtigungen erheblich.

2. Der Account bzw. das Terminal eines IT-Anwenders sollten außerhalb der offiziellen Arbeitszeit gesperrt werden.

3. Accounts, die über einen längeren Zeitraum nicht benutzt werden, sollten gesperrt werden.

Beschränkung der Administratorrechte

1. Administratorrechte müssen beschränkt sein und sich an bestimmten Rollen orientieren.

2. Mit Administratorrechten darf nur gearbeitet werden, wenn dies für die Aufgabenerfüllung notwendig ist. Zur E-Mail-Nutzung und zum Surfen darf kein Account mit Administratorrechten verwendet werden.

Begrenzung von Programmprivilegien

Angreifer können Schadcode ausführen, indem sie Schwachstellen ausnutzen und Pufferüberläufe provozieren. Die Schadroutine „erbt“ dabei die Zugriffsrechte und Systemprivilegien des abgestürzten Programms. Die meisten Programme sind nur mit den eingeschränkten Berechtigungen des Anwenders ausgestattet, der das Programm gestartet hat. Bevorzugtes Ziel eines Angreifers sind daher Pro-

gramme mit Administratorrechten. Ein Schadprogramm kann dann Systemänderungen vornehmen, über das Netz auf Daten zugreifen und großen Schaden anrichten.

Je mehr Programme mit hohen Privilegien ausgestattet sind, desto größer ist die Gefahr, dass sich ein Angreifer über eine Schwachstelle weitreichende Berechtigungen verschafft. Programme, die Administratorrechte benötigen, sollten daher nur verwendet werden, wenn es der Geschäftsprozess unbedingt erfordert und keine Alternative zur Verfügung steht.

Bei der restriktiven Vergabe von Zugriffsrechten reicht es nicht aus, nur die Rechte des gewünschten Programms zu überprüfen. Zusätzlich muss auch die Rechtevergabe all der Programme überprüft werden, die von dem ursprünglichen Programm aus aufgerufen werden.

Sichere Passwörter

Einige Schadprogramme suchen gezielt nach Dateien mit Passwörtern, versuchen geschützte Anwendungen zu starten oder auf gesperrte Dateien zuzugreifen.

1. Es dürfen nur sichere Passwörter verwendet werden. Passwortregeln finden sich z. B. in der im Kasten genannten IT-Grundschutz-Maßnahme.

2. Passwörter müssen sicher gespeichert werden (nicht im Klartext oder in Makros), damit sie nicht einfach ausgelesen werden können.

3. Sichere Passwörter sowie ihre regelmäßige Änderung müssen technisch erzwungen werden.

4. Voreingestellte oder leere Passwörter müssen stets geändert werden.

5. Die meisten Menschen sind überfordert und fühlen sich belästigt, wenn sie sich privat und beruflich eine Vielzahl von Passwörtern merken müssen. Ihr Ausweg besteht darin, Trivialpasswörter oder immer das gleiche Passwort mit nur geringen Variationen zu verwenden. Gelingt es einem Angreifer, das Passwort einer eher unwichtigen Applikation auszulesen, hat er einen guten Ansatzpunkt für Brute-Force-Angriffe gegen den Passwortschutz wichtiger Anwendungen mit hohem Schutzbedarf.

   Wenn Mitarbeiter unsichere Passwörter wählen, liegt aber sehr häufig die Schuld nicht bei ihnen, sondern bei den IT-Verantwortlichen. Diese sollten darauf achten, Maß zu halten und die Anzahl der täglich benötigten Passwörter auf ein Minimum zu begrenzen. Nicht jede Anwendung muss wirklich durch Passworteingaben geschützt werden. Auch der Einsatz technischer Verfahren (Biometrie, Chipkarten, Token, Single-Sign-On etc.) sollte erwogen werden.

→ Weitere Informationen:

GS-K, M 2.11 Regelung des Passwortgebrauchs

6 Absicherung von IT-Systemen und IT-Anwendungen

Beschaffung von IT-Komponenten

1. Technische Aspekte bei der Auswahl von Produkten

Bei der Auswahl von Produkten sollten folgende Fragen gestellt werden:

- Erfordert der Einsatz Techniken, die sich nicht gut oder nur mit zusätzlichen Maßnahmen sichern lassen (z. B. Voice over IP)? Müssen bestehende Sicherheitsrichtlinien gelockert werden (Zulassung Aktiver Inhalte, Freischaltung von Diensten an der Firewall etc.)?
- Wird eine spezielle Anleitung mit Sicherheitsaspekten von Installation, Konfiguration und Betrieb mitgeliefert? Stellt der Hersteller eine Übersicht über Dateien, Prozesse und Nutzung von Systemressourcen zur Verfügung?
- Wurde das Produkt zertifiziert, unabhängig getestet oder von vertrauenswürdigen Organisationen empfohlen?
- Ist das Produkt bereits etabliert und ausgereift oder eine Neuentwicklung?
- Wie ist die Sicherheitshistorie? Wie viele Schwachstellen wurden bekannt?
- Wie ist der Support? Wie schnell wurden Sicherheitspatches nach der Veröffentlichung von Schwachstellen veröffentlicht?
- Wird das Produkt regelmäßig gepflegt? Wie lange werden Updates und Patches bereitgestellt?
- Lässt sich das Produkt mit eingeschränkten Benutzerechten bedienen oder werden Administratorrechte benötigt?
- Ist das Produkt komplex oder einfach aufgebaut? Grundsätzlich sind einfache Produkte vorzuziehen, die nicht mit überflüssigen Funktionen überfrachtet sind.
- Kann der Quellcode selbst compiliert oder zumindest geprüft werden?
- Unterstützt das Produkt Verschlüsselung (bei Datenübertragung und Speicherung)?
- Enthält die IT-Anwendung Funktionen zur Protokollierung?
- Enthält die Software versteckte Funktionen, Spyware oder Rootkit-Funktionalitäten? Wenn möglich, sollte mit dem Hersteller vertraglich vereinbart werden, dass derartige Mechanismen nicht benutzt oder zumindest sorgfältig dokumentiert werden.

2. Software und Dateien

- Software sollte grundsätzlich nur aus bekannten Quellen installiert werden, auch dann, wenn sie nicht aus dem Internet heruntergeladen und auf Datenträgern geliefert wird. Auch Software, die nicht installiert werden muss, kann versteckte Funktionen besitzen. Beispielsweise kann auf einer Werbe-CD ein manipulierter Browser im Hintergrund Programme ausführen - und nicht nur den Produktkatalog anzeigen. Auch bei einzelnen Dateien ist Vorsicht geboten - unabhängig vom Dateityp.

- Nach Möglichkeit sollten Softwarehersteller zur Bereitstellung von Prüfsummen und elektronischen Signaturen gedrängt werden. In Hochsicherheitsbereichen ist diese Anforderung unverzichtbar. Prüfsummen müssen auf einem sicheren Weg übertragen werden.

→ Weitere Informationen:

- GS-K, M 4.177 Sicherstellung der Integrität und Authentizität von Softwarepaketen
- GS-K, M 2.80 Erstellung eines Anforderungskatalogs für Standardsoftware

Eigenentwicklung von Software

Bei der Entwicklung von Software müssen Sicherheitsgesichtspunkte berücksichtigt werden, um z. B. Cross-Site Scripting (XSS), SQL Injection oder Pufferüberläufe zu verhindern. Programmierer sollten daher in den Techniken zur sicheren Programmierung ausgebildet werden.

→ Weitere Informationen:

- Das neue V-Modell® XT - Der Entwicklungsstandard für IT-Systeme des Bundes: http://www.kbst.bund.de unter „Standards und Architekturen“
- Leitfaden „Sicheres Programmieren“ von SAP für die Initiative „Deutschland sicher im Netz“
  https://www.sicher-im-netz.de/?sicherheit/ihre/software/leitfaeden
- Microsoft Security Developer Center: http://msdn.microsoft.com/security/
  z. B.: “Defend Your Code with Top Ten Security Tips Every Developer Must Know” und “Avoiding Buffer Overruns”
- Microsoft Security Developer Center Germany:
  http://www.microsoft.com/germany/msdn/security/default.mspx
- MISRA-C - Guidelines for the use of the C language in critical systems:
  http://www.misra-c2.com

Test von IT-Anwendungen und IT-Systemen

1. **Testanforderungen**

   Neben den üblichen Funktions- und Kompatibilitätstests sollten folgende Punkte getestet und bewertet werden:

   - Test auf Schadprogramme, Spyware, Adware, Keylogger
     Nach Möglichkeit sollten dazu mehrere Schutzprogramme mit signaturbasierten und heuristischen Methoden verwendet werden.
   - Kommunikationsverhalten (z. B. Verbindungen ins Internet, Wartungseinwahlen, Verbindungsanfragen von außen, Zugriffe auf Ressourcen im Intranet (z. B. Datenbanken))
   - Zugriff auf Systemressourcen und Privilegien

- Test auf versteckte Funktionen: Einige Softwareprodukte verwenden Rootkit-Funktionen, um Daten versteckt im Dateisystem abzuspeichern oder ihre Prozesse vor dem Zugriff durch Systemfunktionen zu verbergen. Sicherheitsprodukte nutzen diese Methoden beispielsweise, um nicht von Schadprogrammen deaktiviert zu werden. Auch die Nutzung von Alternate Data Streams (NTFS-Dateisystem) sollte verifiziert werden. Diese „Features“ sind nur in wenigen Ausnahmefällen zu akzeptieren, da Schadprogramme die bereitgestellten Verstecke ebenfalls nutzen können.

2. Dokumentation

Neben Standardinformationen (wie Dateinamen, Versionsstände, Dateigröße aller Dateien, Konfigurationseinstellungen) muss ein Administrator folgende Informationen aufnehmen:

- Welche Prozesse sind zur Laufzeit einer IT-Anwendung/ des Betriebssystems aktiv?
- Werden bestehende Systemdateien, Libraries, Treiber etc. bei der Installation geändert? Bei Windows-Systemen sind z. B. unbedingt die Eintragungen in der Registry zu dokumentieren.
- Welche Libraries und Treiber werden verwendet?
- Prüfsummen aller Dateien mit sicheren Hashverfahren

→ Weitere Informationen:

- GS-K, M 2.34 Dokumentation der Veränderungen an einem bestehenden System
- GS-K, M 4.237 Sichere Grundkonfiguration eines IT-Systems

Standard-Konfigurationen

Eine gewisse Homogenität der IT-Landschaft hat viele Vorteile. Damit ist keine Monokultur bei Betriebssystemen oder Anwendungen gemeint, sondern die Empfehlung, dass IT-Systeme, die für die gleichen Aufgaben eingesetzt werden und den gleichen Anforderungen unterliegen, möglichst homogen ausgestattet und konfiguriert sind. Muss beispielsweise ein Update oder Patch für sehr viele unterschiedliche Systemkonfigurationen getestet werden, ist das kaum effizient möglich. Bei forensischen Untersuchungen muss ein Administrator seine Systeme sehr genau kennen, um bösartige Veränderungen feststellen zu können. Sinnvolle Standardkonfigurationen und eine Zusammenfassung von IT-Systemen zu einheitlichen Gruppen ist daher betriebswirtschaftlich sinnvoll und aus Sicherheitsgründen notwendig.

→ Weitere Informationen:

BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, Kapitel 4.1.6 Komplexitätsreduktion durch Gruppenbildung

Kontrolle von IT-Komponenten

Beim Betrieb von IT-Komponenten (Hard- und Software, Verkabelung) sollten die folgenden Punkte beachtet werden, die zum Teil über das IT-Grundschutz-Niveau hinausgehen:

1. Regelmäßige Überprüfung des Hard- und Software-Bestandes

   In Bereichen mit hohen Vertraulichkeitsanforderungen muss regelmäßig (wöchentlich) automatisch geprüft werden, ob Programme verwendet werden, die für das betreffende IT-System bzw. den IT-Anwender nicht genehmigt wurden. Es muss weiterhin regelmäßig kontrolliert werden, ob nicht-freigegebene Hardware eingesetzt oder alternative Netzzugänge verwendet werden.

2. Regelmäßige Kontrolle von Berechtigungen und Privilegien

   - Unzulässige Berechtigungen eines IT-Anwenders und veränderte Sicherheitseinstellungen müssen erkannt werden (z. B. Administratorrechte oder die Freischaltung von bestimmten Diensten oder Ports).
   - Wenn Mitarbeiter ausgeschieden sind oder neue Aufgaben übernommen haben, müssen die Berechtigungen gelöscht bzw. angepasst werden.
   - Unzulässige Privilegien von Programmen müssen erkannt werden.

→ Weitere Informationen:

GS-K, B 1.9 Hard- und Software-Management

Regelmäßige Updates von Betriebssystemen, Anwendungen und Hardware

1. Es müssen regelmäßig Informationen über neue Schwachstellen und Bedrohungen eingeholt und ausgewertet werden.

2. Alle IT-Systeme (z. B. auch TK-Anlagen, Netzkoppelelemente und Sicherheitsgateways) und IT-Anwendungen müssen in das Patchmanagement einbezogen werden.

   Früher galt die Empfehlung, stets Viren-Schutzprogramme, Browser und Betriebssystem aktuell zu halten. Inzwischen muss diese Beschränkung aufgehoben werden: Alle Anwendungen können Schwachstellen haben, die sich - z. B. durch Pufferüberläufe - für Angriffe ausnutzen lassen.

3. Sicherheitsrelevante Patches und Updates müssen regelmäßig eingespielt werden. Nach Möglichkeit muss jedes Update auf einem Testsystem getestet werden, da Updates nicht immer fehlerfrei funktionieren.

4. Das Management muss in geeigneter Form über alle neuen technischen Entwicklungen informiert werden, die Auswirkung auf die Risikobetrachtung haben könnten.

→ Weitere Informationen:

- GS-K, M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems
- GS-K, M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
- GS-K, M 2.200 Managementreporte und -bewertungen der IT-Sicherheit
- GS-K, M 2.283 Software-Pflege auf Routern und Switches
- CERT-Bund: http://www.bsi.bund.de/certbund
- NIST SP 800-40: Creating a Patch and Vulnerability Management Program, http://csrc.nist.gov/publications/nistpubs/index.html

Umgang mit Sicherheitslücken, für die kein Patch zur Verfügung steht

Sind Sicherheitsprobleme bekannt, die noch nicht durch Updates oder Patches behoben werden können, muss eventuell zusätzliche Sicherheitshardware bzw. Sicherheitssoftware eingesetzt werden. In besonders kritischen Fällen müssen die betroffenen Dienste deaktiviert bzw. die Verarbeitung gefährlicher Dateien verhindert werden. In der Praxis besteht häufig eine zu große Hemmschwelle, weitreichende Maßnahmen zu ergreifen. Viele Sicherheitsbeauftragte fordern beispielsweise bei akuter Gefahr die Mitarbeiter lediglich auf, E-Mails mit bestimmten Merkmalen nicht zu öffnen und besonders misstrauisch zu sein. Wenn ein hohes Risiko besteht, weil ein gefährliches Schadprogramm kursiert, das nicht vom Virenschutz erkannt wird, reicht ein Appell an die Vorsicht nicht aus. Die E-Mail-Nutzung sollte dann technisch für eine gewisse Zeit eingeschränkt oder sogar ganz unterbunden werden. Bestimmte Dateianhänge könnten z. B. aus E-Mails herausgefiltert und in Quarantäne gestellt werden, bis das Viren-Schutzprogramm mit geeigneten Signaturen nachgerüstet ist. Ist ein bestimmter Browser durch eine Schwachstelle gefährdet, sollte ein alternatives Produkt zum Surfen verwendet werden.

ANGRIFFE MIT BILDERN: DIE WMF-SCHWACHSTELLE

In der Weihnachtszeit 2005 wurde bekannt, dass durch speziell präparierte WMF-Bilder auf Windows-Rechnern beliebiger Code ausgeführt werden kann. Der Besuch einer Webseite oder das bloße Abspeichern einer entsprechenden Datei konnte unter Umständen ausreichen, um den Schadcode auszuführen. Erst mehrere Tage nach den ersten Angriffen standen Signaturen für Viren-Schutzprogramme und ein Patch für das Betriebssystem zur Verfügung.

Britische Medien berichteten, dass Angestellte des Parlaments bereits unmittelbar nach Veröffentlichung des ersten Exploits mit präparierten WMF-Dateien angegriffen wurden. Die Sicherheitsbehörden attestierten den Angreifern große Professionalität und gingen von einer hohen Sicherheitsgefährdung aus. In diesem Fall wäre ein generelles Verbot der Internetnutzung am Arbeitsplatz angemessen gewesen.

Software am Ende ihres Lebenszyklus: Einstellung des Herstellersupports

Sehr problematisch ist es, wenn Softwarehersteller den Support für ein Produkt einstellen und keine Sicherheitsupdates mehr anbieten. In diesem Fall müssen Konsequenzen gezogen werden, bevor Sicherheitslücken oder Designfehler bekannt werden. Dies gilt nicht nur für Betriebssysteme, sondern für alle Anwendungen. Ein weiterer produktiver Einsatz in Bereichen mit hohem Schutzbedarf ist ohne zusätzliche Sicherheitsmaßnahmen nicht mehr zu verantworten.

HINWEIS: MICROSOFT SUPPORT LIFECYCLE

Microsoft bietet mindestens 10 Jahre Support für Businessprodukte an: Auf den umfassenden „Mainstream Support“ folgt der reduzierte und z. T. kostenpflichtige „Extended Support“. Sicherheitsupdates werden bis zum Ende der Extended-Support-Phase (kostenlos) zur Verfügung gestellt. Auf den Webseiten von Microsoft sind für alle Produkte die Lebenszyklusphasen verzeichnet.

Einsatz von Datei-Viewern

Dateien aus unbekannten oder nicht vertrauenswürdigen Quellen stellen ein hohes Risiko dar, besonders wenn das Dateiformat die Ausführung von Makros oder Aktiven Inhalten erlaubt. Ein reines Anzeigeprogramm ohne Makrofähigkeiten erhöht daher die Sicherheit deutlich. Von Microsoft gibt es z. B. kostenlose Anzeigeprogramme für alle Officeformate.

Anschluss mobiler Geräte ans Produktivnetz

Wenn Rechner am Produktivnetz angeschlossen sind, werden sie regelmäßig mit Softwareupdates versorgt und unterliegen allen zentral administrierten Kontrollmaßnahmen. Bei mobil genutzten Geräten kann nicht immer sichergestellt werden, dass Software und Einstellungen aktuell sind. Nutzen diese Geräte einen fremden Internetzugang (privat, Hotel, WLAN-Hotspot etc.) oder spielt der Anwender selbständig Software auf, besteht ein Risiko. Mobile Geräte dürfen daher nur dann wieder mit vollen Rechten das Produktivnetz nutzen, wenn sie mit aktuellen Schutzprogrammen untersucht wurden und alle Hausstandards erfüllen.

→ **Weitere Informationen:**

BSI-Broschüre „Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen“,
http://www.bsi.bund.de/literat/doc/mobile/index.htm

Automatische Start- und Vorschaufunktionen deaktivieren

Autostart-Funktionen für CD-Laufwerke oder USB-Sticks müssen deaktiviert werden. Es ist zu empfehlen, grundsätzlich alle Autostart-Funktionen zu deaktivieren, da sich je nach Betriebssystemsversion USB-Sticks als Wechselfestplatte oder USB-Medium ansprechen lassen.

Bei E-Mail-Programmen müssen für den Posteingangsordner alle Vorschaufunktionen abgeschaltet werden.

7 Sichere Vernetzung und Internetnutzung

Die meisten Schadprogramme nutzen das Internet, um auf Rechner zu gelangen oder um mit dem Angreifer zu kommunizieren. Die vorgestellten Maßnahmen haben daher folgende Ziele:

1. Schadprogramme sollen möglichst schon an der Netzaußengrenze abgefangen werden.
2. Ein infizierter Rechner soll nicht von außen kontrollierbar sein.
3. Die Aktivitäten eines Schadprogramms sollen auf den infizierten Rechner beschränkt bleiben. Ein Zugriff über das interne Netz auf weitere Ressourcen und Daten soll nicht möglich sein.
4. Gesammelte Daten sollen nicht zum Angreifer gesendet werden.
5. Netzaktivitäten und unerlaubte Dateizugriffe eines Schadprogramms sollen detektiert werden und Alarm auslösen.

7.1 Sicheres Netzdesign

Erstellung eines Netzkonzeptes unter Sicherheitsaspekten

Eine Übersicht über Geschäftsprozesse, Informationen, Daten und Anwendungen und eine Risikobetrachtung sind notwendige Vorarbeiten, wenn ein Intranet und die Anbindung an das Internet geplant werden. Am sichersten sind Daten in einem Netz ohne Außenverbindung oder sogar auf Stand-alone-Systemen. Bei sehr hohen Sicherheitsanforderungen stehen die Kosten für Sicherheitsmaßnahmen in keinem vernünftigen Verhältnis zum Nutzen einer uneingeschränkten Internetanbindung. Zwei Rechner auf dem Schreibtisch können daher in Einzelfällen sinnvoll sein: ein spezielles System ohne Netzanbindung für sehr schutzbedürftige Daten und ein vernetzter Arbeitsplatz-Rechner für „normale“ Büroarbeiten (siehe Maßnahme „Nutzung alternativer Web-Zugangsmethoden“).

Um Informationen mit hohen Sicherheitsanforderungen angemessen zu schützen, muss die Informationsverarbeitung in verschiedene Bereiche mit unterschiedlichem Schutzbedarf eingeteilt werden. In den besonders zu schützenden Bereichen bzw. bei der Verarbeitung hoch vertraulicher Daten können dann weitreichende Sicherheitsmaßnahmen getroffen werden, während gleichzeitig für weniger schutzbedürftige Routinetätigkeiten ein niedrigeres Sicherheitsniveau gilt. Diese Teilung spart Kosten und erhöht die Akzeptanz der Mitarbeiter. Was in der „normalen“ Welt selbstverständlich ist, sollte auch in der Informationsverarbeitung gelten. Auch ein internes Netz muss daher segmentiert werden. Jeder Mitarbeiter darf nur auf Daten zugreifen, die er für seine Arbeit tatsächlich benötigt. Ein Schutz auf Netzebene ist wesentlich sicherer als über Zugriffsberechtigungen (Hardware ist sicherer als Software).

Arbeitsgruppen sollten daher nach Möglichkeit ein eigenes Netzsegment mit geschützten Grenzen erhalten. Beispielsweise hat ein forschendes Unternehmen sehr hohe Sicherheitsanforderungen für die Entwicklungsabteilung. Die Verwaltung ist weniger durch Spionage gefährdet. Für die Entwicklungsabteilung muss daher ein separates, sehr gut gesichertes Netz betrieben werden. In diesem Beispiel haben die Abteilungen Entwicklung und Verwaltung unterschiedliche Sicherheitsanforderungen. Aber auch bei gleichem Schutzbedarf von zwei Abteilungen ist eine Trennung von Netzbereichen notwendig, wenn die Mitarbeiter keinen Zugriff auf Daten der jeweils anderen Abteilung haben sollen. Folgende Regeln sollten daher immer beachtet werden.

1. Die Verarbeitung vertraulicher Daten muss auf bestimmte Bereiche innerhalb des Intranets begrenzt werden. IT-Systeme und Kommunikationsverbindungen mit einem hohen Schutzbedarf sollten jeweils in einem eigenen Teilnetz betrieben werden.

2. Netzgrenzen sind ausreichend zu schützen. Der Schutz durch Hardware hat dabei Vorrang vor Softwarelösungen.

3. Bei hohen Sicherheitsanforderungen muss die Anbindung an fremde oder öffentliche Netze besonders sorgfältig geschützt werden. Daten mit sehr hohem Schutzbedarf sind ausschließlich auf Systemen ohne Internetanbindung zu verarbeiten.

Zentraler Schutz der Netzgrenzen mit einem Sicherheitsgateway

Zum zentralen Schutz der Netzaußengrenzen sowie besonders gefährdeter interner Grenzen sind verschiedene Sicherheitsgateways (Firewalls) erforderlich. „Sicherheitsgateway“ drückt präziser als „Firewall“ aus, dass moderne Systeme aus verschiedenen soft- und hardware-technischen Komponenten bestehen. Ein Sicherheitsgateway schränkt durch Paketfilter und Application Level Gateways (ALG) die Kommunikationsmöglichkeiten ein und trägt so zur sicheren Kopplung von IP-Netzen bei. Es gelten folgende Mindestvoraussetzungen für die Kombination aus Paketfiltern und Application Level Gateways:

- **Default-deny-Strategie: „Alles ist verboten, was nicht ausdrücklich erlaubt ist.“**

  Die Default-Einstellung der Filterregeln und die Anordnung der Komponenten muss sicherstellen, dass alle Verbindungen, die nicht explizit erlaubt sind, blockiert werden. Dies muss auch bei einem völligen Ausfall der Komponenten des Sicherheitsgateways gelten.

- **Trennung zweier Teilnetze des internen Netzes mit unterschiedlichem Schutzbedarf**

  Falls von einem weniger vertrauenswürdigen Netzsegment aus auf einen Dienst in einem Teilnetz mit hohem Schutzbedarf zugegriffen werden soll, ist der Zugriff über ein ALG abzusichern. Ansonsten ist meistens ein Paketfilter ausreichend.

- **Trennung eines Teilnetzes mit besonderen Sicherheitsanforderungen von einem anderen internen Teilnetz**

  Ein mehrstufiger Aufbau aus Paketfilter - ALG - Paketfilter ist erforderlich. Dieser kann jedoch nur als Grundlage für sehr hohe Sicherheit dienen. In diesem Fall ist eine ergänzende Sicherheitsbetrachtung notwendig.

- **Trennung des eigenen Netzes vom Internet**

  Grundsätzlich ist ein mehrstufiger Aufbau aus Paketfilter - ALG - Paketfilter notwendig. Zumindest für Dienste wie E-Mail und HTTP wird der Einsatz eines entsprechenden Proxyservers dringend empfohlen.

→ BSI Informationen:

- Konzeption von Sicherheitsgateways
  Dieses Dokument beschreibt Möglichkeiten zur modularen Strukturierung von Sicherheitsgateways in IP-Netzen, wobei abhängig vom Schutzbedarf grundlegende Konzepte mit Vorteilen und Risiken erläutert werden,
  http://www.bsi.bund.de/fachthem/sinet/loesungen_netze/konzsichgw.htm
- Anforderungen an Module von Sicherheitsgateways/ Firewalls,
  http://www.bsi.bund.de/fachthem/sinet/loesungen_netze/fw-anf.htm
- GS-K, B 3.301 Sicherheitsgateway (Firewall)
- GS-K, M 2.73 Auswahl geeigneter Grundstrukturen für Sicherheitsgateways

→ Weitere Quellen:

- SANS Institute: http://www.sans.org/rr/whitepapers/firewalls/
- NISCC Technical Note 10/04: Understanding Firewalls,
  http://www.cpni.gov.uk/docs/re-20041221-00963.pdf
- NIST SP 800-41: Guidelines on Firewalls and Firewall Policy,
  http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf

Zentraler Virenschutz

1. Am zentralen E-Mail-Gateway muss ein Viren-Schutzprogramm eingesetzt werden, das ein- und ausgehende E-Mails prüft.

2. Alle weiteren Internet-Dienste (HTTP, FTP, ...) sollten ebenfalls mit Schutzsoftware geschützt werden.

Einsatz von lokalen Desktop-Firewalls

Auf jedem Arbeitsplatz-Rechner sollte eine Desktop-Firewall installiert sein, um den ausgehenden Datenverkehr zu kontrollieren. Auch wenn aufgrund ungepatchter Schwachstellen ein Programm für die Nutzung des Internets vorübergehend gesperrt werden soll, leistet eine Desktop-Firewall gute Dienste. Waren früher Desktop-Firewalls reine Paketfilter, findet man heute weitere Funktionen:

- Whitelist mit zugelassenen Applikationen
- Kontrolle der zu startenden Applikationen
- Kontrolle der Netzzugriffe
- Überwachung von Prozessen, zugehöriger Adressbereiche und von Systemdateien (z. B. DLL-Injection, Prozess-Injection, Code-Injection, Registry-Zugriffe)
- Mechanismen zum Eigenschutz
- signaturbasierte Intrusion Detection

Zur Absicherung der Clients in einem Behörden- oder Unternehmensnetz sollten daher nur Produkte ausgewählt werden, die alle aufgezählten Funktionen bieten können.

Die Einsatzbedingungen in einem Behörden- oder Unternehmensnetz unterscheiden sich deutlich von einem Einzelrechner mit Internetzugang und müssen bei der Beschaffung berücksichtigt werden:

- Einsatz auf Arbeitsplatz-PCs in großen Netzen
- Betrieb innerhalb eines geschlossenen Netzes (nicht direkt am Internet)
- Administration erfolgt zentral und remote
- kein Mehrbenutzersystem, dafür Gruppen und Rollen
- Firewall muss in einer eingeschränkten Benutzerumgebung funktionieren
- Protokollierung und zentrale Auswertung der Logdaten sind notwendig

Bei der Auswahl einer Desktop-Firewall muss darauf geachtet werden, dass sie problemlos zusammen mit dem lokalen Viren-Schutzprogramm und den Administrationstools funktioniert.

Sicherheit Virtueller Netze

Um den Broadcast-Verkehr in einem „geswitchten“ Netz einzuschränken, lassen sich virtuelle Netze (VLANs) bilden. Hierbei wird innerhalb eines physikalischen Netzes eine logische Netzstruktur abgebildet, in der funktionell zusammengehörende Arbeitsstationen und Server zu einem virtuellen Netz verbunden werden. Jedes VLAN bildet eine separate Broadcast-Domäne und kann sich über ein ganzes geswitchtes Netz erstrecken.

Entgegen mancher Werbeaussagen wurden VLANs nicht entwickelt, um Sicherheitsanforderungen bei der Trennung von Netzen zu erfüllen. VLANs bieten eine Vielzahl von Angriffspunkten, so dass insbesondere für die Trennung von schutzbedürftigen Netzen immer zusätzliche Maßnahmen umzusetzen sind. Auf einem Switch sollten keine VLANs mit unterschiedlichem Schutzbedarf konfiguriert sein. Soll dies aus wichtigen Gründen trotzdem geschehen, so müssen in jedem Fall zusätzliche Sicherungsmaßnahmen ergriffen werden. Keinesfalls darf das Netz einer DMZ, die zwischen dem internen Netz und dem Internet steht, als VLAN auf dem selben Switch wie das interne Netz konfiguriert sein.

→ Weitere Informationen:

- GS-K, B 3.302 Router und Switche
- GS-K, M 2.277 Funktionsweise eines Switches

Schutz von Remote-Access- und Fernwartungszugängen

Alle Fernwartungs- und Remote-Access-Zugänge müssen speziell gesichert werden. Dabei muss darauf geachtet werden, dass viele IT-Systeme - in erster Linie TK-Anlagen - Fernwartungszugänge haben. Diese werden leicht übersehen, wenn sie nicht genutzt werden. Fernwartungszugänge sollten nur temporär auf Anfrage und für bekannte Adressen freigeschaltet werden.

→ Weitere Informationen:

GS-K, B 4.4 Remote Access Dienste

Verschlüsselung der Netzkommunikation

Sicherheitsgewinn	Aufwand Realisierung
hoch	hoch

Daten können bei der Übertragung abgehört, verändert oder zur späteren Wiedereinspeisung in das Netz (Replay-Attacke) missbraucht werden. Daher müssen zur Verarbeitung hoch vertraulicher Daten innerhalb des Intranets Verschlüsselungsverfahren mit gegenseitiger Authentisierung der Kommunikationspartner eingesetzt werden.

→ **Weitere Informationen:**

GS-K, M 5.68 Einsatz von Verschlüsselungsverfahren zur Netzkommunikation

Intrusion Detection Systeme

Sicherheitsgewinn	Aufwand Realisierung	Aufwand Betrieb
mittel	mittel - hoch	hoch

Der Schutz durch ein Sicherheitsgateway ist als alleinige Maßnahme in vielen Fällen nicht mehr ausreichend, um die Kommunikation mit dem Internet zu schützen. Intrusion-Detection-Systeme (IDS) erlauben eine - wenn auch eingeschränkte - Überwachung des Netzverkehrs sowie der Systeme und Anwendungen auf Angriffe und Sicherheitsverletzungen. Es ist in einigen Fällen sogar möglich, Angriffsmuster zu beschreiben, wenn die Hersteller von Viren-Schutzprogrammen noch keine Signaturen zur Erkennung eines bestimmten Schadprogramms liefern können. (Beispielsweise könnte nach Exploits oder bestimmten IP-Adressen, die aus CERT-Berichten oder anderen Warnungen bekannt sind, gesucht werden).

IDS sind jedoch keine Wunderwaffe und erfordern einen hohen manuellen Aufwand bei Konfiguration und Auswertung der Logdateien.

→ **Weitere Informationen:**

- BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen, http://www.bsi.bund.de/literat/studien/ids02/index.htm
- NIST SP 800-31 Intrusion Detection Systems, http://csrc.nist.gov/publications/nistpubs/index.html

7.2 Zugelassene Protokolle und Dienste

Dienstvereinbarung zur Internetnutzung

In einer Dienstvereinbarung muss verbindlich geregelt werden, ob bzw. in welchem Umfang die private Internetnutzung erlaubt wird. In der Dienstvereinbarung sollte auch beschrieben werden, wie E-Mail-Verkehr und Webzugriffe protokolliert werden und in welcher Form Auswertungen und Kontrollen durchgeführt werden. Siehe auch Maßnahme „Ausarbeitung von Sicherheitsrichtlinien“ im Kapitel „Integration der Mitarbeiter in den Sicherheitsprozess“.

Blockierung nicht benötigter Protokolle und Dienste

Es sollten nur Dienste und Protokolle genutzt werden, die für dienstliche Zwecke benötigt werden. Es lassen sich folgende Empfehlungen geben:

- Klartextprotokolle wie Telnet und FTP sollten nach Möglichkeit nur noch in geschlossenen Netzen benutzt werden und zur Kommunikation über öffentliche Netze durch sicherere Alternativen (SSH/ SCP) ersetzt werden. Auch im internen Netz sollten sie nur noch verwendet werden, wenn aus zwingenden Gründen ein Umstieg auf SSH oder ein anderes sicheres Protokoll nicht möglich ist.
- Auch POP sollte allenfalls noch intern verwendet werden. Sollen von einem externen Mailserver (etwa bei einem Provider) E-Mails abgerufen werden, so sollte der Variante „POP über SSL“ oder IMAP der Vorzug gegeben werden.
- Internet Relay Chat, Instant Messaging und Filesharing-Dienste sollten nicht freigeschaltet werden.
- Regeln, die mit Komforteinbußen verbunden sind, sollten mit zentralen Mechanismen technisch erzwungen werden. Eine Filterung am Sicherheitsgateway ist wesentlich einfacher als die Nutzung von Mechanismen in Anwendungsprogrammen oder auf Ebene des Betriebssystems.

→ Weitere Informationen:

- GS-K, M 5.39 Sicherer Einsatz der Protokolle und Dienste
- GS-K, M 2.75 Geeignete Auswahl eines Application-Level-Gateways (Hier finden sich grundlegende Aussagen zur Verwendung bestimmter Protokolle und Dienste.)
- GS-K, M 4.202 Sichere Netz-Grundkonfiguration von Routern und Switches

Unterscheidung zwischen „internen“, „vertrauenswürdigen“ und „unbekannten“ Seiten

Beim Netzsicherheitskonzept sollte zwischen „internen“, „vertauenswürdigen“ externen und „unbekannten“ externen Seiten unterschieden werden. Dabei darf aber auch vertrauenswürdigen Seiten nicht blind vertraut werden - auch vertrauenswürdige Seiten können das Opfer von Hackern werden, wie das nachfolgende Beispiel zeigt.

SUPPORT DER GEFÄHRLICHEN ART

Anfang 2006 wurde im Internet berichtet, dass die Internet- Support-Foren eines Prozessor-Herstellers offenbar gehackt worden waren. Im Quellcode befand sich kurzzeitig ein IFrame-Tag, das eine Seite von einem externen Server nachlud. Diese enthielt gleich mehrere Exploits für bekannte Internet-Explorer-Lücken, um Dateien nachzuladen und auszuführen.

Soll das Konzept der „Sicherheitszonen“ unter Windows verwendet werden, finden sich Erläuterungen dazu in der referenzierten IT-Grundschutz-Maßnahme. Die Einstellungen der Sicherheitszonen werden sowohl vom Internet Explorer als auch von Outlook verwendet. Aufgrund dieses komplizierten Designs ist eine zentrale Verwaltung am Sicherheitsgateway zu bevorzugen.

→ **Weitere Informationen:**

- Sicherheitszonen unter Windows: GS-K, M 4.165 Sichere Konfiguration von Outlook 2000
- NISCC Technical Note 05/03 "Configuration and Use of Web Browsers", http://www.cpni.gov.uk/docs/re-20030801-00725.pdf

Nutzung von HTTPS bei vertrauenswürdigen externen Seiten

Wenn regelmäßig schützenswerte Daten mit einer vertrauenswürdigen externen Stelle ausgetauscht werden (z. B. Zahlungsverkehr, E-Government), muss dieser Übertragungsweg geschützt werden. Nach Möglichkeit sollten Verbindungen zu vertrauenswürdigen externen Seiten daher durch HTTPS geschützt werden. Die Gegenseite kann so auch authentisiert werden. Diese Verbindungen sollten zur Wahrung der Vertraulichkeit der Daten nicht über einen SSL-Proxy geführt werden. Da dies mit Sicherheitsrisiken verbunden ist (siehe Maßnahme „Absicherung von SSL"), sollten nur wenige externe Seiten nach sorgfältiger Auswahl für dieses Verfahren freigeschaltet werden.

Absicherung von SSL

Die Verschlüsselung von Daten stellt ein großes Problem für den wirksamen Einsatz von zentralen Schutzmechanismen wie Firewall oder Viren-Schutzprogramm dar. Filter innerhalb des Sicherheitsgateways sind nicht mehr in der Lage, die Nutzdaten auf der Anwendungsschicht auf Schadprogramme zu untersuchen oder Aktive Inhalte zu blocken. Auch die Protokollierungsmöglichkeiten werden durch eine Verschlüsselung stark eingeschränkt.

- SSL-Verbindungen sollten daher über einen SSL-Proxy geführt werden. Ein SSL-Proxy steht zwischen SSL-Server und -Client und entschlüsselt den Datenverkehr temporär. Auf diese Weise lassen sich Aktive Inhalte aus Webseiten, die mittels HTTPS abgerufen werden, entfernen und Viren-Schutzprogramme einbinden.

- Nur bei Verbindungen zu vertrauenswürdigen externen Seiten kann in Einzelfällen auf einen SSL-Proxy verzichtet werden, wenn eine Ende-zu-Ende-Verschlüsselung aufgrund von Datenschutzanforderungen notwendig ist.

- Wird kein SSL-Proxy verwendet, sollte der Zugang zu Webmail-Angeboten untersagt und technisch verhindert werden. Über einen Webmail-Zugang, der in der Regel über HTTPS erfolgt, lassen sich sonst unbemerkt große Datenmengen von innen nach außen bringen.

- Wird ein SSL-Proxy verwendet, müssen die Mitarbeiter im Rahmen der Dienstvereinbarung zur Internetnutzung darüber informiert werden. Dies ist besonders dann notwendig, wenn die Privatnutzung von Webmail oder Online-Banking gestattet ist.

Umgang mit Aktiven Inhalten

Eine gute Übersicht über die Gefahren durch Aktive Inhalte bietet der unten referenzierte Artikel im BSI Forum der Zeitschrift <kes>. Der Missbrauch Aktiver Inhalte stellt eine große Gefahr bei der Internutzung dar.

Anwenderseite

Die Ausführung Aktiver Inhalte sollte im Browser des Anwenders standardmäßig deaktiviert werden. Ausnahmen dürfen nach sorgfältiger Prüfung nur für interne Seiten gemacht werden.

Bei einzelnen vertrauenswürdigen externen Seiten können Java und Javascript freigeschaltet werden, wenn dienstliche Gründe dies erforderlich machen. Andere Aktive Inhalte - insbesondere ActiveX - sollten mit externen Seiten nicht verwendet werden.

Angebot von Webinhalten

Um Kunden oder Geschäftspartner nicht dazu zu zwingen, Aktive Inhalte freizugeben, sollten eigene Webanwendungen und Webangebote auch ohne Aktive Inhalte voll zugänglich sein. Konzepte und Beispiele für die Erstellung von Webseiten ohne Aktive Inhalte finden sich im E-Government-Handbuch des BSI.

→ Weitere Informationen:

- Aktive Inhalte (Teil 1): Grundlagen und Gefahren, BSI Forum in der Zeitschrift <kes> Nr. 5 2005, http://www.bsi.bund.de/literat/forumkes.htm
- http://www.bsi.bund.de/fachthem/sinet/gefahr/aktiveinhalte/index.htm
- E-Government-Handbuch des BSI, Modul E-Government ohne Aktive Inhalte, http://www.bsi.bund.de/fachthem/egov/download/4_EGovoAI.pdf
- Technischer Anhang zum o. g. Modul mit Codebeispielen, http://www.ohne-aktive-inhalte.de/
- GS-K, M 4.100 Sicherheitsgateways und Aktive Inhalte

Nutzung alternativer Web-Zugangsmethoden

Die Nutzung des Internets ist aufgrund von Schwachstellen in Anwendungsprogrammen oder menschlichem Fehlverhalten immer mit Gefahren verbunden. Besonders wenn gelegentlich auch Internetseiten mit Aktiven Inhalten genutzt werden müssen, bedarf der Internetzugang am Arbeitsplatz-Rechner sorgfältiger Planung.

Unter → *Weitere Informationen* sind zwei Artikel des BSI für die Zeitschrift <kes> aufgeführt, die sehr ausführlich verschiedene Web-Zugangsmethoden miteinander vergleichen. Hier deshalb nur stellvertretend eine kurze Vorstellung von vier Möglichkeiten:

Methode	**Web-Funktionalität**	**Bedienungskomfort**	**Sicherheit**	**Realisierungsaufwand**
ungeschütztes Surfen	uneingeschränkt	hoch	nicht vorhanden	minimal
Live-System	uneingeschränkt	niedrig – mittel	mittel – hoch	mittel
Stand-alone Internet-PC	uneingeschränkt	niedrig	sehr hoch	mittel
virtueller Rechner am Arbeitsplatz	uneingeschränkt	hoch	hoch	sehr hoch
Remote-Controlled Browsers System	uneingeschränkt	hoch	sehr hoch	hoch

- **Live-System**

  Ein Live-System ist ein Betriebssystem, das ohne Installation und ohne Beeinflussung der Festplatte direkt von einem Speichermedium (z. B. von CD) gebootet werden kann. Wird ein Zugriff auf die Festplatte zuverlässig unterbunden, können Aktive Inhalte keinen Schaden auf der Festplatte erzeugen, und Schadprogramme können sich nicht festsetzen. Nach Abschluss der Surf-Sitzung und erneutem Booten von der Festplatte steht das zu schützende ursprüngliche System wieder zur Verfügung. Individuelle Konfigurationen können mit auf der Live-CD oder auf einem wiederbeschreibbaren Medium (z. B. USB-Stick) abgelegt werden. Folgende Anforderungen sind an eine Live-CD zu stellen:

  - Es ist kein Zugriff auf die Festplatte möglich.
  - Es ist kein Zugriff auf Netzlaufwerke möglich.
  - Es wird ein gehärtetes, minimales Betriebssystem verwendet.
  - Eine Desktop-Firewall ist installiert.

  Diese Variante hat zwei gravierende Nachteile: Da der Rechner zunächst heruntergefahren werden muss und das Booten mit einer Live-CD langsam ist, wird diese Lösung in der Regel von den IT-Anwendern abgelehnt. Weiterhin wird aus Sicherheitsgründen das Booten eines Arbeitsplatz-PCs mit einem alternativen Bootmedium fast überall unterbunden.

- **Stand-alone Internet-PC**

  Ein Browser wird mit vollem technischen Funktionsumfang auf einem dedizierten PC ohne Verbindung zum Hausnetz betrieben. Da ein solcher Stand-alone-PC in der Regel aber in einem separaten Raum „allein steht“, stößt er bei den Anwendern auf geringe Akzeptanz.

- **Virtueller Rechner am Arbeitsplatz**

  Auf dem Host-Betriebssystem des Arbeitsplatz-PC wird ein virtueller Rechner eingerichtet, der den Browser zum freien Surfen kapselt. Die beiden Rechner sind an unterschiedliche logische Netze angeschlossen. Auch dieser Mechanismus lässt sich durch Schadprogramme aushebeln, der Programmieraufwand und die Anforderungen an die Fähigkeiten des Angreifers sind jedoch sehr hoch.

- **Remote-Controlled Browsers System (ReCoBS)**

  Unter einem Remote-Controlled Browsers System versteht das BSI den Webzugang mithilfe von speziell gesicherten Terminalserver-Systemen. Das ReCoBS ist ein modularer Bestandteil des Sicherheitsgateways und sorgt dafür, dass die Ausführung und Darstellung Aktiver Inhalte auf unterschiedlichen Rechnersystemen erfolgt. Webinhalte werden nur auf einem Terminalserver außerhalb des Hausnetzes ausgeführt. Dort befinden sich Browser, die von den Arbeitsplätzen ferngesteuert werden. An die schutzbedürftigen Arbeitsplätze werden statt Aktiver Inhalte nur unkritische grafische Informationen übermittelt. Ein ReCoBS benötigt ein umfassendes Sicherheitskonzept und ist weit mehr als ein Terminalserver „von der Stange“. Der für ein ReCoBS erforderliche Realisierungsaufwand ist hoch - besonders dann, wenn Dateidownload und Drucken ebenfalls abgesichert werden sollen. Eine ReCoBS-Lösung ermöglicht dafür gleichzeitig ein Maß an Sicherheit, Web-Funktionalität und Bedienkomfort, wie es von keiner der verbreiteten Web-Zugangsmethoden geboten wird.

→ Weitere Informationen:

- Remote-Controlled Browsers System: http://www.bsi.bund.de/fachthem/sinet/gefahr/aktiveinhalte/schutzmoeglichkeiten/recobs/index.htm
- Aktive Inhalte (Teil 2): Sichere Nutzung - Überblick und Empfehlungen, BSI Forum in der Zeitschrift <kes> Nr. 6 2005, http://www.bsi.bund.de/literat/forumkes.htm
- Aktive Inhalte (Teil 3): Remote-Controlled Browsers System - Sichere und bequeme Nutzung von Aktiven Inhalten, BSI Forum in der Zeitschrift <kes> Nr. 1 2006, http://www.bsi.bund.de/literat/forumkes.htm
- GS-K, B 3.208 Internet-PC

Downloadmöglichkeiten einschränken

Das Laden von Dateien aus dem Internet ist prinzipiell mit Gefahren verbunden. Je nach Sicherheitsanforderungen sind Einschränkungen empfehlenswert. Folgende Optionen sollten überlegt werden:

Verboten sind	Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
nur „gefährliche“ Dateitypen	mittel - hoch	niedrig	mittel - hoch
alle Dateien	hoch	niedrig	hoch

- Beschränkung der Dateitypen

  Dateitypen, die häufig von Angreifern manipuliert werden, dürfen am Arbeitsplatz nicht heruntergeladen werden. In erster Linie sind ausführbare und komprimierte Dateien zu sperren.

- Dateidownload wird grundsätzlich nicht gestattet

  Bei hohen Sicherheitsanforderungen sollten keine Dateien von unbekannten Seiten geladen werden (Ausnahme HTML ohne Aktive Inhalte). Der Download von vertrauenswürdigen externen Seiten kann auf Antrag freigegeben werden.

- Dateidownload erfolgt über ein Sandbox-System (experimentell)

  Eine Datei wird zunächst auf ein Sandbox-System geladen, dort von verschiedenen Viren-Schutzprogrammen mit signaturbasierten und heuristischen Methoden untersucht und dann mit dem jeweiligen Anwendungsprogramm ausgeführt. Nach der Ausführung wird das Sandbox-System auf Veränderungen untersucht. Erst wenn die Datei als harmlos eingestuft wurde, wird sie an den Internetnutzer, der den Download angefordert hat, weitergeleitet. Diese Lösung ist sehr aufwendig, zumal die erhältlichen Sandbox-Systeme technisch noch nicht ausgereift sind.

Zusätzliche Authentisierungsmechanismen

Sicherheitsgewinn	Aufwand Realisierung	Komforteinbußen
mittel	mittel	mittel - hoch

Um Informationen an einen Angreifer zu senden, müssen Schadprogramme unbemerkt eine Internetverbindung herstellen oder eine E-Mail verschicken. Wenn das Öffnen einer externen Webseite oder das Abschicken einer E-Mail mit einer Aktion des IT-Anwenders verknüpft wird, erhöht sich der Programmieraufwand für einen Angreifer. Es sind verschiedene Authentisierungsverfahren denkbar:

Passworteingabe, Token, Chipkarte, Bestätigung einer Nachfrage, Abfrage eines biometrischen Merkmals etc. Eine erfolgreiche Authentisierung könnte den Webzugang für eine bestimmte Zeit frei schalten, so dass nicht für jeden Link eine Aktion notwendig ist. Abgebrochene oder fehlerhafte Authentisierungsversuche sollten protokolliert und ausgewertet werden. Wird ein bestimmter Schwellenwert überschritten, sollte automatisch eine Warnmeldung für den zuständigen Administrator generiert werden. Je häufiger das Authentisierungsverfahren gewechselt oder leicht verändert wird, desto schwerer wird sich ein Angreifer bei seiner Überwindung tun.

Es gibt Schadprogramme, die eigene E-Mail-Engines oder Chat-Clients mitbringen. Grundvoraussetzung für den Erfolg der Maßnahme ist daher, dass nur bekannte und zugelassene Programme bzw. Dienste zur Internetnutzung zugelassen sind.

7.3 E-Mail und Browser

Auswahl und Konfiguration von Hard- und Software

1. Es sollte nur aktuelle Software mit guter Sicherheitshistorie eingesetzt werden. Produkte, die häufig Schwachstellen enthalten oder deren Hersteller trotz bekannter Fehler nur unregelmäßig Updates zur Verfügung stellen, sollten gemieden werden.

   Bei der Auswahl von E-Mail-Programmen sollte berücksichtigt werden, dass das Risiko beim Einsatz weit verbreiteter Programme mit großer Funktionsvielfalt am höchsten ist. Besonders wenn ein E-Mail-Programm sehr eng mit dem Betriebssystem oder Datenbanken verzahnt ist, steigt die Gefahr, dass Schwachstellen im Programmcode sich für Angriffe ausnutzen lassen.

2. Die E-Mail-Programme der IT-Anwender müssen durch den Administrator so vorkonfiguriert sein, dass ohne weiteres Zutun der Benutzer maximale Sicherheit erreicht werden kann.

3. Für E-Mails und zum Browsen dürfen nur Accounts mit eingeschränkten Benutzerrechten genutzt werden. Das Surfen mit Administratorrechten birgt hohe Gefahren, da ein Schadprogramm sich unter Umständen so tief ins System einnisten kann, dass es kaum noch detektiert werden kann.

4. Es sollten nur Arbeitsplatz-Systeme für E-Mail oder zum Browsen verwendet werden, die keine Server- oder Netzwerkdienste anbieten.

5. Es dürfen keine unnötigen Browser-Plugins installiert werden.

6. Für den Browser-Cache sollte nicht das Standard-Verzeichnis gewählt werden. Jede Abweichung vom Standard ist eine zusätzliche Hürde für einen Angreifer.

→ Weitere Informationen:

- GS-K, B 5.12 Exchange 2000/ Outlook 2000
- GS-K, M 4.161 Sichere Installation von Exchange/Outlook 2000
- GS-K, M 4.165 Sichere Konfiguration von Outlook 2000

Maßnahmen bei eingehenden E-Mails

Unerwünschte E-Mails, Spam-Abwehr

Das Öffnen offensichtlicher Spam-Mails sollte untersagt werden (z. B. in einer Dienstvereinbarung oder einer eigenen Richtlinie zur E-Mail-Nutzung). Wenn eine E-Mail dem IT-Anwender verdächtig vorkommt, sollte sie ungeöffnet gelöscht werden (z. B. aufgrund der Maßnahme „Prüfung des Dateiformats von Anhängen“). Keinesfalls darf aus Neugierde auf beworbene Links geklickt werden. Eine technische Spam-Filterung ist sehr empfehlenswert, spart Arbeitszeit und schützt vor unvorsichtigen Mitarbeitern.

→ Weitere Informationen:

- BSI-Studie „Antispam-Strategien“, http://www.bsi.bund.de/literat/studien/antispam/index.htm

Automatische Ausführung von E-Mail-Anhängen und Inhalten verhindern

Der E-Mail-Client sollte so eingestellt sein, dass Anhänge nicht versehentlich gestartet werden können, sondern der Anwender zuvor gewarnt und gefragt wird. Das Betriebssystem bzw. der E-Mail-Client sollte außerdem so eingerichtet sein, dass Dateien zunächst nur in Viewern oder anderen Darstellungsprogrammen angezeigt werden, die eventuell in den Dateien enthaltenen Programmcode - wie Makros oder Skripte - nicht ausführen. Diese Viewer müssen daher zur Standard-Konfiguration jedes Arbeitsplatz-Rechners gehören.

Bei E-Mails mit Aktiven Inhalten oder im HTML-Format besteht bereits durch die Anzeige im Vorschaufenster die Gefahr, dass schädliche Inhalte ohne Aktion des IT-Anwenders ausgeführt werden. Im Posteingangsordner müssen daher alle Vorschaufunktionen abgeschaltet werden.

Prüfung des Dateiformats von Anhängen

Bei Windows-Betriebssystemen steuert die Dateiendung, mit welchem Programm die Datei geöffnet wird. Programmierer von Schadprogrammen nutzen das aus, indem sie die wahren Typen verschleiern und IT-Anwender täuschen (Beispiel „Rechnung.pdf.....exe“). Eine Identifizierung und Verifikation des „wahren“ Dateityps durch Schutzprogramme (z. B. am E-Mail-Gateway oder an der Firewall) sorgt für mehr Sicherheit. Werden Dateien gefunden, die falsch oder missverständlich bezeichnet sind, können diese speziell gekennzeichnet und mit Warnhinweisen versehen werden. Ideal wäre die automatische Einstellung in einen Quarantänebereich. Die Analyse der verdächtigen Dateien kann dann in einer speziell gesicherten Umgebung erfolgen.

Anzeige von internen und externen Absendern

Gängige E-Mail-Programme zeigen bei eingehenden E-Mails den Absendernamen oft nur unvollständig ohne den Domainnamen an oder verwenden Angaben der eingehenden E-Mail, die sich leicht fälschen lassen. Angreifer erkundigen sich daher gerne nach Namen von Mitarbeitern, deren Identität sie annehmen können. Erhält das Opfer eine E-Mail, die scheinbar von einem Kollegen verfasst wurde,

wird es wahrscheinlich ohne Misstrauen einen Anhang öffnen oder vertrauliche Daten durch Betätigen der „Antwort-Schaltfläche“ verschicken. Es muss daher sichergestellt werden, dass der Empfänger einer E-Mail einen externen Absender sehr deutlich von einem internen unterscheiden kann.

Schutz vor gefälschten externen Absenderangaben

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
mittel	niedrig	falsche Warnung möglich

Häufig täuschen Angreifer einen falschen Absender vor (Spoofing). Erkennen lässt sich ein falscher Absender unter anderem daran, dass die IP-Adresse nicht zur Domain passt. Wird die E-Mail eines deutschen Absenders (name@firma.de) beispielsweise von einem Server im Ausland verschickt, könnte die Absenderangabe gefälscht sein. Eine Warnung des Empfängers bei Spoofing-Verdacht sollte daher erwogen werden.

Wenn der Aufwand zur Prüfung aller eingehenden E-Mails zu hoch oder mit zu großen Performanceverlusten verbunden ist, sollten zumindest die Protokolldaten regelmäßig ausgewertet werden. Der Sicherheitsgewinn ist deutlich geringer. Ein Angriff lässt sich aber wenigstens nachträglich feststellen.

Formatumwandlung von HTML-Mails

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
hoch	niedrig	mittel

E-Mails im Text-Format bergen nach heutigem Wissensstand sehr viel weniger Gefahren als E-Mails im HTML-Format. Die meisten E-Mails sind auch noch im Text-Format lesbar, so dass eine automatische Umwandlung von HTML-Mails in Text zumutbar ist.

Blockieren von Anhängen

Art der Anhänge	Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
nur die gefährlichsten	mittel - hoch	niedrig	mittel - hoch
alle	hoch	niedrig	sehr hoch

Bestimmte Dateitypen wurden in der Vergangenheit besonders häufig durch Angreifer missbraucht und könnten bei hohen Sicherheitsanforderungen zentral an der Firewall ausgefiltert werden. Welche Dateitypen für die automatische Filterung ausgewählt werden, muss individuell entschieden werden. Informationen zur Gefährlichkeit von Dateitypen finden sich in den referenzierten Maßnahmen.

Text-E-Mails ohne Anhänge gelten zurzeit noch als sicher. Daher erhöht eine Formatumwandlung in Kombination mit dem Herausfiltern aller Anhänge die Sicherheit deutlich.

→ **Weitere Informationen:**

- GS-K, M 4.199 Vermeidung gefährlicher Dateiformate
- GS-K, M 5.109 Einsatz eines E-Mail-Scanners auf dem Mailserver
- GS-K, M 4.222 Festlegung geeigneter Einstellungen von Sicherheitsproxies

Whitelists für E-Mail-Absender und Webadressen

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
mittel - hoch	mittel	mittel - hoch

In einem Verzeichnis können E-Mail-Adressen von vertrauenswürdigen Geschäftspartnern gepflegt werden, für die bestimmte, besonders weitgehende Sicherheitsmaßnahmen mit großen Komforteinbußen nicht gelten. Beispielsweise könnten Dateianhänge von allen Adressen, die nicht in der Whiteliste eingetragen sind, standardmäßig geblockt werden. Diesem Mechanismus darf allerdings nicht blind vertraut werden, da ein Angreifer Absenderadressen fälschen oder fremde Rechner kapern könnte.

Auch beim Surfen können je nach Adresse unterschiedliche Sicherheitsmaßnahmen gelten. Vertrauenswürdige externe Seiten können beispielsweise für die Rechner am Arbeitsplatz freigeschaltet werden. Für alle anderen steht ein spezieller Internet-PC ohne Anschluss ans Intranet zur Verfügung. Der Sicherheitsgewinn darf allerdings nicht überschätzt werden und hängt entscheidend von der Qualität der Whitelist ab. Eine Positivliste ist wirkungslos, wenn prinzipiell jede Seite aufgenommen wird und dort auf unbestimmte Zeit bleibt. In eine Whitelist sollten daher nur wenige, gut bekannte und vertrauenswürdige Webangebote eingetragen werden, z. B. seriöse Medien, große Unternehmen oder Behörden.

Maßnahmen bei ausgehenden E-Mails

Benachrichtigung des Administrators nach Detektion eines Schadprogramms

Wird vom zentralen Viren-Schutzprogramm in einer ausgehenden E-Mail ein Schadprogramm gefunden, muss in jedem Fall automatisch ein Administrator benachrichtigt werden.

Versand von Text-Mails

Es sollten grundsätzlich keine HTML-formatierten E-Mails verschickt werden.

Regeln für E-Mail-Eigenschaften

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
niedrig	niedrig	mittel - hoch

- Bei hohem Schutzbedarf bezüglich Vertraulichkeit kann die Größe ausgehender Mails beschränkt werden, um das Herausschmuggeln großer Datenmengen zu erschweren. Gleichzeitig muss ein IDS überwachen, ob ungewöhnlich viele E-Mails von einem Account verschickt werden.

- Zusätzlich kann das Versenden von Dateianhängen deaktiviert werden.

Suche nach vertraulichen Inhalten und Schlüsselwörtern

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
mittel	mittel - hoch	niedrig (Fehlalarme)

In ausgehenden E-Mails an externe Adressen kann nach vertraulichen Inhalten (z. B. VS - NUR FÜR DEN DIENSTGEBRAUCH) gesucht werden. Ein Angreifer, der davon Kenntnis erlangt, wird beim nächsten Versuch allerdings die Informationen verschlüsseln, so dass die Schutzwirkung der Maßnahme nicht überbewertet werden darf. Die Maßnahme hilft auch gegen das versehentliche Versenden eingestufter Dokumente (z. B. Verwechslung oder Markieren der falschen Datei).

Anomalieerkennung

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
mittel - hoch	hoch	keine

Schadprogramme bringen häufig eigene E-Mail-Programme mit oder missbrauchen die Standard-E-Mail-Anwendung. Dabei unterscheidet sich das E-Mail-Verhalten von Schadsoftware unter Umständen deutlich von dem eines menschlichen IT-Anwenders. Eine Detektion derartiger Anomalien ist mit Zusatzprogrammen oder Intrusion-Detection-Systemen durchaus möglich. Folgende Anomalien könnten beispielsweise auf unautorisierte E-Mail-Aktivität hinweisen:

- E-Mails werden nicht über das Standard-E-Mail-Programm verschickt.

- Die Zeitspanne zwischen Start des E-Mail-Programms und dem Versand einer E-Mail ist auffällig kurz.

- Weder Tastatur noch Maus werden beim Absenden einer E-Mail benutzt.

- Der Versand erfolgt zu ungewöhnlichen Zeiten (nachts, am Wochenende, Rosenmontag in Köln).

- Ein IT-System versendet E-Mails in ganz regelmäßigen Intervallen.

- Eine große Anzahl E-Mails wird innerhalb kurzer Zeit an dieselbe Adresse verschickt.

7.4 Drahtlose Kommunikation und Voice over IP

Absicherung drahtloser Kommunikation

IT-Systeme wie Notebooks, Mobiltelefone oder PDAs verfügen über verschiedene drahtlose Kommunikationsmöglichkeiten und bieten damit einen hohen Komfort und vielfältige Einsatzmöglichkeiten.

Fehlkonfigurationen der Geräte oder Schwachstellen in den verwendeten Protokollen bzw. in ihrer Implementierung eröffnen jedoch auch Angriffsmöglichkeiten.

WLAN ist ein typisches Beispiel für den klassischen Interessenskonflikt zwischen Bequemlichkeit und IT-Sicherheit. Obwohl die Sicherheitsprobleme von WLANs regelmäßig publiziert werden, finden sich in der Praxis immer noch viel zu viele ungesicherte Netze. Auch bei der Gestaltung von Tele- und Heimarbeit ist dieser Umstand zu beachten. Wohnzimmerkompatibilität darf bei professioneller IT-Nutzung nicht über Sicherheitsaspekte gestellt werden.

Aus Sicherheitssichtssicht sollte möglichst auf drahtlose Kommunikationsverbindungen verzichtet werden. Lässt sich ein Einsatz nicht vermeiden, sollten die Sicherheitsempfehlungen des BSI oder anderer kompetenter Stellen beachtet werden.

→ Weitere Informationen:

- „Technische Richtlinie Sicheres WLAN“ des BSI,
  http://www.secumedia.de, SecuMedia Verlag (kostenpflichtig)
  http://www.bsi.ivbb.bund.de/literat/tr/ (nur für Bundesbehörden, kostenlos)
- Startpunkt BSI-Webseite „Basistechnik: Drahtlose Netze (WLAN usw.) und mobile Nutzer“, http://www.bsi.bund.de/fachthem/sinet/basis/basis_WLAN.htm

Voice over Internet Protocol

Voice over IP (VoIP) wird langfristig in vielen Bereichen die bisherige Technik ablösen. Im Vergleich zur leitungsvermittelnden Telefonie bergen VoIP-Systeme zurzeit deutlich größere Risiken - sie erben die Sicherheitsrisiken der IP-Welt und behalten darüber hinaus die meisten aus der TK-Welt.

Geeignete Sicherheitsmaßnahmen sind heute technisch und organisatorisch realisierbar. Allerdings unterstützt nur ein Bruchteil der aktuell auf dem Markt befindlichen Systeme die erforderlichen Sicherheitsmaßnahmen in vollem Umfang. Eine BSI-Studie hat gezeigt, dass zurzeit die für einen verlässlichen Betrieb von VoIP-Systemen notwendigen Sicherheitsmaßnahmen noch mit einem so hohen technischen und finanziellen Aufwand verbunden sind, dass sich die angestrebten Kosteneinsparungen wahrscheinlich nicht realisieren lassen.

Die Kosten für die erforderlichen Sicherheitsmaßnahmen müssen daher bereits frühzeitig in die Planungen mit einbezogen werden. Am Ende sollte die Entscheidung für oder gegen den Einsatz von VoIP-Systemen immer zugunsten der IT-Sicherheit ausfallen.

→ Weitere Informationen:

BSI-Studie zur Sicherheit von Voice over Internet Protocol,
http://www.bsi.bund.de/literat/studien/VoIP/index.htm

8 Detektion und Abwehr von Schadprogrammen

Schutzsoftware zur Detektion von Schadprogrammen wird im weiteren Verlauf auch mit dem historischen Begriff „Viren-Schutzprogramm“ bezeichnet, obwohl alle erhältlichen Produkte verschiedene Arten von Schadprogrammen erkennen können.

Der Schutz vor Schadprogrammen gehört zu den Standardaufgaben jedes Administrators. An dieser Stelle werden daher vor allem die Themen dargestellt, die über IT-Grundschutz hinausgehen oder nicht zur üblichen Praxis zählen. Gängige Viren-Schutzprogramme erfüllen nicht mehr alle Anforderungen und müssen daher durch zusätzliche Tools ergänzt werden.

Funktionsweise und Grenzen von klassischen Viren-Schutzprogrammen

Viren-Schutzprogramme arbeiten nach zwei Verfahren. Bei einer Signaturprüfung werden in den zu prüfenden Dateien typische Codesequenzen von bekannten Schadprogrammen gesucht. Bei einer heuristischen Prüfung wird versucht, mit speziellen Algorithmen potentiell schädlichen Code zu entdecken. Die folgenden Überlegungen beleuchten die Grenzen von Viren-Schutzprogrammen:

- Zeitverzug

  Die Hersteller von Antiviren-Software benötigen eine gewisse Zeit, um Schadprogramme zu identifizieren und Signaturen bereitzustellen. IT-Anwender sind daher in der Zeitspanne zwischen dem ersten Auftreten eines Schadprogramms und der Erkennung durch Schutzsoftware - das können einige Stunden oder auch Tage sein - ohne Schutz gegen dieses spezielle Schadprogramm.

- Begrenzung heuristischer Verfahren

  Heuristische Verfahren arbeiten zurzeit noch sehr ungenau. Erschwerend kommt hinzu, dass mit der Erkennungsrate gleichzeitig auch die Anzahl der Fehlalarme steigt. In der Praxis werden daher im produktiven Einsatz die Programme so konfiguriert, dass sie den IT-Anwender nicht mit einer Vielzahl von falschen Alarmmeldungen belästigen. Es werden daher kaum Schadprogramme erkannt.

- Schadprogramme mit geringer Verbreitung

  Je geringer der Verbreitungsgrad eines Schadprogramms, desto unwahrscheinlicher ist die Bereitstellung einer Signatur durch die Hersteller von Schutzsoftware. Wurde eine Schadsoftware speziell entwickelt, um nur ein ausgewähltes Ziel anzugreifen, ist daher die Entdeckung mit Standard-Schutzsoftware sehr unwahrscheinlich.

- Rechtliche Beschränkungen

  Häufig werden für Angriffe Programme genutzt, die von seriösen Herstellern zu anderen Zwecken hergestellt wurden. Da beispielsweise der Vertrieb von Keyloggern in vielen Ländern legal ist, nehmen Hersteller von Schutzprogrammen sie in der Regel nicht in ihre Signaturdatenbank auf. Eine Entdeckung aller kommerzieller Keylogger mit Standardprogrammen ist daher sehr unwahrscheinlich.

- Unvollständige Analyse von Schadsoftware

  Die Hersteller von Schutzsoftware können unmöglich das Verhalten jeder Schadsoftware genau und umfassend analysieren, da sie pro Tag mehrere hundert verdächtige Dateien erreichen. Die vollständige Analyse eines einzigen Schadprogramms dauert unter Umständen mehrere Tage. Erschwerend kommt hinzu, dass das Verhalten von Programmen von vielen Randbedingungen wie Betriebssystem, Patchlevel oder installierter Software abhängt. Es kann daher auch immer wieder

vorkommen, dass ein Schadprogramm zwar erkannt, aber nicht wirksam an der Ausführung gehindert wird.

8.1 Basisschutz

Konzeption des Virenschutzes

1. Am zentralen E-Mail-Gateway muss ein Viren-Schutzprogramm eingesetzt werden, das ein- und ausgehende E-Mails prüft.

2. Alle weiteren Internet-Dienste (HTTP, FTP, ...) sollten ebenfalls mit Schutzsoftware geschützt werden. Wenn dies aufgrund von Performance-Problemen nicht möglich ist, muss zumindest die Ausführung aller Aktiver Inhalte technisch unterbunden werden (siehe Maßnahme „Umgang mit Aktiven Inhalten“).

3. Auf allen Client-Rechnern muss ein residentes Viren-Schutzprogramm installiert werden.

4. Für den zentralen Schutz am Übergang zum Internet sollte nach Möglichkeit ein anderes Produkt gewählt werden als für den Client-Schutz.

Systemübergreifende Minimalanforderungen

1. Es dürfen nur Produkte eingesetzt werden, die über einen längeren Zeitraum in unabhängigen Tests ihre Qualität unter Beweis gestellt haben. Qualität muss stärker gewichtet werden als Performance.

2. Es müssen alle Dateitypen geprüft werden. Eine Beschränkung auf „ausführbare“ Dateiformate ist nicht mehr zeitgemäß.

3. Viren-Signaturen sind mindestens einmal täglich einzuspielen, bei konkreter Gefahr auch öfter. Ein sofortiges Updates aller Clients muss möglich sein - zur Not durch einen zentral initiierten Neustart der Rechner.

4. Die Logdateien der lokalen und zentralen Schutzprogramme müssen regelmäßig ausgewertet werden.

8.2 Erweiterte Sicherheitsmaßnahmen

Die folgenden Maßnahmen bieten einen erhöhten Schutz, schränken dabei aber z. T. die Verfügbarkeit der Rechner ein oder sind mit Komforteinbußen verbunden. Bei hohen Sicherheitsanforderungen sollten sie dennoch erwogen werden.

Detektion von Fehlfunktionen der Viren-Schutzprogramme

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
mittel - hoch	mittel	keine

Schadprogramme können Schutzsoftware deaktivieren, manipulieren oder Updates verhindern. Der Ausfall eines Viren-Schutzprogramms muss daher schnell entdeckt werden. Fehlfunktionen werden aber nicht nur durch Schadprogramme verursacht. So kann beispielsweise durch eine Störung der Softwareverteilung auf einem Arbeitsplatz-Rechner ein regelmäßiges Update der Viren-Signaturen verhindert werden. Nach Möglichkeit sollten bei Fehlfunktionen automatisch Warnmeldungen generiert werden. Administratoren sollten aber zusätzlich regelmäßig die Funktion der Schutzsoftware auf zentralen Systemen sowie auf Arbeitsplatz-Rechnern testen.

Einsatz von spezialisierten Scannern zur Ergänzung von Standardprodukten

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
hoch	mittel	keine

1. Es sollten Programme eingesetzt werden, die Keylogger oder Spyware aufspüren können. Spezialisierte Programme sind Standard-Viren-Schutzprogrammen darin meistens überlegen.

2. Wünschenswert ist auch der Einsatz von Scannern, die auch individuell erzeugte Signaturen verarbeiten können. Wird beispielsweise durch auffälliges Systemverhalten ein Schadprogramm entdeckt, das von Standard-Viren-Schutzprogrammen nicht erkannt wird, kann der zuständige Administrator oder ein externer Experte eine individuelle Signatur erstellen und weitere betroffene IT-Systeme identifizieren.

Regelmäßige Untersuchung aller Dateien auf Clients und Dateiservern

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
mittel	mittel	mittel (Performance)

Auch wenn bei jedem Dateizugriff eine On-Access-Prüfung durchgeführt wird, hat eine regelmäßige Untersuchung aller Dateien auf Clients und Dateiservern durchaus ihren Sinn. Auf diese Weise können Schadprogramme gefunden werden, für die es noch keine Erkennungssignatur gab, als sie gespeichert wurden. In derartigen Fällen muss beispielsweise untersucht werden, ob das gefundene Schadprogramm vor seiner Entdeckung vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen hat.

Aus Performancegründen sollte eine Prüfung in Zeiten durchgeführt werden, in denen die IT-Ressourcen nicht stark beansprucht werden. Ideal ist ein Programm, das abhängig von der Auslastung des Rechners seine CPU-Nutzung selbständig regelt und „Arbeitspausen“ des PCs für die Überprüfung ausnutzt. Auf den Arbeitsplatz-Rechnern könnte das Viren-Schutzprogramm z. B. mit dem Start des Bildschirmschoners gekoppelt werden.

8.3 Maßnahmen mit hoher Schutzwirkung

Es gibt eine Reihe von forensischen Methoden und Tools, die auch die Detektion von neuen Schadprogrammen erlauben, die Standard-Viren-Schutzprogrammen unbekannt sind. Leider erfordern die Durchführung der Analysen und die Interpretation der Ergebnisse eine spezielle Ausbildung und viel Erfahrung. Zumindest die IT-Systeme mit hohem Schutzbedarf, für die eine konkrete Bedrohung befürchtet wird, sollten regelmäßig von den Administratoren einer genaueren Untersuchung unterzogen werden.

Vorsicht beim Einsatz von spezieller Sicherheitssoftware

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
mittel - hoch	mittel	keine

Beim Einsatz von spezieller Sicherheitssoftware (z. B. Tools zur Rootkit-Erkennung) muss mit großer Vorsicht vorgegangen werden. Es ist nicht ausgeschlossen, dass gerade diese Programme Hintertüren und Schadfunktionen enthalten. Eine Analyse sollte daher nur mit Programmen aus sicherer Herkunft oder mit einem Image auf einem Stand-alone-Laborrechner ohne Netzzugang erfolgen. Bei Erstellen eines Images muss darauf geachtet werden, dass auch ungenutzte oder defekte Bereiche eines Datenträgers mit eingeschlossen werden. Nicht alle Tools zur Image-Erstellung bieten diese Funktionalität.

Manuelle Prozessanalyse

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
hoch	hoch	mittel (Zeit)

Während des normalen Betriebs sollten die Prozesse analysiert werden und mit der Whitelist verglichen werden, die bei der Installation erstellt wurde. Desktop-Firewalls bieten eine ähnliche Funktionalität, sind aber nicht vollständig zuverlässig.

Spezialisierte Detektions- und Analyseprogramme

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
hoch	hoch	mittel (Fehlalarme)

Spezialisierte Detektions- und Analyseprogramme eignen sich in der Regel nur zur manuellen Untersuchung einzelner Rechner.

- **Heuristische Scanner**

  Für genauere Analysen von Dateien können Scanner mit heuristischen Funktionen eingesetzt werden. Da ein Administrator die Durchführung überwacht, können auch experimentelle Funktionen verwendet werden.

- **Rootkit-Detektion**

  Viele Rootkits lassen sich mit speziellen Programmen aufspüren. Dazu werden beispielsweise die Adressen der Systemdienste des Windows-Kernels analysiert. Einige der Programme eignen sich sogar für einen automatisierten Einsatz.

- **Erweiterte Task Manager**

  Eng verwandt mit Anti-Rootkit-Tools sind erweiterte Task Manager für Windows. Sie zeigen umfangreiche Informationen zu Programmen, Prozessen und Diensten an und sind damit den Standardtools des Betriebssystems weit überlegen. Mit ihnen lassen sich auch versteckte Prozesse aufspüren.

→ **Weitere Informationen:**

- "Windows rootkits of 2005", Artikelserie von James Butler und Sherri Sparks auf SecurityFocus - Definition, Einführung in die Technik, Tools, weiterführende Literatur: http://www.securityfocus.com/infocus/1850
- Projekt „Strider GhostBuster Rootkit Detection" von Microsoft: http://research.microsoft.com/rootkit/
- http://www.rootkit.com/

Analyse der Festplatte

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
hoch	hoch	mittel (Zeit)

Eine Festplatte bietet je nach Dateisystem Schadprogrammen verschiedene Möglichkeiten, sich vor Schutzsoftware und Systemtools zu verbergen oder gesammelte Daten versteckt zu speichern. Folgende Bereiche können bei forensischen Untersuchungen mit Spezialtools analysiert werden:

- Alternate Data Streams (NTFS)
- ungenutzte Sektoren
- fehlerhafte Sektoren
- Dateien ohne Zuordnung

→ **Weitere Informationen:**

"Windows NTFS Alternate Data Streams", Don Parker auf SecurityFocus: http://www.securityfocus.com/infocus/1822

Integritätsprüfung

Sicherheitsgewinn	Aufwand Realisierung	Funktionseinbußen
hoch	hoch	niedrig (Performance)

Wichtige Dateien (Systemprogramme, Treiber, Konfigurationsdateien wie die Windows-Registry) sollten regelmäßig auf Veränderungen geprüft werden. In größeren Behörden oder Unternehmen lohnt sich der Betrieb einer zentralen Datenbank mit Hashwerten aller wichtigen Dateien. Ist dies nicht möglich, sollten externe Anbieter für diese Dienstleistung gesucht werden.

→ **Weitere Informationen:**

GS-K, M 4.93 Regelmäßige Integritätsprüfung

9 Vorbereitung auf Sicherheitsvorfälle und Maßnahmen im Schadensfall

Voraussetzung für eine geordnete Reaktion bei vermuteten Sicherheitsvorfällen ist die Umsetzung der Maßnahme „Risikobetrachtung für bedrohte Informationen und IT-Komponenten“ aus dem Kapitel 2 „IT-Sicherheitsmanagement und Organisation“. Zum einen müssen Informationen klassifiziert worden sein, zum anderen müssen die Abhängigkeiten zwischen Daten, IT-Anwendungen und IT-Systemen nachvollzogen werden können.

Neben organisatorischen Maßnahmen sind auch technische Vorbereitungen auf einen Sicherheitsvorfall notwendig. Erfolgreiche Forensik setzt umfangreiche Vorarbeiten voraus. Nur so lassen sich im Ernstfall Spuren sicherstellen, das Verhalten des Täters nachvollziehen und die möglichen Auswirkungen des Vorfalls einschätzen. Zu den technischen Vorbereitungen gehören Protokollierung und Log-Auswertung, Datensicherung und der Einsatz von speziellen Tools zu Forensik und Netzwerkanalyse:

- **Protokollierung**

  Im Netz, auf IT-Systemen und bei IT-Anwendungen müssen möglichst umfangreiche Daten protokolliert und die Logdaten sinnvoll aufbereitet werden. Dazu gehören die richtige Platzierung von Netzwerksensoren und der Betrieb eines Intrusion-Detection-Systems.

- **Datensicherung**

  Forensische Untersuchungen haben spezielle Anforderungen an Datensicherungen. Schadprogramme können sich auch in ungenutzten oder fehlerhaften Sektoren einer Festplatte verbergen. Alternate Data Streams beispielsweise sind NTFS-spezifisch und gehen bei der Konvertierung in ein anderes Dateisystem verloren.

- **Tools**

  Spezielle Tools zur Forensik, Datenrettung oder zur Integritätsprüfung müssen auf einem „sauberen“ System installiert werden. Eine nachträgliche Installation von Software auf einem kompromittierten System kann zum Verlust vom digitalen Spuren führen.

→ Weitere Informationen:

- NIST SP 800-61 “Computer Security Incident Handling Guide”
- NIST SP 800-86 “Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response”
- GS-K, B 1.8 Behandlung von Sicherheitsvorfällen
- GS-K, B 1.3 Notfallvorsorgekonzept
- Musterrichtlinien und Beispielkonzepte zum IT-Grundschutz: Notfallvorsorgekonzept, http://www.bsi.bund.de/gshb/deutsch/musterrichtlinien/index.htm

9.1 Organisatorische Maßnahmen

Übernahme von Verantwortung durch das Management

Innerhalb der Organisationsstruktur muss die Zuständigkeit für IT-Sicherheit klar geregelt und im Management verankert sein. Im Tagesbetrieb muss bei akuten Sicherheitsbedrohungen und Vorfällen schnell und konsequent gehandelt werden.

Entwicklung von Konzepten für verschiedene Vorfälle

Vor dem ersten Sicherheitsvorfall sollten Konzepte mit Handlungsanweisungen für verschiedene Vorfallsarten erarbeitet werden. Bei vielen Angriffen werden mehrere Schäden gleichzeitig eintreten. Mögliche Kategorien von Vorfällen sind:

- Detektion eines Schadprogramms
- Verlust der Verfügbarkeit, Denial-of-Service, Ausfall von IT-Anwendungen
- Unautorisierter Zugriff auf vertrauliche Daten
- Unbefugte Veränderung von Daten
- Unbefugte IT-Nutzung

Im Rahmen der Konzeption müssen Verantwortlichkeiten geklärt und zugewiesen sowie eine Eskalationsstrategie überlegt werden. Die Aufgaben folgender Personen bzw. Funktionen sollten beschrieben werden:

- IT-Benutzer
- IT-Administratoren
- Anwendungsverantwortliche
- IT-Sicherheitsbeauftragter bzw. IT-Sicherheitsmanagement
- Öffentlichkeitsarbeit bzw. Pressestelle
- IT-Sicherheitsrevision
- Rechtsabteilung
- Behörden-/Unternehmensleitung

Folgende Fragen sollten dabei z. B. gestellt werden:

- Wer muss wann benachrichtigt werden?

  Die relevanten Stellen müssen rechtzeitig benachrichtigt werden. Andererseits sollten aber auch keine unnötigen Meldungen generiert werden.

- Wer darf wichtige Entscheidungen treffen?
  - Wird ein Server vom Netz genommen?
  - Wann gilt ein Vorfall als „abgeschlossen“?
  - Werden Ermittlungsbehörden eingeschaltet?

- Wer darf Aussagen gegenüber Presse oder Behörden machen?

Festlegung von Prioritäten

Bei einem IT-Sicherheitsvorfall gibt es verschiedene Handlungsoptionen, die aber z. T. konkurrierende Anforderungen haben oder sich sogar gegenseitig ausschließen. Es ist daher sehr wichtig, im Vorfeld mögliche Sicherheitsvorfälle durchzuspielen und jeweils zu überlegen, welche Ziele in welcher Reihenfolge verfolgt werden sollen:

- Es besteht akute Gefahr, ein noch größerer Schaden soll verhindert werden:
  - Steht die Aufrechterhaltung von Geschäftsprozessen im Vordergrund, muss die Verfügbarkeit von IT-Systemen und IT-Anwendungen wiederhergestellt bzw. gesichert werden.
  - Wenn Vertraulichkeit und Integrität schutzbedürftiger Daten oberste Priorität haben, muss unter Umständen die Internetanbindung unterbrochen werden. So kann verhindert werden, dass ein Angreifer weiterhin Zugriff auf schutzbedürftige IT-Systeme hat.
- Ein Täter soll strafrechtlich verfolgt werden:
  - Es kann durchaus sinnvoll sein, die betroffenen IT-Systeme nicht vom Netz zu trennen und den Täter eine gewisse Zeit zu beobachten. In diesem Fall müssen dann vertrauliche Informationen, auf die der Angreifer auf keinen Fall zugreifen darf, speziell gesichert oder sogar vom Netz getrennt werden.
  - Da deutsche Gerichte hohe Anforderungen an die Objektivität und Qualität von Ermittlungen legen, ist die Einschaltung der zuständigen Behörden notwendig. Die Polizei wird alle Anstrengungen unternehmen, den Geschäftsbetrieb durch ihre Ermittlungen nicht unnötig zu stören. In Einzelfällen müssen jedoch zur Aufklärung schwerer Straftaten IT-Systeme beschlagnahmt werden. Bei ungenügender Vorbereitung kann dann sehr schnell ein gravierendes Verfügbarkeitsproblem entstehen.
- Der entstandene Schaden soll ermittelt werden:
  - Es muss festgestellt werden, ob Daten böswillig manipuliert wurden.
  - Es muss festgestellt werden, ob vertrauliche Daten eingesehen wurden.
- Weitere Vorfälle sollen zukünftig vermieden werden:
  - Alle kompromittierten IT-Systeme und IT-Anwendungen müssen identifiziert und gesäubert werden.
  - Es muss untersucht werden, wie der Täter in die betroffenen IT-Systeme eindringen konnte.

Vorbereitung auf forensische Maßnahmen zur Beweissicherung

Die Konzeption forensischer Untersuchungen und die Auswertung von Protokolldaten erfordern ein hohes Maß an Fachwissen und Erfahrung. Wenn beispielsweise das Konzept mangelhaft ist und keine geeigneten Logdaten geschrieben werden, lassen sich nach einem Vorfall auch keine Beweise sichern. IT-Sicherheitsbeauftragte und Administratoren müssen für diese spezialisierten Aufgaben zusätzlich ausgebildet werden. Je nach eigener Erfahrung und Kompetenz kann es auch erforderlich sein, Kontakt zu externen Sicherheitsdienstleistern aufzunehmen und sich bei der Vorbereitung auf bestimmte Vorfälle und der Erstellung eines Notfallvorsorgekonzeptes beraten zu lassen.

Zeit ist ein wesentlicher Erfolgsfaktor bei forensischen Untersuchungen. Es muss z. B sehr schnell entschieden werden, was mit einem verdächtigen Rechner geschehen soll: Ausschalten, um Schlimmeres zu verhüten, oder eingeschaltet lassen, um keine Spuren - z. B im Arbeitsspeicher oder in temporären Dateien - zu zerstören? Wenn diese Überlegungen erstmalig bei Auftreten eines Vorfalls angestellt werden, vergeht wertvolle Zeit, oder Spuren werden unwiderruflich gelöscht.

Behörden und Unternehmen, die mehrere Niederlassungen haben oder sich in kleineren Städten ohne spezialisierte Polizeiabteilungen für Computerkriminalität und Forensik befinden, sollten frühzeitig die zuständige Ermittlungsbehörde und geeignete Ansprechpartner in Erfahrung bringen.

Notfallvorsorge/ Business Continuity

Sicherheitsvorfälle können in extremen Fällen dazu führen, dass IT-Systeme und Anwendungen für eine längere Zeit ausfallen und nicht genutzt werden können. Für wichtige Geschäftsprozesse und IT-Tätigkeiten muss daher ein Notfallvorsorgekonzept entwickelt werden.

9.2 Protokollierung und Auswertung der Logdateien

Protokollauswertung

Die Analyse von Protokolldaten ist aufwendig und kompliziert - trotzdem sollten diese nicht nur bei Fehlfunktionen und Störungen angesehen werden. Durch Protokollierung und regelmäßige, Anlass unabhängige Auswertung von Logdaten lassen sich auch bislang unentdeckte Schadprogramme aufspüren. Folgende Protokolle sollten in die Analysen einbezogen werden:

- Desktop-Firewalls
- Intrusion Detection System
- Sicherheitsgateway
- Netzkoppelelemente
- E-Mail-Gateway
- Server und Clients

Einsatz eines Protokollierungsservers in einem Sicherheitsgateway

Bei komplizierteren Sicherheitsgateways aus mehreren Komponenten fallen oft große Mengen verschiedener Protokollierungsinformationen an. Um die Auswertung der Protokolle zu erleichtern, empfiehlt sich daher ein zentraler Protokollierungsserver (Loghost).

→ **Weitere Informationen:**

GS-K, M 4.47 Protokollierung der Sicherheitsgateway-Aktivitäten

Protokollierung bei Routern und Switches

Folgende Informationen sollten nach Möglichkeit protokolliert werden:

- Konfigurationsänderungen
- Reboots
- Systemfehler
- Statusänderungen pro Interface, System und Netzsegment
- Login-Fehler
- Anmeldeversuche von Geräten mit nicht registrierten MAC-Adressen
- Verstöße gegen ACL-Regeln (abgewiesene Kommunikationssversuche)

Insbesondere der letzte Punkt sollte für jede ACL aktiviert werden, um alle fehlgeschlagenen Versuche zu erfassen und falsch oder nicht korrekt konfigurierte Regeln erkennen zu können.

→ Weitere Informationen:

GS-K, M 4.205 Protokollierung bei Routern und Switches

Protokollierung der E-Mail-Nutzung

Da viele Schadprogramme über E-Mails verschickt werden, können durch die Protokollierung der E-Mail-Nutzung Sicherheitsvorfälle häufig nachvollzogen werden. Wenn gestohlene Daten über E-Mails an den Angreifer gesendet werden, kann eine gute Protokollierung bei der Identifizierung der Täter helfen.

Protokollierung auf Servern und Clients

Die Protokollierung auf Servern und Clients kann dabei helfen, die Aktivität eines Schadprogramms zu erkennen. Um die Logdaten vor Veränderungen zu schützen, sollten sie auf einen zentralen Log-Server geschrieben werden. Folgende Vorkommnisse sind z. B. von Interesse:

- häufig falsche Passworteingabe für eine Benutzer-Kennung
- Versuche von unberechtigten Zugriffen, z. B. auf Verzeichnisse, für die der IT-Anwender keine Zugriffsberechtigung hat
- Installation von Software
- Veränderung von Systemdateien
- Deaktivierung von Sicherheitsmechanismen
- Zugriff auf vertrauliche oder eingestufte Dateien

Die Sicherheitsverantwortlichen sollten ihren „Heimvorteil“ nutzen. Dazu können beispielsweise Testdateien und -verzeichnisse angelegt werden, die scheinbar vertrauliche Daten enthalten. Da kein Mitarbeiter diese Daten dienstlich nutzt, kann jeder Zugriff einen Alarm auslösen.

→ **Weitere Informationen:**

- GS-K, M 4.148 Überwachung eines Windows 2000/XP Systems
- GS-K, M 4.167 Überwachung und Protokollierung von Exchange 2000 Systemen

10 Literatur und Informationsquellen

BSI-Publikationen

Gerade bei komplexen Themen ist es hilfreich, systematisch vorzugehen und sich die Erfahrungen anderer zu Nutze zu machen. IT-Sicherheitsmanagement und die wichtigsten Standardsicherheitsmaßnahmen aus den Bereichen Organisation, Technik, Personal und Infrastruktur werden ausführlich in folgenden Publikationen des BSI behandelt:

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
- BSI-Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz
- IT-Grundschutz-Kataloge (vormals IT-Grundschutzhandbuch, GS-K)

In diesem Leitfaden werden Kapitel („Bausteine“) der IT-Grundschutzkataloge mit „B“ und einzelne IT-Grundschutz-Maßnahmen mit „M“ bezeichnet.

Beispiel: *GS-K, M 4.148* steht für die Maßnahme M 4.148 aus den IT-Grundschutz-Katalogen.

IT-Grundschutz im Internet

Alle Veröffentlichungen zum IT-Grundschutz (Standards, Kataloge, Hilfsmittel und Beispiele) sind online und beim Bundesanzeiger Verlag in gedruckter Form verfügbar. Startseite: http://www.bsi.bund.de/gshb/index.htm

ISO-Standards

Homepage: http://www.iso.org

Sicherheitsbehörden

- USA: National Institute of Standards and Technology (NIST),
  http://csrc.nist.gov/publications/nistpubs/index.html
- USA: National Security Agency (NSA),
  Security Configuration Guides: http://www.nsa.gov/snac/
- England: Centre for the Protection of National Infrastructure (CPNI), früher: National Infrastructure Security Co-Ordination Centre (NISCC), Homepage: http://www.cpni.gov.uk/