|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Firewall"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300040 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Firewall" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc81149510)

[Dokumentenhistorie 3](#_Toc81149511)

[Inhaltsverzeichnis 4](#_Toc81149512)

[Allgemeine Festlegungen 6](#_Toc81149513)

[Ziel / Zweck 6](#_Toc81149514)

[Geltungsbereich 6](#_Toc81149515)

[Zuständigkeiten 7](#_Toc81149516)

[Genehmigungs- und Änderungsverfahren 7](#_Toc81149517)

[Aufbau des Dokuments 7](#_Toc81149518)

[Sicherheitsrichtlinie „Firewall" 8](#_Toc81149519)

[Basismaßnahmen 8](#_Toc81149520)

[Festlegung einer Strategie für die Firewall-Infrastruktur (NET.3.2.bd.A1) 8](#_Toc81149521)

[Auswahl einer geeigneten Firewall-Grundstruktur (NET.3.2.bd.A2) 8](#_Toc81149522)

[Nutzung von funktionalen Erweiterungen (NET.3.2.bd.A3) 8](#_Toc81149523)

[Etablierung eines geeigneten Firewall-Regel-Prozesses (NET.3.2.bd.A4) 8](#_Toc81149524)

[Namenskonvention für Firewall-Regeln (NET.3.2.bd.A5) 8](#_Toc81149525)

[Festlegen der Firewall-Regeln (NET.3.2.A2) 9](#_Toc81149526)

[Einrichten geeigneter Filterregeln am Paketfilter (NET.3.2.A3) 9](#_Toc81149527)

[Sichere Konfiguration der Firewall (NET.3.2.A4) 9](#_Toc81149528)

[Restriktive Rechtevergabe (NET.3.2.A5) 10](#_Toc81149529)

[Schutz der Administrationsschnittstellen (NET.3.2.A6) 10](#_Toc81149530)

[Notfallzugriff auf die Firewall (NET.3.2.A7) 10](#_Toc81149531)

[Unterbindung von dynamischem Routing (NET.3.2.A8) 10](#_Toc81149532)

[Protokollierung (NET.3.2.A9) 10](#_Toc81149533)

[Abwehr von Fragmentierungsangriffen am Paketfilter (NET.3.2.A10) 11](#_Toc81149534)

[Einspielen von Updates und Patches (NET.3.2.A11) 11](#_Toc81149535)

[Vorgehen bei Sicherheitsvorfällen (NET.3.2.A12) 12](#_Toc81149536)

[Regelmäßige Datensicherung (NET.3.2.A13) 12](#_Toc81149537)

[Betriebsdokumentationen (NET.3.2.A14) 12](#_Toc81149538)

[Beschaffung einer Firewall (NET.3.2.A15) 12](#_Toc81149539)

[Standardmaßnahmen 12](#_Toc81149540)

[Aufbau einer "P-A-P"-Struktur (NET.3.2.A16) 13](#_Toc81149541)

[Deaktivierung von IPv4 oder IPv6 (NET.3.2.A17) 13](#_Toc81149542)

[Administration über ein gesondertes Managementnetz (NET.3.2.A18) 13](#_Toc81149543)

[Schutz vor TCP SYN Flooding, UDP Paket Storm und Sequence Number Guessing am Paketfilter (NET.3.2.A19) 13](#_Toc81149544)

[Absicherung von grundlegenden Internetprotokollen (NET.3.2.A20) 13](#_Toc81149545)

[Temporäre Entschlüsselung des Datenverkehrs (NET.3.2.A21) 13](#_Toc81149546)

[Sichere Zeitsynchronisation (NET.3.2.A22) 14](#_Toc81149547)

[Systemüberwachung und -Auswertung (NET.3.2.A23) 14](#_Toc81149548)

[Revision und Penetrationstests (NET.3.2.A24) 14](#_Toc81149549)

[Maßnahmen bei erhöhtem Schutzbedarf 14](#_Toc81149550)

[Erweiterter Integritätsschutz für die Konfigurationsdateien (NET.3.2.A25 - CI) 14](#_Toc81149551)

[Auslagerung von funktionalen Erweiterungen auf dedizierte Hardware (NET.3.2.A26 - CIA) 15](#_Toc81149552)

[Einsatz verschiedener Firewall-Betriebssysteme und -Produkte in einer mehrstufigen Firewall-Architektur (NET.3.2.A27 - CI) 15](#_Toc81149553)

[Zentrale Filterung von aktiven Inhalten (NET.3.2.A28 - CI) 15](#_Toc81149554)

[Einsatz von Hochverfügbarkeitslösungen (NET.3.2.A29 - A) 15](#_Toc81149555)

[Bandbreitenmanagement für kritische Anwendungen und Dienste (NET.3.2.A30 - A) 15](#_Toc81149556)

[Einsatz von zertifizierten Produkten (NET.3.2.A31 - CI) 15](#_Toc81149557)

# Allgemeine Festlegungen

## Ziel / Zweck

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 zentralen 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 oder mehrere <Institution>-interne Netze oder der IaaS-, PaaS- und SaaS-Lösung einen unterschiedlich hohen Schutzbedarf besitzen.

Ziel dieser Sicherheitsrichtlinie 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. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteine NET.3.2 "Firewall" zurückgegriffen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „Firewall“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Firewall"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Festlegung einer Strategie für die Firewall-Infrastruktur (NET.3.2.bd.A1)

Bevor von der <Institution> eine Firewall-Infrastruktur bereitgestellt und betrieben wird, muss festgelegt sein, welche generelle Strategie die im Hinblick auf die Kontrolle von Informations- und Kontrollflüssen einnimmt. Insbesondere muss geklärt und festgelegt werden, an welchen Netzgrenzen und an welchen Sicherheitszonengrenzen die Firewall Komponenten aufgebaut werden sollen.

### Auswahl einer geeigneten Firewall-Grundstruktur (NET.3.2.bd.A2)

Auf der Basis der festgelegten Strategie muss entschieden werden, mit welchen Firewall Komponenten und in welcher Abstufung die Firewall-Infrastruktur realisiert werden soll. Hierbei muss sichergestellt sein, dass eine Umgehung einer Firewall Komponente als Kontrollinstanz bei der Kopplung von Sicherheitsbereichen und Sicherheitszonen nicht möglich ist.

Der Zugriff auf öffentliche Netze und auf interne Systeme erfolgt idealerweise über eine dreistufige Firewall-Infrastruktur. Zwischen den Firewall-Stufen wird ein Transfer-Segment implementiert. Eingehender und ausgehender Datenverkehr muss basierend auf dem Schutzbedarf und der Netzstruktur mehrstufig kontrolliert werden. Mittels einer dreistufigen Firewall-Infrastruktur besteht die Möglichkeit, unterschiedliche Notfall-Szenarien auszuarbeiten. Zusätzlich wird eine weitere Sicherheits-Schicht innerhalb des Server-Backbones im Data-Center zur Filterung der OST-West-Kommunikationsflüsse eingeführt.

### Nutzung von funktionalen Erweiterungen (NET.3.2.bd.A3)

Bei der Verwendung von funktionalen Erweiterungen (z. B. Intrusion Prevention System (IPS), Anti-Malware, Advanced Threat Protection, Web-Application-Firewall und SMTP-Gateway, DNS) muss sichergestellt sein, dass die definierten Anforderungen an die Schutzziele Integrität, Authentizität und Verfügbarkeit der Firewall-Infrastruktur weiterhin erfüllt sind.

### Etablierung eines geeigneten Firewall-Regel-Prozesses (NET.3.2.bd.A4)

Es muss, dass einrichten, ändern und löschen von Firewall-Regeln über einen Prozess geregelt und dokumentiert sein. Ebenfalls müssen die Verantwortlichen benannt sein, welche die Firewall-Regeln und deren Auswirkungen koordinieren und zum Zwecke der Nachweisbarkeit bei Sicherheitsvorfällen archivieren.

### Namenskonvention für Firewall-Regeln (NET.3.2.bd.A5)

Für die Benennung von Objekten in der Firewall muss eine Namenskonvention definiert und etabliert werden. Die zu verwendenden Namen müssen übergreifend von einer Koordinationsstelle definiert und vergeben werden.

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

Die Kommunikation zwischen den eingebundenen Netzen wird über die Firewalls geleitet. Die Firewall-Regeln lassen nur die unbedingt benötigten Kommunikationsbeziehungen zu. Alle anderen Verbindungen werden durch die Firewall unterbunden (Whitelist-Ansatz).

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

Wird IPv6 eingesetzt, müssen die Funktionen des IPv6-Protokolls adäquat zum IPv4-Protokoll von der Firewall Komponente beherrscht werden. IPv6 muss sich analog zu IPv4 konfigurieren lassen.

Wird eine App-basierte Filterung eingesetzt, müssen die Funktionen adäquat zum IP-basierten Filtern umsetzbar sein. Die Filterung muss zusätzlich die Möglichkeiten bieten, auf Basis von App-Gruppen sowie Standard Anwendungsports und abweichend von diesen filtern zu können.

Beim Einsatz von ICMP sollten Mechanismen implementiert sein, die den Missbrauch von ICMP Types und Codes erkennen und verhindern. Die nachfolgend aufgeführten ICMP-Pakettypen sind mindestens zu betrachten:

* Typ 0 (Echo-Replay)
* Typ 5 (Redirect)
* Typ 3 (Destination Unreachable)
* Typ 8 (Echo Request)
* Typ 13 (Timestamp Request)
* Typ 15 (Information Request)
* Typ 17 (Address Mask Request)

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

Alle Firewalls werden vor dem Einsatz sicher konfiguriert. Die Firewalls werden ausschließlich von dafür autorisierten Personen in Betrieb genommen und betrieben.

Eine Firewall wird so konfiguriert, dass ausschließlich zwingend erforderliche Dienste verfügbar sind. Wenn funktionale Erweiterungen benutzt werden, sind die Sicherheitsrichtlinien und Vorgaben der <Institution> weiterhin zu erfüllen. Der Einsatz solcher Erweiterungen wird begründet und dokumentiert. Nicht benötigte (Auskunfts-) dienste sowie nicht benötigte funktionale Erweiterungen werden deaktiviert oder ganz deinstalliert.

Die Inhalte der Betriebsdokumentation müssen nachvollziehbar dokumentiert sein. Die Betriebsdokumentation sollte angelehnt an den Lebenszyklus folgende inhaltlichen Phasen beinhalten:

* Inbetriebnahme,
* Betrieb,
* Aussonderung und
* Wiederanlauf.

Die Dokumentation muss gegen unbefugten Zugriff geschützt werden. Änderungen müssen nachvollziehbar dokumentiert bzw. referenziert sein. Änderungen an den Firewall Diensten und dem Regelwerk müssen nachvollziehbar dokumentiert bzw. referenziert sein.

### Restriktive Rechtevergabe (NET.3.2.A5)

Es wird geregelt, wer auf die Firewalls zugreifen darf, z. B. um sie zu konfigurieren oder zu überwachen. Dabei werden nur immer so viele Zugriffsrechte vergeben, wie für die jeweiligen Aufgaben erforderlich sind (Need-to-know-Prinzip). Unautorisierte Benutzerkonten werden entfernt. Es wird sichergestellt, dass mit Administrator-Rechten (bzw. Root-Rechten) nur gearbeitet wird, wenn es notwendig ist.

### Schutz der Administrationsschnittstellen (NET.3.2.A6)

Der Zugang auf die Administrationsschnittstelle der Firewall muss kryptografisch abgesichert erfolgen. Die kryptografischen Algorithmen und Protokolle müssen den Vorgaben der <Institution> entsprechen. Die Zugänge müssen auf einzelne Quelladressen eingeschränkt werden. Es muss der direkte Zugriff auf die Administrationsschnittstellen aus nicht-vertrauenswürdigen Netzen verhindert werden.

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

Zur effizienten und zeitnahen Handhabung von Störungen werden Maßnahmen zur Diagnose und Fehlerbehebung bereits im Vorfeld geplant und vorbereitet. Für typische Störungen werden entsprechende Handlungsanweisungen abgeleitet.

Die Anforderungen und Vorgaben für die Notfallplanung für Firewalls berücksichtigen dabei die Anforderungen und Vorgaben der übergreifenden Störungs- und Notfallvorsorge sowie des allgemeinen Notfallvorsorgekonzepts. Die <Institution> gewährleistet, dass die Dokumentationen zur Notfallvorsorge und die entsprechenden Handlungsanweisungen in Papierform oder in elektronischer Form vorliegen.

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

In den Einstellungen der Firewall wird das dynamische Routing deaktiviert, es sei denn, der Paketfilter wird entsprechend der Sicherheitsrichtlinie "Router und Switches“ als Perimeter-Router eingesetzt.

Im Rahmen der Notfallvorsorge werden das notwendige Vorgehen und die Handlungsanweisungen regelmäßig überprüft. Dieses schließt auch den Notfallzugriff mit ein.

### Protokollierung (NET.3.2.A9)

Zum Zwecke einer übergreifenden Auswertung von Ereignissen muss die Zeit-Synchronisation der Firewall Komponenten mit den etablierten Zeitquellen der <Institution> erfolgen.

Die Firewall muss alle sicherheitsrelevanten Ereignisse und Konfigurationsänderungen protokollieren. Hieraus ableitend sind mindestens folgende Ereignisse protokolliert:

* Abgewiesene Netzverbindungen mit Datum und Uhrzeit
	+ Quell- und Ziel-IP-Adressen,
	+ Quell- und Zielport,
	+ ICMP/ICMPv6-Typ,
	+ Quell- und Ziel-Sicherheitszone
	+ Zielapplikation
* Fehlgeschlagene Zugriffe auf System-Ressourcen aufgrund fehlerhafter Authentisierung, mangelnder Berechtigung oder nicht vorhandener Ressourcen
* Fehlermeldungen der Firewall-Dienste
* Allgemeine Systemfehlermeldungen

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

Die erhobenen Daten dürfen nicht von unbefugten Personen eingesehen und müssen unveränderbar gespeichert werden. Auch müssen bei der Protokollierung gesetzliche und interne Regelungen der <Institution> (u. a. Sicherheitsrichtlinie Protokollierung) eingehalten werden.

Von den Betriebsverantwortlichen muss ein Plan für die Auswertung der Protokollierungen erstellt werden sowie in Zusammenarbeit mit dem Informationssicherheitsmanagementteam eine Anordnung welche Protokolldaten regelmäßig, sporadisch oder nur bei Bedarf ausgewertet werden.

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

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

### Einspielen von Updates und Patches (NET.3.2.A11)

Die Betriebsverantwortlichen für die Firewall-Infrastruktur müssen sich aktiv über bekannt gewordene Schwachstellen informieren. Die Betriebsverantwortlichen für die Firewall-Infrastruktur müssen bekannt gewordene Schwachstellen und für das betreute System identifizierte Schwachstellen zeitnah in Abhängigkeit vom Schutzbedarf und der Kritikalität beheben.

Die Einschätzung der Relevanz von Sicherheitspatches oder sicherheitsrelevanten Änderungen erfolgt zusammen mit dem Informationssicherheitsmanagementteam. Vorab sollte auf Testsystemen bzw. bereitgestellten Infrastrukturen überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen sowie die vereinbarten Schutzbedürfnisse reduzieren. Solange keine Patches für bekannte und relevante Schwachstellen verfügbar sind, müssen geeignete Maßnahmen getroffen werden, um die Firewall-Infrastruktur zu schützen.

Die <Institution> gewährleistet, dass sicherheitsrelevante Patches und Updaten nur aus vertrauenswürdigen Quellen bezogen werden. Insofern Hersteller Prüfsummen für ihre Systeme anbieten, werden die entsprechenden Update-Prüfsummen bzw. digitale Signaturen überprüft.

### Vorgehen bei Sicherheitsvorfällen (NET.3.2.A12)

Bei einem Sicherheitsvorfall müssen die Verantwortlichen in der <Institution> in Übereinstimmung mit der Sicherheitsvorfallbehandlung passende Gegenmaßnahmen einleiten.

Die möglichen Konsequenzen sicherheitskritischer Ereignisse müssen untersucht werden. Letztlich müssen alle erforderlichen Maßnahmen ergriffen werden, um auszuschließen, dass auf das Netz bzw. die IaaS, PaaS und SaaS-Lösung der <Institution> zugegriffen werden kann.

### Regelmäßige Datensicherung (NET.3.2.A13)

Es müssen, vor Installationen und Konfigurationsänderungen sowie in zyklischen Abständen, Systemsicherungen vorgenommen werden. Die <Institution> gewährleistet dabei, dass ein Zugriff auf die Sicherungskopien auch während Notfallsituationen möglich ist.

### Betriebsdokumentationen (NET.3.2.A14)

Die Inhalte der Betriebsdokumentation müssen nachvollziehbar dokumentiert sein. Die Betriebsdokumentation sollte angelehnt an den Lebenszyklus folgende inhaltlichen Phasen beinhalten:

* Inbetriebnahme,
* Betrieb,
* Aussonderung und
* Wiederanlauf.

Die Dokumentation muss gegen unbefugten Zugriff geschützt werden. Änderungen müssen nachvollziehbar dokumentiert bzw. referenziert sein.

### Beschaffung einer Firewall (NET.3.2.A15)

Vor der Beschaffung einer Firewall wird eine Anforderungsliste erstellt, anhand derer die am Markt erhältlichen Produkte bewertet werden. Es wird darauf geachtet, dass das angestrebte Sicherheitsniveau mit der Firewall erreichbar ist.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Aufbau einer "P-A-P"-Struktur (NET.3.2.A16)

Sofern eine "Paketfilter – Application-Level-Gateway – Paketfilter" (P-A-P)-Struktur aufgebaut wird, sollte diese aus mehreren Komponenten mit jeweils geeigneter Hard- und Software bestehen. Für die wichtigsten verwendeten Protokolle müssen Sicherheitsproxys auf Anwendungsschicht (Application-Level-Gateway) vorhanden sein und für andere Dienste zumindest generische Sicherheitsproxys für TCP und UDP. Die Sicherheitsproxys müssen innerhalb einer abgesicherten Laufzeitumgebung des Betriebssystems ablaufen.

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

Sofern das Kommunikationsdesign keinen Dual-Stack Betrieb vorsieht, sollte das nicht benötigte IP-Protokoll (IPv4 oder IPv6) am entsprechenden Firewall-Interface nicht aktiviert werden.

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

Die Komponenten der Firewall-Infrastruktur sollten ausschließlich über ein dediziertes Management-Netz administriert werden, welches nicht die etablierte Sicherheitsinfrastruktur der <Institution> umgeht. Eine gegebenenfalls vorhandene In-Band-Konfigurierbarkeit ist in diesem Fall nicht erforderlich und sollte deaktiviert werden.

Beim Einsatz von cloudbasierten Lösungen für das Management von Firewall-Komponenten müssen die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit hinsichtlich der Absicherung der Steuerungskommunikation und der Nutzdatenübertragung beachtet und eingehalten werden.

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

Ein erfolgreicher DoS oder DDoS-Angriff kommt einer Einladung zu weiteren Angriffen gleich. Aus diesem Grunde sollten Mechanismen zur Erkennung und Abwehr von hochvolumigen Angriffen, TCP-State-Exhaustion Angriffen und Angriffen auf Applikationsebene implementiert sein. Hieraus ableitend sollte die Firewall die Parametrierung für halboffene und offene Verbindungen ermöglichen. Die Konfiguration von sogenannten Rate Limits für UDP-Datenströme unterstützen sowie bei ausgehenden Verbindungen in öffentliche Netze für TCP eine zufällige Generierung von Initial Sequence Numbers (ISN) aktivieren, sofern dies nicht bereits durch Sicherheits-Proxys realisiert wurde.

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

Um ins Internet zu kommunizieren, sollten die Protokolle HTTP, SMTP und DNS inklusive ihrer verschlüsselten Versionen über protokollspezifische Sicherheitsproxys geleitet werden.

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

Verschlüsselte Verbindungen in nicht-vertrauenswürdige Netze sollten temporär entschlüsselt werden, um das Protokoll zu verifizieren und die Daten auf Schadsoftware zu prüfen. Hierbei müssen die Schutzziele hinsichtlich Vertraulichkeit und Verfügbarkeit der übertragenden Informationen sowie die rechtlichen Rahmenbedingungen beachtet werden.

Die Komponente, die den Datenverkehr temporär entschlüsselt, d. h. aufbricht und somit einen Man-in-the-Middle durchführt, muss unterbinden, dass nicht freigegebene Verschlüsselungsoptionen und kryptografische Algorithmen benutzt werden. Mit temporären entschlüsseln ist nicht SSL-Offloading gemeint.

### Sichere Zeitsynchronisation (NET.3.2.A22)

Zum Zwecke einer übergreifenden Auswertung von Ereignissen muss die Zeit-Synchronisation der Firewall Komponenten mit den etablierten Zeitquellen der <Institution> erfolgen. Die Firewall sollte keine externe Zeitsynchronisation zulassen.

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

Firewalls sind in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept einzubinden und die angefallenen Protokolldaten sind proaktiv auszuwerten. Im Rahmen des Einrichten der automatischen und schwellwertbasierten Systemüberwachung ist zu hinterlegen, welche Protokolle regelmäßig, sporadisch oder nur anlassbezogen auszuwerten sind. Bei Fehlern oder wenn Grenzwerte überschritten werden, erfolgt eine Alarmierung der Betriebsverantwortlichen. Protokolldaten oder Statusmeldungen sollten nur über sichere Kommunikationswege an zentrale Logging-Server übertragen werden.

### Revision und Penetrationstests (NET.3.2.A24)

Im Rahmen von regelmäßigen Penetrationstests werden die Komponenten der Firewall-Infrastruktur gegenüber bekannten Sicherheitsschwachstellen überprüft. Zusätzlich wird in regelmäßigen Revisionen festgestellt, ob der Ist-Zustand den festgelegten Anforderungen und Vorgaben entspricht. Sowohl für Penetrationstests als auch Revisionen werden die Ergebnisse mit dem Soll-Zustand abgeglichen und die entsprechenden Abweichungen und Ergebnisse dokumentiert. Die <Institution> stellt über geregelte Verfahren sicher, dass Abweichungen im Anschluss nachverfolgt und geschlossen werden.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Erweiterter Integritätsschutz für die Konfigurationsdateien (NET.3.2.A25 - CI)

Stürzt ein System ab, wird sichergestellt, dass keine alten oder fehlerhaften Konfigurationen beim Prozessneustart benutzt werden. Dies gilt auch, wenn es einem Angreifer gelingt, die Firewall neu zu starten.

### Auslagerung von funktionalen Erweiterungen auf dedizierte Hardware (NET.3.2.A26 - CIA)

Um das Angriffspotenzial weiter zu minimieren, lagert die <Institution> funktionale Erweiterungen der Firewall auf dedizierte Hard- und Software aus.

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

In einer mehrstufigen Firewall-Architektur werden unterschiedliche Betriebssysteme und -Produkte für die äußeren und inneren Firewalls eingesetzt, damit sich eine potenzielle Schwachstelle eines Betriebssystems oder eines Produkts weniger weitreichend auswirkt.

### Zentrale Filterung von aktiven Inhalten (NET.3.2.A28 - CI)

Aktive Inhalte sollten gemäß den Sicherheitszielen der <Institution> zentral gefiltert werden. Dafür kann bei Bedarf auch der verschlüsselte Datenverkehr entschlüsselt werden, um das Entfernen oder Blockieren aktiver Inhalte zu ermöglichen. Die erforderlichen Sicherheits-Proxys müssen das Herausfiltern von aktiven Inhalten unterstützen.

### Einsatz von Hochverfügbarkeitslösungen (NET.3.2.A29 - A)

Die Realisierung einer Hochverfügbarkeitslösung garantiert einen reibungslosen Betrieb der Firewalls bzw. dessen Sicherheitsfunktionen. Es sollten zwei voneinander unabhängige Zugangsmöglichkeiten zum externen Netz bestehen.

### Bandbreitenmanagement für kritische Anwendungen und Dienste (NET.3.2.A30 - A)

Um Bandbreitenmanagement einzuführen, sollten die Firewalls an Netzübergängen und am Übergang zwischen verschiedenen Sicherheitszonen Bandbreitenmanagement-Funktion enthalten.

### Einsatz von zertifizierten Produkten (NET.3.2.A31 - CI)

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