



NET.3: Netzkomponenten

NET.3.2: Firewall

1 Beschreibung

1.1 Einleitung

Eine Firewall ist ein System aus soft- und hardwaretechnischen Komponenten, das dazu eingesetzt wird, IP-basierte Datennetze sicher zu koppeln. Dazu wird mithilfe einer Firewall-Struktur der technisch mögliche Informationsfluss auf die in einer Sicherheitsrichtlinie als vorher sicher definierte Kommunikation eingeschränkt. Sicher bedeutet hierbei, dass ausschließlich die erwünschten Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen werden.

Um Netzübergänge abzusichern, wird oft nicht mehr eine einzelne Komponente verwendet, sondern eine ganze Reihe von IT-Systemen, die unterschiedliche Aufgaben übernehmen, z. B. ausschließlich Pakete zu filtern oder Netzverbindungen mithilfe von Proxy-Funktionen strikt zu trennen. Der in diesem Baustein verwendete Begriff „Application Level Gateway“ (ALG) bezeichnet eine Firewall-Komponente, die Datenströme auf Basis von Sicherheitsproxies regelt.

Eine Firewall wird am Übergang zwischen unterschiedlich vertrauenswürdigen Netzen eingesetzt. Unterschiedlich vertrauenswürdige Netze stellen dabei nicht unbedingt nur die Kombination aus Internet und Intranet dar. Vielmehr können auch zwei institutionsinterne Netze einen unterschiedlich hohen Schutzbedarf besitzen. So hat z. B. das Netz der Bürokommunikation meistens einen geringeren Schutzbedarf als das Netz der Personalabteilung, in dem besonders schützenswerte, personenbezogene Daten übertragen werden.

1.2 Zielsetzung

Ziel des Bausteins ist es, eine Firewall bzw. eine Firewall-Struktur mithilfe der in den folgenden Kapiteln beschriebenen Anforderungen sicher einsetzen zu können, um Netze mit unterschiedlichen Schutzanforderungen sicher miteinander zu verbinden.

1.3 Abgrenzung und Modellierung

Der Baustein NET.3.2 *Firewall* ist auf jede im Informationsverbund eingesetzte Firewall anzuwenden.

Ein typischer Anwendungsfall ist die Absicherung einer Außenverbindung, z. B. beim Übergang eines internen Netzes zum Internet oder bei Anbindungen zu Netzen von Geschäftspartnern. Aber auch bei einer Kopplung von zwei institutionsinternen Netzen mit unterschiedlich hohem Schutzbedarf ist der Baustein anzuwenden, z. B. bei der Trennung des Bürokommunikationsnetzes vom Netz der Entwicklungsabteilung, wenn dort besonders vertrauliche Daten verarbeitet werden.

Der vorliegende Baustein baut auf den Baustein NET.1.1 *Netz-Architektur und -design* auf und enthält konkrete Anforderungen, die zu beachten und zu erfüllen sind, wenn netzbasierte Firewalls beschafft,

aufgebaut, konfiguriert und betrieben werden.

Um Netze abzusichern, sind meistens weitere Netzkomponenten erforderlich, z. B. Router und Switches. Anforderungen hierzu werden jedoch nicht in diesem Baustein aufgeführt, sondern sind in NET.3.1 *Router und Switches* zu finden. Wenn eine Firewall die Aufgaben eines Routers oder Switches übernimmt, gelten für sie zusätzlich die Anforderungen des Bausteins NET.3.1 *Router und Switches*.

Darüber hinaus wird nicht auf Produkte wie sogenannte Next Generation Firewalls (NGFW) oder Unified Threat Management (UTM)-Firewalls eingegangen, die zusätzlich funktionale Erweiterungen enthalten, z. B. VPN, Systeme zur Intrusion Detection und Intrusion Prevention (IDS/IPS), Virens Scanner oder Spam-Filter. Sicherheitsaspekte dieser funktionalen Erweiterungen sind nicht Gegenstand des vorliegenden Bausteins, sondern werden z. B. in den Bausteinen NET.3.3 *VPN* und OPS.1.1.4 *Schutz vor Schadprogrammen* behandelt.

Ebenso wird nicht auf eine Anwendungserkennung bzw. -filterung eingegangen. Sie ist eine gängige Funktion von Next Generation Firewalls sowie IDS/IPS. Da sich die Implementierungen zwischen den Produkten unterscheiden, wird empfohlen, sie je nach Einsatzszenario individuell zu betrachten. In diesem Baustein wird auch nicht auf die individuellen Schutzmöglichkeiten für extern angebotene Server-Dienste eingegangen, z. B. durch ein Reverse Proxy oder für Webdienste mithilfe einer Web Application Firewall (WAF). Darüber hinaus werden Aspekte der infrastrukturellen Sicherheit (z. B. geeignete Aufstellung oder Stromversorgung) nicht in diesem Baustein aufgeführt, sondern finden sich in den jeweiligen Bausteinen der Schicht INF *Infrastruktur*.

Firewalls sollten grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement* sowie OPS.1.1.2 *ordnungsgemäße IT-Administration* mitberücksichtigt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein NET.3.2 *Firewall* von besonderer Bedeutung.

2.1 Distributed Denial of Service (DDoS)

Bei einem DDoS-Angriff auf ein geschütztes Netz (z. B. TCP SYN Flooding, UDP Packet Storm) kann die Firewall aufgrund der vielen Netzverbindungen, die verarbeitet werden müssen, ausfallen. Das kann dazu führen, dass bestimmte Dienste im Local Area Network (LAN) nicht mehr verfügbar sind oder das gesamte LAN ausfällt.

2.2 Manipulation

Gelingt es einem Angreifer, unberechtigt auf eine Firewall oder eine entsprechende Verwaltungsoberfläche zuzugreifen, kann er dort Dateien beliebig manipulieren. So kann er beispielsweise die Konfiguration ändern, zusätzliche Dienste starten oder Schadsoftware installieren. Ebenso kann er auf dem manipulierten IT-System die Kommunikationsverbindungen mitschneiden. Auch lassen sich beispielsweise die Firewall-Regeln so verändern, dass aus dem Internet auf die Firewall und auf das Intranet der Institution zugegriffen werden kann. Weiterhin kann ein Angreifer einen Denial-of-Service (DoS)-Angriff starten, indem er im Regelwerk den Zugriff auf einzelne Server-Dienste verhindert.

2.3 Umgehung der Firewall-Regeln

Angreifer können mithilfe grundlegender Mechanismen in den Netzprotokollen die Firewall-Regeln umgehen (z. B. durch Fragmentierungsangriffe), um in einen durch die Firewall geschützten Bereich einzudringen. Im geschützten Bereich können sie anschließend weiteren Schaden anrichten, z. B. schützenswerte Daten auslesen, manipulieren oder löschen.

2.4 Fehlerhafte Konfiguration und Bedienungsfehler einer Firewall

Eine fehlerhaft konfigurierte oder falsch bediente Firewall kann sich gravierend auf die Verfügbarkeit von Diensten auswirken. Werden beispielsweise Firewall-Regeln falsch gesetzt, können Netzzugriffe blockiert werden. Weiterhin können fehlerhafte Konfigurationen dazu führen, dass IT-Systeme nicht mehr vollständig oder gar nicht mehr geschützt sind. Im schlimmsten Fall sind dadurch interne Dienste für Angreifer erreichbar.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins *NET.3.2 Firewall* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	

3.1 Basis-Anforderungen

Die folgenden Anforderungen **MÜSSEN** für den Baustein *NET.3.2 Firewall* vorrangig erfüllt werden:

NET.3.2.A1 Erstellung einer Sicherheitsrichtlinie (B)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie erstellt werden. In dieser MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie Firewalls sicher betrieben werden können. Die Richtlinie MUSS allen im Bereich Firewalls zuständigen Mitarbeitern bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

NET.3.2.A2 Festlegen der Firewall-Regeln (B)

Die gesamte Kommunikation zwischen den beteiligten Netzen MUSS über die Firewall geleitet werden. Es MUSS sichergestellt sein, dass von außen keine unerlaubten Verbindungen in das geschützte Netz aufgebaut werden können. Ebenso DÜRFEN KEINE unerlaubten Verbindungen aus dem geschützten Netz heraus aufgebaut werden.

Für die Firewall MÜSSEN eindeutige Regeln definiert werden, die festlegen, welche Kommunikationsverbindungen und Datenströme zugelassen werden. Alle anderen Verbindungen MÜSSEN durch die Firewall unterbunden werden (Whitelist-Ansatz). Die Kommunikationsbeziehungen mit angeschlossenen Dienst-Servern, die über die Firewall geführt werden, MÜSSEN in den Regeln berücksichtigt sein.

Es MÜSSEN Verantwortliche benannt werden, die Filterregeln entwerfen, umsetzen und testen. Zudem MUSS geklärt werden, wer Filterregeln verändern darf. Die getroffenen Entscheidungen sowie die relevanten Informationen und Entscheidungsgründe MÜSSEN dokumentiert werden.

NET.3.2.A3 Einrichten geeigneter Filterregeln am Paketfilter (B)

Basierend auf den Firewall-Regeln aus NET.3.2.A2 *Festlegen der Firewall-Regeln* MÜSSEN geeignete

Filterregeln für den Paketfilter definiert und eingerichtet werden.

Ein Paketfilter MUSS so eingestellt sein, dass er alle ungültigen TCP-Flag-Kombinationen verwirft. Grundsätzlich MUSS immer zustandsbehaftet gefiltert werden. Auch für die verbindungslosen Protokolle UDP und ICMP MÜSSEN zustandsbehaftete Filterregeln konfiguriert werden. Die Firewall MUSS die Protokolle ICMP und ICMPv6 restriktiv filtern.

NET.3.2.A4 Sichere Konfiguration der Firewall (B)

Bevor eine Firewall eingesetzt wird, MUSS sie sicher konfiguriert werden. Alle Konfigurationsänderungen MÜSSEN nachvollziehbar dokumentiert sein. Die Integrität der Konfigurationsdateien MUSS geeignet geschützt werden. Bevor Zugangspasswörter abgespeichert werden, MÜSSEN sie mithilfe eines zeitgemäßen kryptografischen Verfahrens abgesichert werden (siehe CON.1 *Kryptokonzept*). Eine Firewall MUSS so konfiguriert sein, dass ausschließlich zwingend erforderliche Dienste verfügbar sind. Wenn funktionale Erweiterungen benutzt werden, MÜSSEN die Sicherheitsrichtlinien der Institution weiterhin erfüllt sein. Auch MUSS begründet und dokumentiert werden, warum solche Erweiterungen eingesetzt werden. Nicht benötigte (Auskunfts-)Dienste sowie nicht benötigte funktionale Erweiterungen MÜSSEN deaktiviert oder ganz deinstalliert werden. Informationen über den internen Konfigurations- und Betriebszustand MÜSSEN nach außen bestmöglich verborgen werden.

NET.3.2.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.2.A6 Schutz der Administrationsschnittstellen (B)

Alle Administrations- und Managementzugänge der Firewall MÜSSEN auf einzelne Quell-IP-Adressen bzw. -Adressbereiche eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht vertrauenswürdigen Netzen heraus nicht auf die Administrationsschnittstellen zugegriffen werden kann.

Um die Firewall zu administrieren bzw. zu überwachen, DÜRFEN NUR sichere Protokolle eingesetzt werden. Alternativ MUSS ein eigens dafür vorgesehenes Administrationsnetz (Out-of-Band-Management) verwendet werden. Für die Benutzerschnittstellen MÜSSEN geeignete Zeitbeschränkungen vorgegeben werden.

NET.3.2.A7 Notfallzugriff auf die Firewall (B)

Es MUSS immer möglich sein, direkt auf die Firewall zuzugreifen zu können, sodass sie im Notfall auch dann lokal administriert werden kann, wenn das gesamte Netz ausfällt.

NET.3.2.A8 Unterbindung von dynamischem Routing (B)

In den Einstellungen der Firewall MUSS das dynamische Routing deaktiviert sein, es sei denn, der Paketfilter wird entsprechend dem Baustein NET.3.1 *Router und Switches* als Perimeter-Router eingesetzt.

NET.3.2.A9 Protokollierung (B)

Die Firewall MUSS so konfiguriert werden, dass sie mindestens folgende sicherheitsrelevante Ereignisse protokolliert:

- abgewiesene Netzverbindungen (Quell- und Ziel-IP-Adressen, Quell- und Zielport oder ICMP/ICMPv6-Typ, Datum, Uhrzeit),
- fehlgeschlagene Zugriffe auf System-Ressourcen aufgrund fehlerhafter Authentisierungen, mangelnder Berechtigung oder nicht vorhandener Ressourcen,
- Fehlermeldungen der Firewall-Dienste,
- allgemeine Systemfehlermeldungen und
- Konfigurationsänderungen (möglichst automatisch).

Werden Sicherheitsproxies eingesetzt, MÜSSEN Sicherheitsverletzungen und Verstöße gegen Access-Control-Listen (ACLs oder auch kurz Access-Listen) in geeigneter Weise protokolliert werden. Hierbei MÜSSEN mindestens die Art der Protokollverletzung bzw. des ACL-Verstoßes, Quell- und Ziel-IP-Adresse, Quell- und Zielpport, Dienst, Datum und Zeit sowie, falls erforderlich, die Verbindungsdauer protokolliert werden.

Wenn sich ein Benutzer am Sicherheitsproxy authentisiert, MÜSSEN auch Authentisierungsdaten oder ausschließlich die Information über eine fehlgeschlagene Authentisierung protokolliert werden.

NET.3.2.A10 Abwehr von Fragmentierungsangriffen am Paketfilter (B)

Am Paketfilter MÜSSEN Schutzmechanismen aktiviert sein, um IPv4- sowie IPv6 Fragmentierungsangriffe abzuwehren.

NET.3.2.A11 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.2.A12 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.2.A13 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.2.A14 Betriebsdokumentationen (B)

Die betrieblichen Aufgaben einer Firewall MÜSSEN nachvollziehbar dokumentiert werden. Es MÜSSEN alle Konfigurationsänderungen sowie sicherheitsrelevante Aufgaben dokumentiert werden, insbesondere Änderungen an den Systemdiensten und dem Regelwerk der Firewall. Die Dokumentation MUSS vor unbefugten Zugriffen geschützt werden.

NET.3.2.A15 Beschaffung einer Firewall (B)

Bevor eine Firewall beschafft wird, MUSS eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Es MUSS darauf geachtet werden, dass das von der Institution angestrebte Sicherheitsniveau mit der Firewall erreichbar ist. Grundlage für die Beschaffung MÜSSEN daher die Anforderungen aus der Sicherheitsrichtlinie sein.

Wird IPv6 eingesetzt, MUSS der Paketfilter die IPv6-Erweiterungsheader (Extension Header) überprüfen. Zudem MUSS sich IPv6 adäquat zu IPv4 konfigurieren lassen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein NET.3.2 *Firewall*. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.3.2.A16 Aufbau einer „P-A-P“-Struktur (S)

Eine „Paketfilter – Application-Level-Gateway – Paketfilter“- (P-A-P)-Struktur SOLLTE eingesetzt werden. Sie MUSS aus mehreren Komponenten mit jeweils dafür geeigneter Hard- und Software bestehen. Für die wichtigsten verwendeten Protokolle SOLLTEN Sicherheitsproxies auf Anwendungsschicht vorhanden sein. Für andere Dienste SOLLTEN zumindest generische Sicherheitsproxies für TCP und UDP genutzt werden. Die Sicherheitsproxies SOLLTEN zudem innerhalb einer abgesicherten Laufzeitumgebung des Betriebssystems ablaufen.

NET.3.2.A17 Deaktivierung von IPv4 oder IPv6 (S)

Wenn das IPv4- oder IPv6-Protokoll in einem Netzsegment nicht benötigt wird, SOLLTE es am jeweiligen Firewall-Netzzugangspunkt (z. B. am entsprechenden Firewall-Interface) deaktiviert werden. Falls das IPv4- oder IPv6-Protokoll nicht benötigt bzw. eingesetzt wird, SOLLTE es auf der Firewall komplett deaktiviert werden.

NET.3.2.A18 Administration über ein gesondertes Managementnetz (S)

Firewalls SOLLTEN ausschließlich über ein separates Managementnetz (Out-of-Band-Management) administriert werden. Eine eventuell vorhandene Administrationsschnittstelle über das eigentliche Datennetz (In-Band) SOLLTE deaktiviert werden. Die Kommunikation im Managementnetz SOLLTE über Management-Firewalls (siehe NET.1.1 *Netz-Architektur und -design*) auf wenige Managementprotokolle mit genau festgelegten Ursprüngen und Zielen beschränkt werden. Die verfügbaren Sicherheitsmechanismen der eingesetzten Managementprotokolle zur Authentisierung, Integritätssicherung und Verschlüsselung SOLLTEN aktiviert sein. Alle unsicheren Managementprotokolle SOLLTEN deaktiviert werden (siehe NET.1.2 *Netz-Management*).

NET.3.2.A19 Schutz vor TCP SYN Flooding, UDP Paket Storm und Sequence Number Guessing am Paketfilter (S)

Am Paketfilter, der Server-Dienste schützt, die aus nicht vertrauenswürdigen Netzen erreichbar sind, SOLLTE ein geeignetes Limit für halboffene und offene Verbindungen gesetzt werden.

Am Paketfilter, der Server-Dienste schützt, die aus weniger oder nicht vertrauenswürdigen Netzen erreichbar sind, SOLLTEN die sogenannten Rate Limits für UDP-Datenströme gesetzt werden.

Am äußeren Paketfilter SOLLTE bei ausgehenden Verbindungen für TCP eine zufällige Generierung von Initial Sequence Numbers (ISN) aktiviert werden, sofern dieses nicht bereits durch Sicherheitsproxies realisiert wird.

NET.3.2.A20 Absicherung von grundlegenden Internetprotokollen (S)

Die Protokolle HTTP, SMTP und DNS inklusive ihrer verschlüsselten Versionen SOLLTEN über protokollspezifische Sicherheitsproxies geleitet werden.

NET.3.2.A21 Temporäre Entschlüsselung des Datenverkehrs (S)

Verschlüsselte Verbindungen in nicht vertrauenswürdige Netze SOLLTEN temporär entschlüsselt werden, um das Protokoll zu verifizieren und die Daten auf Schadsoftware zu prüfen. Hierbei SOLLTEN die rechtlichen Rahmenbedingungen beachtet werden.

Die Komponente, die den Datenverkehr temporär entschlüsselt, SOLLTE unterbinden, dass veraltete Verschlüsselungsoptionen und kryptografische Algorithmen benutzt werden.

Der eingesetzte TLS-Proxy SOLLTE prüfen können, ob Zertifikate vertrauenswürdig sind. Ist ein Zertifikat nicht vertrauenswürdig, SOLLTE es möglich sein, die Verbindung abzuweisen. Eigene Zertifikate SOLLTEN nachrüstbar sein, um auch „interne“ Root-Zertifikate konfigurieren und prüfen zu können. Vorkonfigurierte Zertifikate SOLLTEN überprüft und entfernt werden, wenn sie nicht benötigt werden.

NET.3.2.A22 Sichere Zeitsynchronisation (S)

Die Uhrzeit der Firewall SOLLTE mit einem Network-Time-Protocol (NTP)-Server synchronisiert werden. Die Firewall SOLLTE keine externe Zeitsynchronisation zulassen.

NET.3.2.A23 Systemüberwachung und -Auswertung (S)

Firewalls SOLLTEN in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden. Es SOLLTE ständig überwacht werden, ob die Firewall selbst sowie die darauf betriebenen Dienste korrekt funktionieren. Bei Fehlern oder wenn Grenzwerte überschritten werden, SOLLTE das Betriebspersonal alarmiert werden. Zudem SOLLTEN automatische Alarmmeldungen generiert werden, die bei festgelegten Ereignissen ausgelöst werden. Protokolldaten oder Statusmeldungen SOLLTEN NUR über sichere Kommunikationswege übertragen werden.

NET.3.2.A24 Revision und Penetrationstests (S)

Die Firewall-Struktur SOLLTE regelmäßig auf bekannte Sicherheitsprobleme hin überprüft werden. Es SOLLTEN regelmäßige Penetrationstests und Revisionen durchgeführt werden.

NET.3.2.A32 Notfallvorsorge für die Firewall (S)

Diagnose und Fehlerbehebungen SOLLTEN bereits im Vorfeld geplant und vorbereitet werden. Für typische Ausfallszenarien SOLLTEN entsprechende Handlungsanweisungen definiert und in regelmäßigen Abständen aktualisiert werden.

Die Notfallplanungen für die Firewall SOLLTEN mit der übergreifenden Störungs- und Notfallvorsorge abgestimmt sein. Sie SOLLTEN sich am allgemeinen Notfallvorsorgekonzept orientieren (siehe DER.4 *Notfallmanagement*). Es SOLLTE sichergestellt sein, dass die Dokumentationen zur Notfallvorsorge und die darin enthaltenen Handlungsanweisungen in Papierform vorliegen. Das im Rahmen der Notfallvorsorge beschriebene Vorgehen SOLLTE regelmäßig geprobt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein NET.3.2 *Firewall* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

NET.3.2.A25 Erweiterter Integritätsschutz für die Konfigurationsdateien (H)

Um eine abgestürzte Firewall wieder herzustellen, SOLLTE sichergestellt werden, dass keine alten oder fehlerhaften Konfigurationen (unter anderem Access-Listen) benutzt werden. Dies SOLLTE auch gelten, wenn es einem Angreifer gelingt, die Firewall neu zu starten.

NET.3.2.A26 Auslagerung von funktionalen Erweiterungen auf dedizierte Hardware (H)

Funktionale Erweiterungen der Firewall SOLLTEN auf dedizierte Hard- und Software ausgelagert werden.

NET.3.2.A27 Einsatz verschiedener Firewall-Betriebssysteme und -Produkte in einer mehrstufigen Firewall-Architektur (H)

In einer mehrstufigen Firewall-Architektur SOLLTEN unterschiedliche Betriebssysteme und -Produkte für die äußeren und inneren Firewalls eingesetzt werden.

NET.3.2.A28 Zentrale Filterung von aktiven Inhalten (H)

Aktive Inhalte SOLLTEN gemäß den Sicherheitszielen der Institution zentral gefiltert werden. Dafür SOLLTE auch der verschlüsselte Datenverkehr entschlüsselt werden. Die erforderlichen Sicherheitsproxies SOLLTEN es unterstützen, aktive Inhalte zu filtern.

NET.3.2.A29 Einsatz von Hochverfügbarkeitslösungen (H)

Paketfilter und Application-Level-Gateway SOLLTEN hochverfügbar ausgelegt werden. Zudem SOLLTEN zwei voneinander unabhängige Zugangsmöglichkeiten zum externen Netz bestehen, z. B. zwei Internetzugänge von unterschiedlichen Providern. Interne und externe Router sowie alle weiteren beteiligten aktiven Komponenten (z. B. Switches) SOLLTEN ebenfalls hochverfügbar ausgelegt sein.

Auch nach einem automatischen Failover SOLLTE die Firewall-Struktur die Anforderungen der Sicherheitsrichtlinie erfüllen (Fail safe bzw. Fail secure).

Die Funktion SOLLTE anhand von zahlreichen Parametern überwacht werden. Die Funktionsüberwachung SOLLTE sich nicht auf ein einzelnes Kriterium stützen. Protokolldateien und Warnmeldungen der Hochverfügbarkeitslösung SOLLTEN regelmäßig kontrolliert werden.

NET.3.2.A30 Bandbreitenmanagement für kritische Anwendungen und Dienste (H)

Um Bandbreitenmanagement für kritische Anwendungen und Dienste zu gewährleisten, SOLLTEN Paketfilter mit entsprechender Bandbreitenmanagementfunktion an Netzübergängen und am Übergang zwischen verschiedenen Sicherheitszonen eingesetzt werden.

NET.3.2.A31 Einsatz von zertifizierten Produkten (H)

Firewalls mit einer Sicherheitsevaluierung nach Common Criteria SOLLTEN eingesetzt werden, mindestens mit der Stufe EAL4.

4 Weiterführende Informationen

4.1 Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld Firewall veröffentlicht:

- Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf: BSI-TL-02103 - Version 2.0
- Kryptographische Verfahren: Empfehlungen und Schlüssellängen – Teil 2: Verwendung von Transport Layer Security (TLS): BSI-TR-02102-2
- Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-41 „Guidelines on Firewalls and Firewall Policy“ Empfehlungen zum Einsatz von Firewalls.

5 Anlage: Kreuzreferenztablelle zu elementaren Gefährdungen

Die Kreuzreferenztablelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tablelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein NET.3.2 *Firewall* von Bedeutung.

G 0.8	Ausfall oder Störung der Stromversorgung
G 0.9	Ausfall oder Störung von Kommunikationsnetzen
G 0.14	Ausspähen von Informationen (Spionage)
G 0.18	Fehlplanung oder fehlende Anpassung
G 0.19	Offenlegung schützenswerter Informationen
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle
G 0.21	Manipulation von Hard- oder Software
G 0.22	Manipulation von Informationen
G 0.23	Unbefugtes Eindringen in IT-Systeme
G 0.25	Ausfall von Geräten oder Systemen
G 0.26	Fehlfunktion von Geräten oder Systemen
G 0.27	Ressourcenmangel
G 0.29	Verstoß gegen Gesetze oder Regelungen
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen
G 0.39	Schadprogramme

- G 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.41 Sabotage
- G 0.43 Einspielen von Nachrichten
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen