Vorwort

Immer mehr Rechner sind mit dem Internet verbunden. Für ihren Schutz sorgen entsprechende Sicherheitskomponenten. Sicherheitsgateways – oft auch Firewalls genannt – stellen die am weitesten verbreitete Lösung in größeren Netzen dar. Doch was an Angeboten auf dem Markt für den privaten Internet-PC noch ausreichen mag, genügt den Anforderungen großer Netze wie in Unternehmen und Behörden nicht. Sowohl die Struktur des zentralen Sicherheitsgateways als auch die Konfiguration der einzelnen Komponenten müssen exakt auf die Sicherheitsbedürfnisse der Organisation zugeschnitten sein.

Mit der Veröffentlichung „Konzeption von Sicherheitsgateways" unterstützt das BSI die IT-Verantwortlichen und Administratoren dabei, ein solches System aus Soft- und Hardwarekomponenten für den entsprechenden Schutzbedarf und andere Rahmenbedingungen richtig anzupassen. Empfehlungen helfen, den Schutzbedarf des internen Netzes zu ermitteln, die erforderliche Basisstruktur auszuwählen und die entsprechenden Bestandteile zu platzieren. Darüber hinaus wird gezeigt, welche Kriterien bei der Auswahl eines Produktes eine Rolle spielen können. Das Ziel: Das Sicherheitsgateway soll nur erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zulassen und die übertragenen Daten kontrollieren.

Doch klar ist: Je komplexer das Sicherheitsgateway, desto höher ist das Risiko einer fehlerhaften Konfiguration. Zudem reicht ein allein auf technische Lösungen ausgerichteter Ansatz zum Schutz der IT nicht aus. IT-Sicherheit gilt es im Alltag zu „leben". Das bedeutet: Nur wenn IT-Sicherheits-Policies eingehalten werden, können Sicherheitsgateways ihr volles Schutzpotenzial entwickeln. Und nur dann ist das eigene Rechner-Netz geschützt.

Bonn, im September 2005

Dr. Udo Helmbrecht, Präsident des BSI

1. Übersicht

Gegenstand dieses Dokuments ist die Beschreibung von Möglichkeiten zur modularen Strukturierung von Sicherheitsgateways in IP-Netzen, wobei abhängig vom Schutzbedarf grundlegende Konzepte mit Vorteilen und Risiken erläutert werden. Eigentliche Zielgruppe sind Administratoren, in einzelnen Fällen kann auch der Privatnutzer Informationen zur Absicherung seiner Internetverbindung finden.
Der Inhalt der „Konzeption von Sicherheitsgateways" als Teil des IT-Sicherheitskonzepts wird im Folgenden anhand des Titels erläutert.

1.1 Definition des Begriffs „Sicherheitsgateway"

Ein Sicherheitsgateway (oft auch Firewall genannt) ist ein System aus soft- und hardwaretechnischen Komponenten. Es gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsrichtlinie ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen werden. Zudem können mit Sicherheitsgateways die übertragenen Daten kontrolliert werden.

Sicherheitsgateways werden am zentralen Übergang zwischen zwei unterschiedlich vertrauenswürdigen Netzen eingesetzt. Unterschiedlich vertrauenswürdige Netze stellen dabei nicht unbedingt nur die Kombination Internet-Intranet dar. Vielmehr können auch zwei organisationsinterne Netze unterschiedlich hohen Schutzbedarf besitzen, z. B. bei der Trennung des Bürokommunikationsnetzes vom Netz der Personalabteilung, in dem besonders schutzwürdige, personenbezogene Daten übertragen werden.

Die Verwendung des Begriffs Sicherheitsgateway anstatt des üblicherweise verwendeten Begriffs „Firewall" soll verdeutlichen, dass zur Absicherung von Netzübergängen heute nicht mehr ein einzelnes Gerät verwendet wird, sondern eine Menge von Rechnern, die unterschiedliche Aufgaben übernehmen, z. B. Paketfilterung, Schutz vor Viren oder die Überwachung des Netzverkehrs.

1.2 Erläuterung des Begriffs „Konzeption"

In diesem Dokument wird weniger auf den Prozess der Planung bzw. Vorgehensweise bei der Konzeption von Sicherheitsgateways eingegangen, sondern es werden vielmehr die technischen Möglichkeiten zur Absicherung von Netzübergängen beschrieben. Dabei ist es unerheblich, ob es sich bei dem zu implementierenden Sicherheitsgateway um eine Neuinstallation oder um die Ersetzung eines bestehenden Systems handelt.

Es werden grundlegende Konzepte mit Vorteilen und Risiken unter Einbezug des Grundschutzhandbuchs (hier sind beispielsweise verschiedene Schutzklassen definiert) sowie der Firewall-Studien I + II des BSI [BSI1997], [BSI2001] erläutert. Auch verschiedene IDS-Studien des BSI werden herangezogen.

1.3 Anspruch des Dokuments

Im vorliegenden Dokument werden Vorschläge zur Konzeption eines Sicherheitsgateways unterbreitet, wobei versucht wurde, möglichst allgemeingültige Konzeptionsmöglichkeiten zu benennen. Es werden Vorschläge unter Berücksichtigung der in der Regel bei der Konzeption eines Sicherheitsgateways geltenden Rahmenbedingungen gemacht.

Dieses Dokument erhebt nicht den Anspruch, für jeden erdenklichen Spezialfall eine sichere Lösung zu liefern. U. U. sind Eigenentwicklungen oder eigene Kreativität des Administrators vonnöten. Möglicherweise sind die hier unterbreiteten Vorschläge auch nicht in jeder Einsatzumgebung technisch umsetzbar.

Der Betrieb eines Sicherheitsgateways ist in drei verschiedenen Formen möglich:

1. Das Sicherheitsgateway wird in „Eigenregie“ (d. h. durch Mitarbeiter der eigenen Organisation) betrieben. Mit diesem Fall beschäftigt sich der Leitfaden in der Hauptsache.
2. Das Sicherheitsgateway ist im eigenen Haus installiert und wird von einem Dienstleister fernbetreut. Dieser Fall wird am Rande betrachtet.
3. Das Sicherheitsgateway ist bei einem Dienstleister installiert und wird von diesem betreut. Dieser Fall wird am Rande betrachtet.

1.4 Übersicht über den Aufbau des Dokuments

Kapitel 2 beschreibt die grundlegenden Möglichkeiten von Sicherheitsgateways anhand des Vier-Schichten-Referenzmodells (auch oft „TCP/IP-Modell“ genannt).

Kapitel 3 beschreibt, wie der Inhalt dieses Dokuments in den Gesamtprozess der Installation eines Sicherheitsgateways einzuordnen ist. So z. B. steht der eigentlichen Konzeption noch die Erstellung einer Sicherheitsrichtlinie voran. Anschließend an die Konzeption sind Wartungskonzepte und Konzepte zum Ausbau des Sicherheitsgateways notwendig.

Kapitel 4 beschreibt die Funktionalität der einzelnen Komponenten eines Sicherheitsgateways und die Bedrohungen, denen mit diesen Komponenten entgegengewirkt werden kann. Die Beschreibungen der einzelnen Komponenten sind als grundlegende Definitionen und als Basis für die weiteren Ausführungen dieses Dokuments zu verstehen.

Kapitel 5 beschäftigt sich erstmals mit konkreten Vorschlägen zum Aufbau, indem zwei grundlegende Strukturierungsmöglichkeiten für Sicherheitsgateways vorgestellt werden. In dem darauffolgenden Kapitel werden Möglichkeiten zur funktionalen Erweiterung der Grundstruktur beschrieben, wobei je nach (Schutz-)Bedarf eine Auswahl der vorgestellten Komponenten erfolgen sollte. Während es sich bei den bisherigen Ausführungen um Strukturierungsmöglichkeiten handelte (d. h. um Möglichkeiten zur „Verkabelung“ der einzelnen Komponenten des Sicherheitsgateways), werden in Kapitel 8 Konfigurationsmöglichkeiten, d. h. Einstellungen der Software, beschrieben.

Einzelne Angriffe unter Ausnutzung von Sicherheitsproblemen im Zusammenhang mit häufig verwendeten Protokollen sind beispielhaft in Anhang A zusammengetragen.

In Anhang B werden verbleibende Risiken aufgelistet, zu deren Beseitigung derzeit keine technischen Lösungen existieren. Diese Risiken gehen über die im Anhang A beschriebe-

nen Sicherheitsprobleme hinaus, indem sie beispielsweise auch den Risikofaktor Mensch berücksichtigen.

Des Weiteren werden im Anhang C Hinweise zur Festeilung des Schutzbedarfs und der grundlegenden Struktur eines Sicherheitsgateways unterbreitet. Produktunabhängige Auswahlkriterien zur Anschaffung der Komponenten eines Sicherheitsgateways finden sich in Anhang D und Verweise auf weiterführende Informationen des Grundschutzhandbuchs in Anhang G. Zudem befindet sich im Anhang eine Auflistung, welche Software existiert, mit der sich Teile eines Sicherheitsgateway unter dem Betriebssystem Linux umsetzen lassen (Anhang F).

Spezielle Informationen bzgl. der Konfiguration des Paketfilters „IPTables“ unter Linux befinden sich in Anhang E.

2. Einsatzmöglichkeiten von Sicherheitsgateways

Eine Sicherheitsproblematik in Zusammenhang mit Netzen entsteht immer dann, wenn unterschiedlich vertrauenswürdige Netze (d. h. der Betreiber des einen Netzes vertraut der Sicherheit des anderen Netzes nicht) physikalisch miteinander verbunden werden. Prinzipiell besteht dann die Möglichkeit, dass Nutzer des weniger vertrauenswürdigen Netzes im vertrauenswürdigen Netz die Vertraulichkeit, Integrität und Verfügbarkeit der dort gespeicherten oder übertragenen Daten gefährden.

Eine Zuordnung von Angriffen kann beispielsweise anhand der Netzschichten des Vier-Schichten-Referenzmodells („TCP/IP-Referenzmodell") vorgenommen werden. Das Referenzmodell wird in der folgenden Abbildung beschrieben. Einzelne, detailliert beschriebene (Beispiel-)Angriffe und entsprechende Gegenmaßnahmen zu den aufgelisteten Netzschichten befinden sich in Anhang A.

Schicht	Protokolle (Auswahl)
4. Anwendung	FTP, HTTP, SMTP, Telnet, NNTP, DNS, POP3
3. Transport	TCP, UDP
2. Netzwerk	IP, ICMP, OSPF, (ARP)
1. Netzzugang	Ethernet, Token Ring, FDDI, WLAN

Angriffe auf der MAC-, IP-, TCP-, UDP- und ICMP-Ebene (der Begriff „Ebene" wird im Folgenden synonym zu „Schicht" verwendet) basieren vor allem auf fehlerhaften Header-Daten oder auf geschickter Fragmentierung der übertragenen Pakete. Auf Anwendungsebene hingegen werden vor allem schadhafte Nutzdaten zu Angriffen verwendet, d. h., es werden nicht mehr nur „Spielräume" der Protokoll-Spezifikationen (und der Implementierung durch den TCP/IP-Stack des Betriebssystems) ausgenutzt, sondern vielmehr auch Programmierfehler in der Anwendungssoftware (z. B. des Browsers).

Eine allgemeine Bewertung des Gefährdungspotenzials in Abhängigkeit von den einzelnen Anwendungsschichten ist nicht möglich. Angriffe auf den unterschiedlichen Ebenen können allgemein betrachtet die gleichen Konsequenzen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten haben.

Eine Unterscheidung bzgl. des Gefährdungspotenzials ist hingegen möglich nach:

- der Richtung des Kommunikationsaufbaus (ein Kommunikationsaufbau aus dem vertrauenswürdigen Netz in das nicht-vertrauenswürdige Netz ist besser zu kontrollieren)
- der Verwendung verbindungsloser und verbindungsorientierter Protokolle (verbindungsorientierte Protokolle sind leichter zu kontrollieren)

Die Möglichkeiten von Sicherheitsgateways beschränken sich in der Regel auf den Schutz vor Bedrohungen, die innerhalb der Schichten 2–4 des Vier-Schichten-Referenzmodells liegen. Grenzen der technischen Möglichkeiten sind im Anhang B aufgelistet.

3. Einordnung der Konzeption in den Gesamtzusammenhang

Die folgenden Kapitel stellen jeweils einen Schritt im Prozess zum Aufbau einer sicheren Netzkopplung von vertrauenswürdigen Netzen mit nicht-vertrauenswürdigen Netzen dar. Abbildung 3.1 soll den Ablauf in Form eines Wasserfallmodells verdeutlichen.

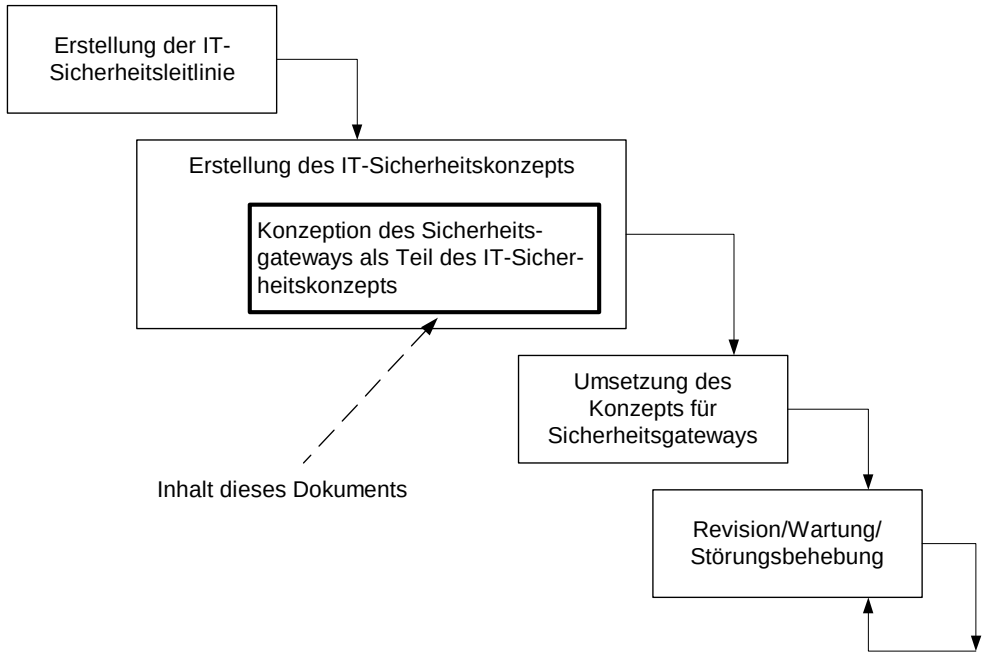

Abb. 3.1: Prozess zum Aufbau einer sicheren Netzkopplung

Die Inhalte der einzelnen Phasen werden in den folgenden Unterkapiteln beschrieben.

3.1 Erstellung oder Anpassung einer IT-Sicherheitsleitlinie

Die IT-Sicherheitsleitlinie (oft auch „Policy" genannt) definiert das angestrebte IT-Sicherheitsniveau, mit dem die Aufgaben durch die Organisation erfüllt werden. Die IT-Sicherheitsleitlinie beinhaltet die von der Organisation angestrebten IT-Sicherheitsziele sowie die verfolgte IT-Sicherheitsstrategie. Sie ist somit Anspruch und Aussage zugleich, dass das IT-Sicherheitsniveau auf allen Ebenen der Organisation erreicht werden soll.

Beispiele für Sicherheitsziele (das genaue Vorgehen zur Gewinnung der Sicherheitsziele ist im Grundschutzhandbuch des BSI [BSI-2002III] beschrieben):

- Hohe Verlässlichkeit des Handelns, besonders bzgl. der Verfügbarkeit der IT, der Korrektheit und der Vertraulichkeit
- Gewährleistung des guten Rufs der Institution in der Öffentlichkeit

- Erhaltung der in Technik, Informationen, Arbeitsprozesse und Wissen investierten Werte
- Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen
- Sicherung der Authentizität der Informationen, z. B. wenn sie als Basis für weitreichende Entscheidungen dienen
- Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen
- Reduzierung der im Schadensfall entstehenden Kosten
- Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Organisation

Die einzelnen IT-Sicherheitsziele können auf unterschiedliche Arten umgesetzt werden. Hierzu sollten generelle IT-Sicherheitsstrategien erarbeitet werden. Mögliche IT-Sicherheitsstrategien können sein:

- Weitestgehende Verschlüsselung aller nach außen gehenden Informationen
- Einsatz starker Authentisierungsverfahren für alle Zugriffe auf IT-Systeme
- Isolierung besonders sensitiver IT-Anwendungen auf nicht vernetzte IT-Systeme

Eine IT-Sicherheitsleitlinie umfasst das Sicherheitsniveau für die gesamte Organisation. Somit wird auch das Sicherheitsniveau für Sicherheitsgateways festgelegt. Dabei werden Aufgaben und Funktionen des Sicherheitsgateways auf allgemeiner Ebene betrachtet, ohne konkrete Vorgaben zur Umsetzung des Sicherheitsgateways zu machen. Konkretere Vorgaben sind Teil des IT-Sicherheitskonzepts, dessen Inhalt im folgenden Kapitel vorgestellt wird.

3.2 Konzeption des Sicherheitsgateways

Die Übersetzung der IT-Sicherheitsleitlinie in konkrete Maßnahmen zum Aufbau einer IT-Infrastruktur geschieht mit Hilfe des IT-Sicherheitskonzepts. Ein IT-Sicherheitskonzept ist das zentrale Dokument im IT-Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen. (Anm.: Das Grundschutzhandbuch unterscheidet zwischen dem IT-Sicherheitskonzept und dem Dokument zur Umsetzung des IT-Sicherheitskonzepts, das aus dem IT-Sicherheitskonzept abgeleitet wird. Diese Unterscheidung wird der Einfachheit halber in diesem Dokument nicht vorgenommen. Die Begriffe „IT-Sicherheitskonzept“ und „Unterlagen zur Umsetzung des IT-Sicherheitskonzepts“ werden in diesem Dokument synonym verwendet.)

Das Problem bei der Ableitung des Sicherheitsgatewaykonzepts aus der IT-Sicherheitsleitlinie besteht darin, aus der High-Level-Policy des IT-Sicherheitskonzepts ein Low-Level-Regelsystem zu erzeugen, das die Struktur des Sicherheitsgateways und die auf den einzelnen Komponenten vorzunehmenden Einstellungen detailliert beschreibt, so dass das Ergebnis den gewünschten Vorgaben entspricht. Die vorliegenden Hinweise zur Konzeption von Sicherheitsgateways sollen hierzu eine Hilfestellung darstellen.

Gerade wegen der Vielzahl unterschiedlicher Einsatzszenarien und Zusatzfunktionen ist es notwendig, sich vor dem Einsatz eines Sicherheitsgateways Klarheit über die eigene Zielsetzung und die spezifischen Anforderungen zu verschaffen. Insbesondere sollten folgende Punkte in ein Sicherheitskonzept aufgenommen werden:

- Einsatzzweck (unterstützte Geschäftsprozesse, notwendige Funktionen)
- Notwendige Schutzwirkung (Identifikation der bedrohten Werte, Bewertung der Risiken, Definition geeigneter Sicherheitsmaßnahmen)
- Richtlinien für die Definition von Filterregeln und insbesondere für den Nachweis von deren Konsistenz
- Technische Anforderungen (Abschätzung des zu erwartenden Durchsatzes, Definition von Verfügbarkeitsanforderungen, Integration in die IT-Umgebung)
- Betriebliche Anforderungen (Anforderungen an die Administration und den Support)

Zur Erstellung des Sicherheitsgatewaykonzepts werden z. B. zu folgenden Themengebieten Vorschläge unterbreitet, die den Entwurf des Sicherheitsgateways unterstützen sollen:

- Feststellung des Schutzbedarfs
- Platzierung des Sicherheitsgateways
- Festlegung des Aufbaus
- Identifikation der zu beschaffenden Module (d. h. Festlegung der zu beschaffenden Produkttypen) und Produktauswahl
- Festlegung der Konfiguration, z. B.
  - Auflistung der erlaubten Verbindungen
  - Auflistung der erlaubten Verbindungsaufbauten von außen nach innen
  - Auflistung der erlaubten Verbindungsaufbauten von innen nach außen
  - Auflistung der notwendigen Dienste und der geeigneten Behandlung
    - Beschreibung der E-Mail-Behandlung (Einstellungen zu aktiven Inhalten, Spam-Filter, Bad Mails, Sperrung von Nutzern etc.)
    - Beschreibung der WWW-Behandlung (Einstellungen zu aktiven Inhalten, URL-Filterung etc.)
  - Auflistung der zugelassenen Befehle, Optionen oder Parameter innerhalb der Protokolle
- Einstellungen bzgl. der Protokollierung
- Aufbau eines Antragswesens (mit dem z. B. Dienste für einen bestimmten Zeitraum freigeschaltet werden)
- Festlegung der Verantwortlichkeit
- Vertreterregelung zur Wartung und zur Kontaktaufnahme mit dem Hersteller der Komponenten des Sicherheitsgateways

Bei der Konzeption eines Sicherheitsgateways ist auf deren Fortschreibung und Umsetzung zu achten. Die Vorgaben für Filterregeln beispielsweise sollten den laufenden organisatorischen Änderungen des IT-Betriebs (Aufnahme neuer Benutzer, Änderung von Benutzerrechten) Rechnung tragen.

Zur Vermeidung von Fehlplanungen sollte bereits in der Konzeptionsphase der Betriebsrat informiert werden, so dass er das Vorhaben und seine Auswirkungen nachvollziehen kann.

Rechtliche Probleme beim Einsatz von Sicherheitsgateways müssen im Einzelfall betrachtet werden, so dass weitere allgemeingültige Aussagen an dieser Stelle nicht möglich sind.

3.3 Umsetzung des Sicherheitskonzepts

In dieser Phase erfolgt die Umsetzung des Sicherheitskonzepts, d. h., es werden die erforderlichen Komponenten entsprechend den Vorgaben des Sicherheitskonzepts ausgewählt, beschafft, installiert und konfiguriert.

Die Auswahl von geeigneten Komponenten spielt in dieser Phase eine wichtige Rolle. Checklisten im Anhang, die allgemeine Anforderungen an Komponenten von Sicherheitsgateways beschreiben, sollen Unterstützung bei der Auswahl leisten.

Die Umsetzungsphase könnte nach dem folgenden Vorschlag untergliedert werden:

1. Gründung eines Projektteams zur Implementation des Sicherheitsgateways
2. Identifizierung und Verteilung von Arbeitspaketen
3. Schulung der Projektbeteiligten
4. Einkauf von Unterstützungsleistung, falls nicht alle Arbeitspakete von Organisationsmitgliedern übernommen werden können
5. Abklärung (und Dokumentation) von Detailproblemen mit dem Hersteller der jeweiligen Produkte
6. Beschaffung, Installation und Konfiguration der Komponenten
7. Dokumentation von Struktur und Konfiguration des Sicherheitsgateways
8. Dokumentation von Problemen bei der Installation des Sicherheitsgateways
9. Dokumentation, welche Nutzer welche Dienste benötigen

Am Ende der Umsetzungsphase sollte sich das Sicherheitsgateway in einem betriebsfähigen Zustand befinden. Dieser Zustand muss im Zuge der Revision regelmäßig überprüft werden.

3.3.1 Revision

Die Revision stellt einen organisatorischen Kontrollmechanismus dar, mit dem eine regelmäßige Prüfung des ordnungsgemäßen Betriebs und die Nachvollziehbarkeit der Arbeitsweise des Sicherheitsgateways ermöglicht werden soll. Die Revision ist eine periodisch wiederkehrende Daueraufgabe, die an die Umsetzungsphase des Sicherheitskonzepts anschließt.

Die Revision ist eine von der Administration getrennte Rolle. Revisoren haben ausschließlich lesenden Zugriff auf alle den Betrieb betreffenden Informationen des Sicherheitsgateways. Hierzu zählen Konfigurations- ebenso wie Protokolldaten. Zum Zweck der Nachvollziehbarkeit ist es wichtig, dass für jede relevante Aktion festgehalten wird, von wem sie zu welchem Zeitpunkt und auf Grund welchen Anlasses durchgeführt wurde.

Die Protokolldaten sind von erheblichem Nutzen, wenn es gilt, zu bestimmten Vorfällen Nachforschungen anzustellen. Sie können zudem z. B. bei Rechtsstreitigkeiten als Beweismittel herangezogen werden. Deshalb ist es wichtig, dass die für die Revision notwendigen Daten nicht unbemerkt manipuliert werden können. Die Verlässlichkeit der bei der Revision in diesem Zusammenhang verwendeten Daten, wie Authentisierungsinformationen, Zeitstempel und sonstige Informationen, sowie deren Vollständigkeit sind ein Maß für die Revisionstauglichkeit eines Systems.

Die Revision von Sicherheitsgateways wird in diesem Dokument nicht weiter behandelt. Das BSI wird hierzu eine eigene Studie erstellen.

3.3.2 Wartung und Störungsbehebung

Die Wartung dient der proaktiven Störungsvermeidung, die Störungsbehebung der (reaktiven) Beseitigung der Ausfallursache. Die Phase der Wartung und Störungsbehebung schließt an die Umsetzungsphase des Sicherheitskonzepts an. Sie verläuft parallel, aber unabhängig von der Revision.

Vor Inbetriebnahme des Sicherheitsgateways muss Klarheit bestehen, welchen Risiken eine Organisation bei einem Ausfall von Teilen oder des gesamten Sicherheitsgateways ausgesetzt ist. Das Verhalten des Sicherheitsgateways bei solchen Geschehnissen sollte vorab feststehen. Einerseits sollte die Möglichkeit eines administrativen Zugriffs zum Zweck der Fehlererkennung und evtl. auch der Fehlerbehebung bei partiellen Ausfällen aufrechterhalten bleiben. Andererseits sollte die Möglichkeit bestehen, bei erkannten Ausfällen zunächst jeglichen Verkehr zu unterbinden. Auf diese Weise kann der Administrator zunächst versuchen, die möglichen Fehlerursachen zu eruieren und gegebenenfalls erfolgte Eindringversuche abzuwehren, bevor weiterer Verkehr über das Sicherheitsgateway geleitet wird.

Zuständigkeiten bzgl. der Fehlerbehebung im Falle eines Ausfalls sollten vor Inbetriebnahme des Sicherheitsgateways abgeklärt werden. Eine Vertreterregelung kann im Bedarfsfall die Fehlerbehebung beschleunigen.