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

Sicherheitsrichtlinie "Router und Switches"

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 | ISMS300039 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [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](#_Toc81148161)

[Dokumentenhistorie 3](#_Toc81148162)

[Inhaltsverzeichnis 4](#_Toc81148163)

[Allgemeine Festlegungen 6](#_Toc81148164)

[Ziel / Zweck 6](#_Toc81148165)

[Geltungsbereich 6](#_Toc81148166)

[Zuständigkeiten 6](#_Toc81148167)

[Genehmigungs- und Änderungsverfahren 7](#_Toc81148168)

[Aufbau des Dokuments 7](#_Toc81148169)

[Sicherheitsrichtlinie „Router und Switches" 8](#_Toc81148170)

[Basismaßnahmen 8](#_Toc81148171)

[Sichere Grundkonfiguration eines Routers oder Switches (NET.3.1.A1) 8](#_Toc81148172)

[Einspielen von Updates und Patches (NET.3.1.A2) 9](#_Toc81148173)

[Restriktive Rechtevergabe (NET.3.1.A3) 9](#_Toc81148174)

[Schutz der Administrationsschnittstellen (NET.3.1.A4) 9](#_Toc81148175)

[Schutz vor Fragmentierungsangriffen (NET.3.1.A5) 10](#_Toc81148176)

[Notfallzugriff auf Router und Switches (NET.3.1.A6) 10](#_Toc81148177)

[Protokollierung bei Routern und Switches (NET.3.1.A7) 10](#_Toc81148178)

[Regelmäßige Datensicherung (NET.3.1.A8) 10](#_Toc81148179)

[Betriebsdokumentationen (NET.3.1.A9) 10](#_Toc81148180)

[Standardmaßnahmen 11](#_Toc81148181)

[Beschaffung eines Routers oder Switches (NET.3.1.A11) 11](#_Toc81148182)

[Erstellung einer Konfigurations-Checkliste für Router und Switches (NET.3.1.A12) 12](#_Toc81148183)

[Administration über ein gesondertes Managementnetz (NET.3.1.A13) 12](#_Toc81148184)

[Schutz vor Missbrauch von ICMP-Nachrichten (NET.3.1.A14) 12](#_Toc81148185)

[Bogon- und Spoofing-Filterung (NET.3.1.A15) 12](#_Toc81148186)

[Schutz vor "IPv6 Routing Header Type-0"-Angriffen (NET.3.1.A16) 12](#_Toc81148187)

[Schutz vor DoS- und DDoS-Angriffen (NET.3.1.A17) 13](#_Toc81148188)

[Einrichtung von Access Control Lists (NET.3.1.A18) 13](#_Toc81148189)

[Sicherung von Switch-Ports (NET.3.1.A19) 13](#_Toc81148190)

[Sicherheitsaspekte von Routing-Protokollen (NET.3.1.A20) 13](#_Toc81148191)

[Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur (NET.3.1.A21) 13](#_Toc81148192)

[Notfallvorsorge bei Routern und Switches (NET.3.1.A22) 13](#_Toc81148193)

[Revision und Penetrationstests (NET.3.1.A23) 14](#_Toc81148194)

[Maßnahmen bei erhöhtem Schutzbedarf 14](#_Toc81148195)

[Einsatz von Netzzugangskontrollen (NET.3.1.A24 - IA) 14](#_Toc81148196)

[Erweiterter Integritätsschutz für die Konfigurationsdateien (NET.3.1.A25 - I) 14](#_Toc81148197)

[Hochverfügbarkeit (NET.3.1.A26 - A) 14](#_Toc81148198)

[Bandbreitenmanagement für kritische Anwendungen und Dienste (NET.3.1.A27 - A) 15](#_Toc81148199)

[Einsatz von zertifizierten Produkten (NET.3.1.A28 - A) 15](#_Toc81148200)

# Allgemeine Festlegungen

## Ziel / Zweck

Router und Switches bilden das Rückgrat heutiger IT-Netze. Ein Ausfall eines oder mehrerer dieser Komponenten kann zum kompletten Stillstand der gesamten IT-Infrastruktur führen. Dies bedeutet Router und Switches müssen daher besonders abgesichert werden.

Router arbeiten auf der ISO-OSI-Schicht 3 (Netzschicht) und vermitteln Datenpakete anhand der Ziel-IP-Adresse im IP-Header. Router sind in der Lage, Netze mit unterschiedlichen Topographien zu verbinden. Ein Router identifiziert eine geeignete Verbindung zwischen dem Quellsystem bzw. Quellnetz und dem Zielsystem bzw. Zielnetz. In den meisten Fällen geschieht dies, indem er die Datenpakete an den nächsten Router weitergibt.

Switches arbeiteten ursprünglich auf der ISO-OSI-Schicht 2, mittlerweile sind Switches jedoch mit unterschiedlichen Funktionen erhältlich und keine typischen Switches mehr. Die Hersteller von Switches kennzeichnen die Switches meist mit dem OSI-Layer, der unterstützt wird. Dadurch entstanden die Begriffe Layer-2-, Layer-3- und Layer-4-Switch, wobei es sich bei Layer-3- und Layer-4-Switches eigentlich funktional bereits um Router handelt. Die ursprünglich unterschiedlichen Funktionen von Switches und Routern sind somit heute auf Grund der besseren Performance oft auf einem Gerät vereint.

Ziel dieser Sicherheitsrichtlinie ist es, Router und Switches bzw. deren Infrastrukturen mithilfe der in den folgenden Kapiteln beschriebenen Anforderungen sicher einsetzen zu können. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteine NET.3.1 "Router und Switches" 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 „Router und Switches“ 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 „Router und Switches"

## Basismaßnahmen

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

### Sichere Grundkonfiguration eines Routers oder Switches (NET.3.1.A1)

Netzkomponenten werden nur von geeigneten, geschulten und autorisierten Mitarbeitenden betrieben. Bei der Verwendung von funktionalen Erweiterungen (z. B. Spiegelports, Firewallfunktionen oder Virtualisierung) muss sichergestellt sein, dass die definierten Anforderungen an die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der Komponenten und der Netzinfrastruktur weiterhin erfüllt sind. Im Rahmen der Anforderungserhebung und Inbetriebnahme wird zusätzlich die Verwendung der entsprechenden Erweiterung begründet und dokumentiert.

Alle Netzkomponenten müssen so konfiguriert sein, dass sie den Schutzbedarf angemessen erfüllen und nur zwingend erforderliche Dienste, Protokolle und funktionale Erweiterungen verwendeten werden. Nicht benötigte Dienste, Protokolle und funktionale Erweiterungen sind deaktiviert oder ganz deinstalliert. Dafür muss eine passende standardisierte Basiskonfiguration zusammengestellt und dokumentiert werden. Bei der Zusammenstellung der Basiskonfiguration sind mindestens die folgenden Themen zu betrachten:

* Benutzerkonten und Passwörter
* Berechtigungsgruppen
* Authentication-, Authorization- und Accounting-Server
* Management-Interface
* Login-Banner
* Nicht genutzte Switch-Ports
* Dynamische Trunking-Protokolle
* VLAN Trunking Protocol (VTP)
* Default- und Native-VLAN
* NTP-Parameter
* Nicht benötigte Dienste
* Protokollierung
* Backup der Konfiguration
* Filterlisten (Access-Control-Lists)
* Cisco Discovery Protocol (CDP)
* Local Link Discovery Protocol (LLDP)
* Storm Control
* Private VLAN (PVLAN)
* Port Blocking
* Port Security
* Spanning-Tree - Bridge Protocol Data Unit (BPDU) Guard
* Spanning-Tree - Root Guard
* Dynamic Host Conﬁguration Protocol (DHCP) Snooping

Insofern Router und Switches nicht benutzte Schnittstellen aufweisen, werden zum Zwecke des Monitoring auch diese auf ein nicht zugewiesenen VLAN verknüpft. Es ist sicherzustellen, dass jegliche Änderungen an den standardisierten Basiskonfigurationen nachvollziehbar dokumentiert sind. Die <Institution> legt angemessene Maßnahmen fest, um die Integrität von Konfigurationsdateien zu sichern.

Die <Institution> gewährleistet, dass Informationen über interne Konfigurations- und Betriebszustände nicht an Unberechtigte kommuniziert werden. Dieses schließt auch Auskunftsdienste in Richtung des Herstellers ein.

Im Rahmen der Inbetriebnahme von Netzkomponenten werden Standardbenutzerkonten idealerweise gelöscht, ist dies nicht möglich müssen diese an die Vorgaben der <Institution> angepasst werden.

### Einspielen von Updates und Patches (NET.3.1.A2)

Die Verantwortlichen für die betriebenen Netzkomponenten müssen sich aktiv über bekannt gewordene Schwachstellen informieren.

Die Verantwortlichen für die Netzkomponenten 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 unter Verwendung des bereitgestellten Templates. 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 Router und Switches 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.

### Restriktive Rechtevergabe (NET.3.1.A3)

Für die Netzkomponenten muss ein Berichtigungskonzept erstellt, dokumentiert und angewendet werden. Auditoren, technische Konten für die Überwachung sowie den Administratoren sollten nur so viele Berechtigungen eingeräumt werden, wie für die Aufgabenerfüllung notwendig ist (Minimalprinzip). Es muss regelmäßig überprüft werden, ob die zugeteilten Rechte noch angemessen sind.

### Schutz der Administrationsschnittstellen (NET.3.1.A4)

Der Zugang auf die Administrationsschnittstelle der Netzkomponenten muss kryptografisch abgesichert erfolgen. Die kryptografischen Algorithmen und Protokolle müssen den Vorgaben der <Institution> entsprechen.

Administrations- und Managementzugänge von Routern und Switches werden auf einzelne Quell-IP-Adressen bzw. IP-Adressbereich eingeschränkt um unberechtigte Zugriffe zu verhindern. Ferner werden Maßnahmen ergriffen, die den direkten Zugriff auf Managementschnittstellen aus nicht vertrauenswürdigen Netzen unterbinden. Die Zugriffe über Managementschnittstellen werden zusätzlich durch Zeitbeschränkungen geschützt.

Insofern Management-Interfaces über nicht benötigte Dienste verfügen, werden diese deaktiviert. Sollte eine Netzkomponente über eine dedizierte Hardwareschnittstelle verfügen, ist diese über angemessene Maßnahmen vor unberechtigten Zugriff zu schützen.

### Schutz vor Fragmentierungsangriffen (NET.3.1.A5)

Beim Einsatz von IPv4 und IPv6 müssen Mechanismen implementiert sein, die Fragmentierungsangriffe erkennen und verhindern.

### Notfallzugriff auf Router und Switches (NET.3.1.A6)

Es muss für die verantwortlichen Administratoren immer möglich sein, direkt auf Router und Switches z. B. dem Konsolen-Port zuzugreifen, sodass diese im Rahmen des Notfallmanagements weiterhin lokal administriert werden können.

### Protokollierung bei Routern und Switches (NET.3.1.A7)

Zum Zwecke einer übergreifenden Auswertung von Ereignissen muss die Zeit-Synchronisation der Netzkomponenten mit den etablierten internen bzw. freigegeben Zeitquellen der <Institution> erfolgen.

Die Netzkomponenten müssen alle sicherheitsrelevanten Ereignisse und Konfigurationsänderungen protokollieren. Änderungen an der Konfiguration sollten zudem automatisch protokolliert werden. 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> eingehalten werden.

Es muss ein Plan für die Auswertung der Protokollierungen erstellt werden sowie eine Anordnung welche Protokolldaten regelmäßig, sporadisch oder nur bei Bedarf ausgewertet werden.

### Regelmäßige Datensicherung (NET.3.1.A8)

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.3.1.A9)

Die Inhalte der Betriebsdokumentation müssen nachvollziehbar 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.

## Standardmaßnahmen

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

### Beschaffung eines Routers oder Switches (NET.3.1.A11)

Im Rahmen der Beschaffung von Routern und Switches wird eine Anforderungsliste erstellt, auf derer Basis bestehende Angebote bewertet werden. Die <Institution> gewährleistet, dass lediglich diejenigen Geräte beschafft werden, die das angestrebte Sicherheitsniveau erreichen können und nicht zu einer heterogenen Infrastruktur führen.

Beim Einsatz von Zero-Touch-Deployment-Techniken wird bereits in der Beschaffungsphase darauf geachtet, dass nur die Systeme eingekauft werden, die eine kryptografisch abgesichert Kommunikation und Übertragung von Konfigurations- und Betriebssystemelementen anbieten.

Müssen hohe oder sehr hohe Anforderungen an die Vertraulichkeit und Integrität erfüllt werden sind Zero-Touch-Deployment-Techniken, welche auf Protokolle wie TFTP und DHCP aufsetzen nicht zu verwenden.

Virtualisierungstechniken bieten die Möglichkeit, die physische Switch-Hardware nochmals in logische Switches zu separieren. Hierbei ist darauf zu achten, dass dem virtuellen System dedizierte Hardwareressourcen zugewiesen werden können. Zusätzlich ist darauf zu achten, dass beim Einsatz von Virtualisierungstechniken nicht ein gestörter Prozess zum Komplettausfall des Hardwaresystems führt. Die nachfolgend aufgeführten Ressourcen können als Grundlage für die Anforderungsliste herangezogen werden:

* IPv4 multicast route memory
* IPv4 unicast route memory
* IPv6 multicast route memory
* IPv6 unicast route memory
* Port channels
* Switched Port Analyzer (SPAN) monitor sessions
* VLANs
* Virtual routing and forwarding (VRF) instances
* CPU share ratio

Beim Einsatz eines virtuellen Switches dürfen die physischen Switch-Ports nur einem virtuellen Switch zur Verhinderung von Brücken zu teilbar sein.

### Erstellung einer Konfigurations-Checkliste für Router und Switches (NET.3.1.A12)

Für Router und Switches werden Konfigurations-Checklisten erstellt, die zur Überprüfung der sicherheitsrelevanten Einstellungen der Geräte verwendet werden. Auf Grund der Abhängigkeit vom Einsatzzweck werden die unterschiedlichen sicheren Konfigurationen und daraus abgeleiteten Anforderungen in den Konfigurations-Checklisten berücksichtigt.

### Administration über ein gesondertes Managementnetz (NET.3.1.A13)

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

Beim Einsatz von cloud-basierten Lösungen für das Management von Netzkomponenten sollten die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit hinsichtlich der Absicherung der Steuerungskommunikation und der Nutzdatenübertragung beachtet und eingehalten werden.

### Schutz vor Missbrauch von ICMP-Nachrichten (NET.3.1.A14)

ICMP hat als Protokoll der Transportschicht eigentlich die Aufgabe, Fehler- und Diagnoseinformationen zu transportieren. Ein Angreifer kann jedoch durch den Missbrauch von ICMP-Nachrichten die Verfügbarkeit des Netzes stören als auch Informationen über das Netz herausfinden. 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)

### Bogon- und Spoofing-Filterung (NET.3.1.A15)

Die <Institution> trifft angemessene Maßnahmen, die verhindern, dass Angreifer mithilfe von gefälschten, reservierten oder noch nicht zugewiesenen IP-Adressen Zugriff zu Routern und Switches erhalten.

### Schutz vor "IPv6 Routing Header Type-0"-Angriffen (NET.3.1.A16)

Die <Institution> trifft beim Einsatz von IPv6 angemessene Maßnahmen, die Angriffe auf den Routing-Header vom Type-0 erkennen und verhindern.

### Schutz vor DoS- und DDoS-Angriffen (NET.3.1.A17)

Die <Institution> trifft angemessene Maßnahmen, welche hochvolumige Angriffe und TCP-State-Exhaustion-Angriffe erkennen und verhindern.

### Einrichtung von Access Control Lists (NET.3.1.A18)

Die <Institution> stellt sicher, dass der Zugriff auf Router und Switches über Access Control Lists realisiert wird. In Abhängigkeit von der Sicherheitsrichtlinie wird in den Access Control Lists festgelegt, über welche IT-Systeme und Netze mit welchen Methoden auf Router oder Switches zugegriffen werden darf. Insofern sich aus der Sicherheitsrichtlinie keinen spezifischen Regelungen ableiten lassen, wird für die Einstellung der Access Control List der Allow-List-Ansatz angewendet.

### Sicherung von Switch-Ports (NET.3.1.A19)

Die <Institution> trifft angemessene Maßnahmen, die den unberechtigten Zugriff zu Switches unterbinden. Zur Sicherstellung der Verfügbarkeit sollten Layer-2- und Layer-3-Systeme NICHT mittels Makro-Techniken konfiguriert werden.

### Sicherheitsaspekte von Routing-Protokollen (NET.3.1.A20)

Router werden so konfiguriert, dass sie sich authentisieren, wenn sie Routing-Informationen austauschen oder Updates für Routing-Tabellen verschicken. Dementsprechend stellt die <Institution> sicher, dass ausschließlich Routing-Protokolle verwendet werden, die eine Authentisierung unterstützen.

Dynamische Routing-Protokolle sollten ausschließlich in sicheren Netzen verwendet werden. Sie sollten nicht in demilitarisierten Zonen (DMZ) eingesetzt werden. Im Rahmen von SDN ist bei Einsatz von dynamischen Routingprotokollen sicherzustellen, dass deren Einsatz nicht die etablierten Schutzbedürfnisse reduziert.

### Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur (NET.3.1.A21)

Die <Institution> stellt sicher, dass alle Router und Switches an das zentrale Identitäts- und Berechtigungsmanagement angebunden sind.

### Notfallvorsorge bei Routern und Switches (NET.3.1.A22)

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 Router und Switches 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 vorliegen.

Im Rahmen der Notfallvorsorge werden das notwendige Vorgehen und Handlungsanweisungen regelmäßig überprüft.

### Revision und Penetrationstests (NET.3.1.A23)

Im Rahmen von regelmäßigen Penetrationstests werden Router und Switches 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).

### Einsatz von Netzzugangskontrollen (NET.3.1.A24 - IA)

Anstelle einer Port-based Access Control nach Standard IEEE 802.1x-2001 und IEEE 802.1x-2004 verwendet die <Institution> eine Access Control nach IEEE 802.1x 2010 auf Basis von EAP-TLS.

### Erweiterter Integritätsschutz für die Konfigurationsdateien (NET.3.1.A25 - I)

Die <Institution> stellt über angemessene Maßnahmen sicher, dass abgestürzte Router und Switches bei der Wiederherstellung oder Neustart keine alten oder fehlerhaften Konfigurationen verwenden.

### Hochverfügbarkeit (NET.3.1.A26 - A)

Die <Institution> gewährleistet durch die Verwendung einer Hochverfügbarkeitslösung den angemessenen Betrieb von Router oder Switches sowie die geeignete Sicherheitskonfiguration. Router und Switches werden gemäß den Anforderungen der Sicherheitsrichtlinie der <Institution> redundant ausgelegt.

### Bandbreitenmanagement für kritische Anwendungen und Dienste (NET.3.1.A27 - A)

Zur Gewährleistung eines angemessenen Bandbreitenmanagements für kritische Anwendungen und Dienste werden Router und Switches Funktionen verwendet, die die Priorisierung von Bandbreiten zulassen.

### Einsatz von zertifizierten Produkten (NET.3.1.A28 - A)

Die <Institution> stellt sicher, dass ausschließlich Router und Switches verwendet werden, die mindestens eine Sicherheitsevaluierung der Stufe EAL4 nach Common Criteria vorweisen.