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

Sicherheitsrichtlinie "Netzarchitektur und -design sowie Netzmanagement"

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 Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300036 | [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](#_Toc81040163)

[Dokumentenhistorie 3](#_Toc81040164)

[Inhaltsverzeichnis 4](#_Toc81040165)

[Allgemeine Festlegungen 5](#_Toc81040166)

[Ziel / Zweck 5](#_Toc81040167)

[Geltungsbereich 6](#_Toc81040168)

[Zuständigkeiten 6](#_Toc81040169)

[Genehmigungs- und Änderungsverfahren 6](#_Toc81040170)

[Aufbau des Dokuments 6](#_Toc81040171)

[Sicherheitsrichtlinie „Netzarchitektur und -design sowie Netzmanagement" 8](#_Toc81040172)

[Basismaßnahmen 8](#_Toc81040173)

[Netzarchitektur und -design 8](#_Toc81040174)

[Netzmanagement 11](#_Toc81040175)

[Standardmaßnahmen 13](#_Toc81040176)

[Netzarchitektur und -design 13](#_Toc81040177)

[Netzmanagement 16](#_Toc81040178)

[Maßnahmen bei erhöhtem Schutzbedarf 19](#_Toc81040179)

[Netzarchitektur und -design 19](#_Toc81040180)

[Netzmanagement 21](#_Toc81040181)

# Allgemeine Festlegungen

## Ziel / Zweck

Die meisten Institutionen so auch die <Institution> benötigen heute für ihren Geschäftsbetrieb und für die Erfüllung ihrer Fachaufgaben unterschiedliche Datennetze, über die beispielsweise Informationen und Daten ausgetauscht sowie verteilte Anwendungen realisiert werden. In solche Netze werden nicht nur herkömmliche Endgeräte und das Internet angeschlossen. Sie integrieren zunehmend auch mobile Endgeräte und Elemente, die dem Internet of Things (IoT) zugerechnet werden. Insofern sich die <Institution> für eine Cloud-First oder Hybrid Initiative verschreibt, werden stärker die Datennetze der Cloud-Service-Providergenutzt. Die Vorteile, die sich dadurch ergeben, sind unbestritten. Durch die unterschiedlichen Verantwortlichkeiten und teil unterschiedlichen gesetzlichen Anforderungen für die Cloud-Dienstleister steigt die Gefahr der unkontrollierten Kommunikationsflüsse sowie das Risiko der unerwünschten Segmentierung und Separierung der Netze. Aus diesem Grunde ist es wichtig, das eigene Netz bereits durch eine sichere Netzarchitektur zu schützen. Dafür muss zum Beispiel geplant werden, wie ein lokales Netz (Local Area Network, LAN) oder ein Wide Area Network (WAN) sicher aufgebaut werden kann oder die sichere Integration von Cloud-Services erfolgen sollte.

Um ein hohes Sicherheitsniveau zu gewährleisten, sind zusätzliche sicherheitsrelevante Aspekte zu berücksichtigen. Beispiele hierfür sind eine sichere Trennung verschiedener Mandanten und Gerätegruppen auf Netzebene und die Kontrolle ihrer Kommunikation durch Firewall-Techniken. Ein weiteres wichtiges Sicherheitselement ist ein zuverlässiges Netzmanagement. Denn dieses ist Grundvoraussetzung für den sicheren und effizienten Betrieb moderner Netze. Dazu ist es erforderlich, dass das Netzmanagement alle Netzkomponenten umfassend integriert. Außerdem müssen geeignete Maßnahmen umgesetzt werden, um die Netzmanagement-Kommunikation und -infrastruktur zu schützen.

Das Netzmanagement umfasst viele wichtige Funktionen wie z. B. die Netzüberwachung, die Konfiguration der Komponenten, die Behandlung von Ereignissen und die Protokollierung. Eine weitere wichtige Funktion ist das Reporting, das als gemeinsame Plattform für Netz und IT-Systeme angelegt werden kann. Alternativ kann es dediziert als einheitliche Plattform oder als Bestandteil der einzelnen Netzmanagement-Komponenten realisiert werden.

Die Netzmanagement-Infrastruktur besteht aus zentralen Management-Systemen, wie z. B. einem SNMP-Server, Administrations-Endgeräten mit Software für Managementzugriffe und dezentralen Managementagenten. Außerdem gehören dedizierte Managementwerkzeuge wie z. B. Probes bzw. spezifische Messgeräte sowie Managementprotokolle wie z. B. SNMP oder SSH dazu. Auch Managementschnittstellen wie dedizierte Ethernet-Ports oder Konsolen-Ports sind Bestandteil einer Netzmanagement-Infrastruktur.

Ziel dieser Sicherheitsrichtlinie ist es, die Informationssicherheit als integralen Bestandteil der Netzarchitektur und des Netzdesigns sowie des Netzmanagements zu etablieren. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben der BSI Bausteine NET.1.1 "Netzarchitektur und -design" und NET.1.2 "Netzmanagement" 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 „Netzarchitektur und -design sowie Netzmanagement“ 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 „Netzarchitektur und -design sowie Netzmanagement"

## Basismaßnahmen

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

### Netzarchitektur und -design

#### Dokumentation des Netzes (NET.1.1.A2)

Durch die Verantwortlichen muss in Zusammenarbeit mit den Architekten und Planern eine vollständige Dokumentation der durch die <Institution> betriebenen Netze (inklusive Netzplan) erstellt und nachhaltig gepflegt werden. Darin müssen die initiale Ist-Aufnahme sowie alle durchgeführten Änderungen im Netz enthalten sein. Auch muss die logische Struktur des Netzes dokumentiert werden, insbesondere wie die Subnetze zugeordnet und wie das Netz zoniert und segmentiert werden.

Für die Erhebung der erforderlichen Netzdokumentationen soll übergreifend für alle Netze ein Tool verwendet werden.

#### Anforderungsspezifikation für das Netz (NET.1.1.A3)

Die nachfolgend aufgeführten Anforderungen an das Netzdesign, die Netzplanung sowie den Netzbetrieb muss allen Verantwortlichen in der <Institution> und Dienstleistern bekannt sein.

Managed Clients müssen anhand des Verfahrens für Network Access Control IEEE 802.1X (2010) mittels EAP-TLS identifiziert werden. Mittels NAC können Managed Clients eigenen Netzzonen/Sicherheitszonen zugeordnet werden, von denen aus bestimmte Kommunikationsbeziehungen erlaubt werden.

Öffentlich zugängliche IT-Systeme sind potenziell dem Risiko ausgesetzt, kompromittiert zu werden. Die Kommunikation zwischen diesem Sicherheitsbereich und anderen Sicherheitsbereichen innerhalb des Rechenzentrumsverbundes muss durch besondere Mechanismen gesteuert werden.

Wird von den Anforderungen aus dieser Sicherheitsrichtlinie abgewichen, muss dies dokumentiert und mit dem Informationssicherheitsbeauftragten abgestimmt werden. Es muss regelmäßig geeignet überprüft werden, ob diese Sicherheitsrichtlinie noch korrekt umgesetzt ist. Die Ergebnisse müssen sinnvoll dokumentiert werden.

#### Netztrennung in Sicherheitszonen (NET.1.1.A4)

Sicherheitszonen (SZ) werden gemäß Sicherheits- und Verfügbarkeitsanforderungen der Verfahren bzw. IT-Services gebildet. Folgende Anforderungen müssen für die Einordnung von Applikationsteilen in bestehende Zonen bzw. für die Schaffung von neuen Sicherheitszonen berücksichtigt werden:

* Schutzbedarf gemäß Standard "Klassifizierung von Informationen"
* Anspruch auf logische bzw. physische Trennung von anderen Applikationen
* Geforderte Verfügbarkeit

Wird ein Sicherheitsbereich oder eine Sicherheitszone mittels einer Sicherheitskomponente (bspw. Firewall) von anderen Sicherheitsbereichen bzw. Sicherheitszonen getrennt, darf die Sicherheitskomponente bei der Verbindung zwischen den Sicherheitsbereichen bzw. Zonen nicht umgangen werden.

Die Sicherheitskomponente, die zwei Sicherheitsbereiche bzw. zwei Zonen miteinander verbindet, ist die einzige Kopplung zwischen den betroffenen Sicherheitsbereichen bzw. Zonen.

Auf die im Sicherheitsbereich angesiedelten Dienste und Systeme kann von allen Sicherheitsbereichen aus über zuvor definierte, abgestimmte und freigegeben Protokolle zugegriffen werden.

Der Zugriff auf den Sicherheitsbereich „Administration“ erfolgt über Sprungserver und nur nach erfolgter Authentisierung und Autorisierung des Benutzers inklusive zweitem Faktor (2FA). Der administrative Zugriff auf Systeme soll möglichst über dedizierte Admin-Zugänge (physisch oder virtuell von den Zugängen für Anwendungen getrennt) erfolgen.

Die Kommunikation zwischen verschiedenen Sicherheitsbereichen bzw. Sicherheitszonen wird mindestens mittels Sicherheitskomponenten eingeschränkt und kontrolliert. Erfordert das Sicherheitsgefälle zwischen zwei Sicherheitsbereichen bzw. Zonen eine Entkopplung der IP-Kommunikation zwischen ihnen, wird dazu eine Komponente aus den folgenden Kategorien eingesetzt:

* Forward Proxies
* Reverse Proxies
* Application Level Gateways (ALGs)
* Web Application Firewalls (WAFs)
* Sprungserver mit Authentisierung

#### Client-Server-Segmentierung (NET.1.1.A5)

Clients und Server müssen in unterschiedlichen Sicherheitszonen platziert werden. Die Kommunikation zwischen diesen Sicherheitszonen muss mindestens durch einen zustandsbehafteten Paketfilter kontrolliert werden.

Für Gastzugänge und für Netzbereiche, in denen keine ausreichende interne Kontrolle über die Endgeräte gegeben ist, müssen dedizierte Sicherheitssegmente eingerichtet werden.

#### Endgeräte-Segmentierung im internen Netz (NET.1.1.A6)

Es dürfen nur Endgeräte in einem Netzsegment/Sicherheitszone positioniert werden, die einem ähnlichen Sicherheitsniveau entsprechen.

#### Absicherung von schützenswerten Informationen (NET.1.1.A7)

Schützenswerte Informationen müssen über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente kommuniziert wird.

#### Grundlegende Absicherung des Internetzugangs (NET.1.1.A8)

Der Internetzugang muss entsprechend Kapitel "Netztrennung in Sicherheitszonen" gestaltet werden. Der Internetverkehr muss über die etablierte Firewall-Struktur geführt werden. Die Datenflüsse müssen durch die Firewall-Struktur auf die benötigten und freigegebenen Protokolle und Kommunikationsbeziehungen eingeschränkt werden.

#### Grundlegende Absicherung der Kommunikation mit nicht vertrauenswürdigen Netzen (NET.1.1.A9)

Für jedes Netzsegment/Sicherheitszone muss festgelegt werden, inwieweit es als vertrauenswürdig einzustufen ist. Nicht vertrauenswürdig Netzsegmente/Sicherheitszonen müssen wie das Internet behandelt und entsprechend abgesichert werden.

#### DMZ-Segmentierung für Zugriffe aus dem Internet (NET.1.1.A10)

Die Firewall-Struktur muss für alle Dienste bzw. Anwendungen, die aus dem Internet erreichbar sind, um eine sogenannte externe DMZ ergänzt werden. Es sollte ein Konzept zur DMZ-Segmentierung (siehe Kapitel "Anforderungsspezifikation für das Netz" und Kapitel "Netztrennung in Sicherheitszonen") erstellt werden, dass die Sicherheitsrichtlinie und die Anforderungsspezifikation nachvollziehbar umsetzen.

#### Absicherung eingehender Kommunikation vom Internet in das interne Netz (NET.1.1.A11)

Ein Zugriff auf das interne Netz der <Institution> muss über einen sicheren Kommunikationskanal erfolgen und auf vertrauenswürdige IT-Systeme und Benutzer beschränkt werden. Die authentisierten Netzzugriffe ins interne Netz der <Institution> müssen die etablierte Firewall-Infrastruktur (siehe Sicherheitsrichtlinie Firewall) durchlaufen.

#### Absicherung ausgehender interner Kommunikation zum Internet (NET.1.1.A12)

Ausgehende Kommunikation aus dem internen Netzen der <Institution> zum Internet muss an einem Sicherheits-Proxy entkoppelt werden. Die Entkopplung muss in hierfür vorgesehenen Sicherheitsbereich" erfolgen.

#### Netzplanung (NET.1.1.A13)

Jede Netzimplementierung muss geeignet, vollständig und nachvollziehbar geplant werden. Dabei müssen die Sicherheitsrichtlinie sowie die Anforderungsspezifikation beachtet werden. Darüber hinaus müssen in der Planung mindestens die folgenden Punkte bedarfsgerecht berücksichtigt werden:

* Anbindung von Internet, weiterer Standorte,
* Topologie des Gesamtnetzes und der Netzbereiche, d. h. Sicherheitszonen und -segmente,
* Dimensionierung und Redundanz der Netz- und Sicherheitskomponenten, Übertragungsstrecken und Außenanbindungen,
* Zu nutzende Protokolle und deren grundsätzliche Konfiguration und Adressierung, insbesondere IPv4/IPv6-Subnetze von Endgerätegruppen,
* Administration und Überwachung.

Die Netzplanung muss regelmäßig überprüft werden.

#### Umsetzung der Netzplanung (NET.1.1.A14)

Das geplante und verantwortete Netz muss fachgerecht und entsprechend den Bedürfnissen der <Institution> umgesetzt werden. Dies muss während der Abnahme geprüft werden.

#### Regelmäßiger Soll-Ist-Vergleich (NET.1.1.A15)

Es muss regelmäßig durch das Informationssicherheitsmanagementteam geprüft werden, ob das bestehende Netz dem Soll-Zustand entspricht. Dabei muss mindestens geprüft werden, inwieweit es die Sicherheitsrichtlinie und Anforderungsspezifikation erfüllt und inwiefern die umgesetzte Netzstruktur dem aktuellen Stand der Netzplanung entspricht. Dafür müssen die verantwortlichen Bereiche für die Planung und den Betrieb geeignete Prüfkriterien erarbeiten und mit dem <Informationssicherheitsbeauftragter> abstimmen.

### Netzmanagement

#### Planung des Netzmanagements (NET.1.2.A1)

Die Netzmanagement-Infrastruktur muss geeignet geplant werden. Hierbei sollten alle Anforderungen (siehe Kapitel "Anforderungsspezifikation für das Netz" und Kapitel "Netztrennung in Sicherheitszonen") spezifiziert und Verantwortliche adressiert werden sowie das Rollen- und Berechtigungskonzept Berücksichtigung finden. Mindestens müssen folgende Themen berücksichtigt werden:

* Zu trennende Management-Bereiche,
* Zugriffsmöglichkeiten auf die Management-Server,
* Kommunikation für den Management-Zugriff,
* Benutzte Protokolle, z. B. IPv4 und IPv6,
* Anforderungen an Management-Werkzeuge,
* Schnittstellen, um erfasste Ereignis- oder Alarmmeldungen weiterzuleiten,
* Protokollierung, inklusive erforderlicher Schnittstellen zu einer zentralen Protokollierungslösung,
* Reporting und Schnittstellen zu übergreifenden Lösungen,
* Korrespondierende Anforderungen an die einzubindenden Netzkomponenten.

#### Anforderungsspezifikation für das Netzmanagement (NET.1.2.A2)

Ausgehend von den Ergebnissen aus Kapitel "Planung des Netzmanagements" müssen Anforderungen an die Netzmanagement-Infrastruktur und -Prozesse spezifiziert werden. Dabei müssen alle wesentlichen Elemente für das Netzmanagement berücksichtigt werden.

#### Rollen- und Berechtigungskonzept für das Netzmanagement (NET.1.2.A3)

Es muss ein Rollen- und Berechtigungskonzept für das Netzmanagement erstellt, umgesetzt und gepflegt werden. Das Konzept muss die speziellen Tätigkeiten und den zugehörigen Zugriff auf Informationen im Netzmanagement abbilden.

#### Grundlegende Authentisierung für den Netzmanagement-Zugriff (NET.1.2.A4)

Für den Management-Zugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden. Dafür müssen die Vorgaben der <Institution> für die Authentisierungsgüte und den Umgang mit den Authentisierungsinformationen umgesetzt werden. Auch müssen alle Default-Passwörter auf den Netzkomponenten geändert werden. Die neuen Passwörter müssen ausreichend stark sein und der technische Richtlinie - Umgang mit Passwörtern entsprechen.

#### Einspielen von Updates und Patches (NET.1.2.A5)

Die Verantwortlichen für das Netzmanagement müssen sich aktiv über bekannt gewordene Schwachstellen informieren.

Die Verantwortlichen müssen bekannt gewordene Schwachstellen und für das betreute Netzmanagementsystem oder -anwendung 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 Netzmanagement-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.

#### Regelmäßige Datensicherung (NET.1.2.A6)

Alle eingesetzten Netzmanagement-Lösungen müssen in das Datensicherungskonzept eingebunden werden. Hierbei müssen alle spezifischen Daten für das Netzmanagement berücksichtigt werden. Es müssen mindestens die Systemdaten für die Einbindung der zu verwaltenden Komponenten bzw. Objekte, Ereignismeldungen, Statistikdaten sowie vorgehaltene Daten für das Konfigurationsmanagement gesichert werden.

#### Grundlegende Protokollierung von Ereignissen (NET.1.2.A7)

Die etablierte und verantwortete Netzmanagement-Lösung muss in das Protokollierungskonzept eingebunden werden. Darüber hinaus müssen mindestens folgende Ereignisse protokolliert werden:

* unautorisierte Zugriffe bzw. Zugriffsversuche,
* Leistungs- oder Verfügbarkeitsschwankungen des Netzes,
* Fehler in automatischen Prozessen (z. B. bei der Konfigurationsverteilung) sowie
* eingeschränkte Erreichbarkeit von Netzkomponenten.

#### Zeit-Synchronisation (NET.1.2.A8)

Alle Komponenten des Netzmanagements, inklusive der eingebundenen Netzkomponenten, müssen eine synchrone Uhrzeit nutzen. Zum Zwecke einer übergreifenden Auswertung von Ereignissen muss die Zeit-Synchronisation mit den etablierten bzw. freigegebenen Zeitquellen der <Institution> erfolgen.

Für das Management-Netz sollten zur Erkennung eines FalseTickers drei Zeit-Instanz in diesem Netz positioniert und betrieben werden.

#### Sicherung der Netzmanagement-Kommunikation (NET.1.2.A9)

Erfolgt die Netzmanagement-Kommunikation über die produktive Infrastruktur, müssen hierfür nach dem Stand der Technik sichere Protokolle verwendet werden.

#### Beschränkung der SNMP-Kommunikation (NET.1.2.A10)

Im Netzmanagement dürfen keine unsicheren Versionen des Simple Network Management Protocol (SNMP) eingesetzt werden. Grundsätzlich sollte über SNMP nur mit den minimal erforderlichen Zugriffsrechten (lesend, schreibend, Reduzierung der MIB-Views) zugegriffen werden.

## Standardmaßnahmen

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

### Netzarchitektur und -design

#### Spezifikation der Netzarchitektur (NET.1.1.A16)

Auf Basis dieser Sicherheitsrichtlinie und der Anforderungsspezifikation muss eine Architektur für die zu etablierenden Sicherheitsbereiche und Sicherheitszonen (siehe Kapitel "Anforderungsspezifikation für das Netz" und Kapitel "Netztrennung in Sicherheitszonen") entwickelt und nachhaltig gepflegt werden. Dabei sollten alle relevanten Architekturelemente zur Erfüllung der internen Anforderungen betrachtet werden, mindestens jedoch:

* Netzarchitektur des internen Netzes mit Festlegungen dazu, wie Netzvirtualisierungstechniken, Layer-2- und Layer-3-Kommunikation sowie Redundanzverfahren einzusetzen sind,
* Netzarchitektur für Außenanbindungen, inklusive Firewall-Architekturen (siehe Sicherheitsrichtlinie Firewall) und Vorgaben an die Standortkopplung,
* Festlegung, an welchen Stellen des Netzes welche Sicherheitskomponenten wie Firewalls oder IDS/IPS zu platzieren sind und welche Sicherheitsfunktionen diese realisieren müssen,
* Vorgaben für die Netzanbindung der verschiedenen IT-Systeme,
* Netzarchitektur in Virtualisierungs-Hosts, wobei insbesondere Network Virtualization Overlay (NVO) und die Architektur in vertikal integrierten Systemen (ViS) zu berücksichtigen sind,
* Festlegungen der grundsätzlichen Architektur-Elemente für eine Multi-Cloud sowie Absicherung der Anbindungen zu private Cloud und public Cloud,
* Architektur zur sicheren Administration und Überwachung der IT-Infrastruktur.

#### Spezifikation des Netzdesigns (NET.1.1.A17)

Basierend auf der Netzarchitektur muss das Netzdesign für die Sicherheitsbereiche und darin enthaltenen Sicherheitszonen und Außenanbindungen entwickelt und nachhaltig gepflegt werden. Dafür sollten die relevanten Architekturelemente detailliert werden, mindestens jedoch:

* Zulässige Formen von Netzkomponenten inklusive virtualisierter Netzkomponenten,
* Festlegungen darüber, wie WAN- und Funkverbindungen abzusichern sind,
* Anbindung von Endgeräten an Switching-Komponenten, Verbindungen zwischen Netzelementen sowie Verwendung von Kommunikationsprotokollen,
* Redundanzmechanismen für alle Netzelemente,
* Adresskonzept für IPv4 und IPv6 sowie zugehörige Routing- und Switching-Konzepte,
* Virtualisierte Netze in Virtualisierungs-Hosts inklusive NVO,
* Aufbau, Anbindung und Absicherung der Multi-Cloud Komponenten sowie deren sichere Anbindung,
* Festlegungen zum Netzdesign für die sichere Administration und Überwachung der IT-Infrastruktur.

#### P-A-P-Struktur für die Internet-Anbindung (NET.1.1.A18)

Zwischen den zwei Firewall-Stufen sollte ein proxy-basiertes Application-Layer-Gateways (ALG) bzw. müssen entsprechende Sicherheits-Proxies realisiert werden. Diese müssen jeweils über ein Transfernetz (dual-homed) zur äußeren Firewall und zur internen Firewall angebunden werden. In diesen Transfernetzen darf nur das proxy-basierte ALG bzw. dürfen nur entsprechende Sicherheits-Proxies integriert werden. Jeglicher Datenverkehr muss über das ALG bzw. entsprechende Sicherheits-Proxies entkoppelt werden. Ein Transportnetz, das beide Firewall-Stufen direkt miteinander verbindet, darf nicht konfiguriert werden. Die interne Firewall muss zudem die Angriffsfläche des ALGs bzw. der Sicherheits-Proxies gegenüber Innentätern oder IT-Systemen im internen Netz reduzieren.

Authentisierte und vertrauenswürdige Netzzugriffe, ausgehend von einem VPN-Gateway ins interne Netz, sollten nicht das ALG bzw. die Sicherheits-Proxies der P-A-P-Struktur durchlaufen.

#### Separierung der Infrastrukturdienste (NET.1.1.A19)

Server, die grundlegende Dienste für die IT-Infrastruktur bereitstellen, müssen in einem dedizierten Sicherheitsbereich (siehe Kapitel "Anforderungsspezifikation für das Netz" und Kapitel "Netztrennung in Sicherheitszonen") positioniert werden. Die Kommunikation mit ihnen sollte durch einen zustandsbehafteten Paketfilter (Firewall) kontrolliert werden.

#### Zuweisung dedizierter Subnetze für IPv4/IPv6-Endgerätegruppen (NET.1.1.A20)

Unterschiedliche IPv4-/IPv6- Endgeräte sollten je nach verwendeten Protokoll (IPv4-/IPv6- oder IPv4/IPv6-DualStack) dedizierten Netzsegmenten/Subnetzen zugeordnet werden.

#### Separierung des Management-Bereichs (NET.1.1.A21)

Es sollte durchgängig ein Out-of-Band-Management genutzt werden, um die physischen und virtuellen Infrastrukturen der <Institution> zu verwalten. Dabei sollten alle Endgeräte, die für das Management der IT-Infrastruktur benötigt werden, in dedizierten Sicherheitszonen im Sicherheitsbereich „Administration“ positioniert werden. Die Kommunikation mit diesen Endgeräten sollte durch einen zustandsbehafteten Paketfilter (Firewall) kontrolliert werden. Die Kommunikation von und zu diesen Management-Segmenten sollte auf die notwendigen Management-Protokolle mit definierten Kommunikations-Endpunkten beschränkt werden.

Der Sicherheitsbereich „Administration“ sollte mindestens die folgenden Sicherheitszonen umfassen, die abhängig von der Sicherheitsrichtlinie und der Anforderungsspezifikation weiter unterteilt werden sollten:

* Segment(e) für IT-Systeme, die für die Authentisierung und Autorisierung der administrativen Kommunikation zuständig sind,
* Segment(e) für die Administration der IT-Systeme,
* Segment(e) für die Überwachung und das Monitoring,
* Segment(e), die die zentrale Protokollierung inklusive Syslog-Server und SIEM-Server enthalten,
* Segment(e) für IT-Systeme, die für grundlegende Dienste des Management-Bereichs benötigt werden,
* Segment(e) für die Management-Interfaces der zu administrierenden IT-Systeme.

Die verschiedenen Management-Interface der IT-Systeme müssen nach ihrem Einsatzzweck und ihrer Netzplatzierung über einen zustandsbehafteten Paketfilter (Firewall) getrennt werden. Dabei sollten die IT-Systeme (Management-Interface) zusätzlich folgender Zugehörigkeit über dedizierte Firewalls getrennt werden:

* IT-Systeme, die aus dem Internet erreichbar sind,
* IT-Systeme im internen Netz,
* Sicherheitskomponenten, die sich zwischen den aus dem Internet erreichbaren IT-Systemen und dem internen Netz befinden.

Es muss sichergestellt werden, dass die Segmentierung nicht durch die Management-Kommunikation unterlaufen werden kann, d. h. eine Überbrückung von Segmenten muss ausgeschlossen werden.

#### Spezifikation des Segmentierungskonzepts (NET.1.1.A22)

Auf Basis der Anforderungen aus Kapitel "Anforderungsspezifikation für das Netz" und Kapitel "Netztrennung in Sicherheitszonen" sollte ein umfassendes Segmentierungs- und Separierungskonzept inklusive vorhandener virtualisierter Netze (z. B. PaaS (Docker, openshift) IaaS (KVM, VMware)) geplant, umgesetzt, betrieben und nachhaltig gepflegt werden. Das Konzept für die Segmentierung bei erhöhten Schutzbedarf muss mindestens die folgenden Punkte für die produktive Umgebung umfassen:

* Initial anzulegende Sicherheitssegmente und Vorgaben dazu, wie neue Sicherheitssegmente für erhöhten Schutzbedarf zu schaffen sind und wie physische und virtuelle Endgeräte in den Sicherheitssegmenten zu positionieren sind.
* Festlegung für die Segmentierung von Entwicklungs- und Testsystemen (Staging) bei erhöhten Schutzbedarf
* Netzzugangskontrolle (IEEE 802.1X (2010) mit EAP-TLS für Sicherheitssegmente mit Clients
* Anbindung von Netzbereichen, die über Funktechniken (z. B. WLAN, Richtfunk, Bluetooth) oder Standleitung an die Sicherheitssegmente mit angebunden sind
* Anbindung der Virtualisierungs-Hosts und von virtuellen Maschinen auf den Hosts an die Sicherheitssegmente
* Rechenzentrumsautomatisierung vom zentralen IT-Dienstleister
* Festlegungen dazu, wie Endgeräte einzubinden sind, die mehrere Sicherheitssegmente versorgen (bspw. Firewall-, IDS/IPS-, Load Balancer-, Anti-Malware-, Monitoring- und Speicher- sowie Datensicherungslösungen)

Für jedes Sicherheitssegment sollte konzipiert werden, wie es netztechnisch realisiert und betrieben werden soll. Darüber hinaus muss festgelegt werden, welche Sicherheitsfunktionen die Koppelelemente zwischen den Sicherheitssegmenten bereitstellen müssen.

#### Trennung von Sicherheitssegmenten (NET.1.1.A23)

IT-Systeme mit unterschiedlichem Schutzbedarf sollten in verschiedenen Sicherheitssegmenten platziert werden. Ist dies nicht möglich, muss sich der Schutzbedarf nach dem höchsten vorkommenden Schutzbedarf im Sicherheitssegment richten. Darüber hinaus sollten die Sicherheitssegmente abhängig von ihrer Größe und den Segmentierungsanforderungen (siehe Kapitel "Anforderungsspezifikation für das Netz" und Kapitel "Netztrennung in Sicherheitszonen") weiter unterteilt werden. Es muss sichergestellt werden, dass keine Überbrückung von Segmenten oder gar Sicherheitszonen möglich ist.

#### Sichere logische Trennung mittels VLAN (NET.1.1.A24)

Durch ein logisches LAN (VLAN/VXLAN) darf keine Verbindung zwischen einer Sicherheitszone vor dem Application-Layer-Gateway (ALG) bzw. den Sicherheits-Proxies einer P-A-P-Struktur und dem dahinterliegenden Netz geschaffen werden.

Generell muss sichergestellt werden, dass keine Überbrückung von Sicherheitszonen möglich ist, wenn logische LANs eingesetzt werden.

#### Fein- und Umsetzungsplanung von Netzarchitektur und -design (NET.1.1.A25)

Eine Fein- und Umsetzungsplanung für die Netzarchitektur und das Netzdesign sollte durchgeführt, dokumentiert, geprüft und in die etablierte Dokumentlenkung überführt werden.

#### Spezifikation von Betriebsprozessen für das Netz (NET.1.1.A26)

Für einen sicheren und effektiven Betrieb der Netz-Infrastruktur sind Betriebsprozesse bedarfsgerecht zu etablieren und zu dokumentieren. Dabei sollte insbesondere berücksichtigt werden, wie sich die Sicherheitszonierung und Separierung auf den IT-Betrieb auswirken.

#### Einbindung der Netzarchitektur in die Notfallplanung (NET.1.1.A27)

Initial und in regelmäßigen Abständen sollte nachvollziehbar analysiert werden, wie sich die Netzarchitektur und die abgeleiteten Konzepte auf die Notfallplanung und Durchführung von Notfallübungen auswirken.

### Netzmanagement

#### Ist-Aufnahme und Dokumentation des Netzmanagements (NET.1.2.A12)

Es ist eine Dokumentation zu erstellten, die beschreibt, wie die Management-Infrastruktur des Netzes aufgebaut ist. Darin sind die initiale Ist-Aufnahme sowie alle durchgeführten Änderungen im Netzmanagement zu hinterlegen. Insbesondere ist zu dokumentieren, welche Netzkomponenten mit welchen Management-Werkzeugen verwaltet werden. Außerdem sind alle für das Netzmanagement benutzten IT-Arbeitsplätze und -Endgeräte sowie alle Informationsbestände, Management-Daten und Informationen über den Betrieb des Netzmanagements zu erfassen. Letztlich sind sämtliche Schnittstellen zu Anwendungen und Diensten außerhalb des Netzmanagements zu dokumentieren.

Der so dokumentierte Ist-Zustand der Management-Infrastruktur muss mit der Dokumentation der Netz-Infrastruktur abgeglichen werden. Die Dokumentation sollte vollständig und immer aktuell sein.

#### Erstellung eines Netzmanagement-Konzepts (NET.1.2.A13)

Es ist ein Netzmanagement-Konzept zu erstellen und nachhaltig zu pflegen. Dabei sind mindestens folgende Aspekte bedarfsgerecht zu berücksichtigen:

* Methoden, Techniken und Werkzeuge für das Netzmanagement,
* Absicherung des Zugangs und der Kommunikation,
* Netztrennung, insbesondere Zuordnung von Netzmanagement-Komponenten zu Sicherheitszonen,
* Umfang des Monitorings und der Alarmierung je Netzkomponente,
* Protokollierung,
* Automatisierung, insbesondere zentrale Verteilung von Konfigurationsdateien auf Switches,
* Meldeketten bei Störungen und Sicherheitsvorfällen,
* Bereitstellung von Netzmanagement-Informationen für andere Betriebsbereiche und
* Einbindung des Netzmanagements in die Notfallplanung.

#### Fein- und Umsetzungsplanung (NET.1.2.A14)

Es ist eine Fein- und Umsetzungsplanung für die Netzmanagement-Infrastruktur zu erstellen. Hierbei sind alle im Netzmanagement-Konzept adressierten Punkte zu berücksichtigen.

#### Konzept für den sicheren Betrieb der Netzmanagement-Infrastruktur (NET.1.2.A15)

Ausgehend von dieser Sicherheitsrichtlinie und dem Netzmanagement-Konzept ist ein Konzept für den sicheren Betrieb der Netzmanagement-Infrastruktur zu erstellen. Darin sind der Anwendungs- und Systembetrieb für die Netzmanagement-Werkzeuge zu berücksichtigen. Auch ist zu prüfen, wie sich die Leistungen anderer operativer Einheiten einbinden und steuern lassen.

#### Einrichtung und Konfiguration von Netzmanagement-Lösungen (NET.1.2.A16)

Lösungen für das Netzmanagement sind anhand dieser Sicherheitsrichtlinie und der Fein- und Umsetzungsplanung aufzubauen, sicher zu konfigurieren und in Betrieb zu nehmen. Danach sind die spezifischen Prozesse für das Netzmanagement einzurichten.

#### Regelmäßiger Soll-Ist-Vergleich (NET.1.2.A17)

Es wird regelmäßig und nachvollziehbar geprüft, inwieweit die Netzmanagement-Lösung der <Institution> dem Sollzustand entspricht. Auch muss in dieser geprüft werden, inwieweit die umgesetzte Management-Struktur und die genutzten Prozesse dem aktuellen Stand entsprechen. Weiter muss verglichen werden, ob die Management-Infrastruktur auf dem aktuellen Stand der Technik ist.

#### Schulungen für Management-Lösungen (NET.1.2.A18)

Für die eingesetzten Netzmanagement-Lösungen werden Schulungs- und Trainingsmaßnahmen konzipiert und durchgeführt. Die Maßnahmen berücksichtigen die individuellen Gegebenheiten im Configuration-, Availability- und Capacity-Management sowie typische Situationen im Fehlermanagement. Die Schulungen und Trainings werden regelmäßig wiederholt, mindestens jedoch, wenn sich größere technische oder prozessuale Änderungen innerhalb der Netzmanagement-Lösung oder den Verantwortlichkeiten ergeben.

#### Starke Authentisierung des Management-Zugriffs (NET.1.2.A19)

Für den administrativen Zugriff auf Netzkomponenten wird eine dem Stand der Technik entsprechende Authentisierungsmethode verwendet. Die administrativen Zugänge werden über einen zentralen Authentisierungsserver mittels personalisierter Konten über entsprechend sichere Protokolle authentisiert.

#### Absicherung des Zugangs zu Netzmanagement-Lösungen (NET.1.2.A20)

Der Zugriff auf zentrale Netzmanagement-Lösungen und Management-Informationen ist durch eine dem Stand der Technik entsprechende Authentisierungsmethode geschützt. Die Zugänge müssen über einen zentralen Authentisierungsserver mittels personalisierter Konten authentisiert werden.

Es müssen dem Stand der Technik entsprechende Authentisierungs- und Verschlüsselungsmethoden realisiert sein, falls auf Netzmanagement-Werkzeuge von einem Netz außerhalb der Management-Netze, insbesondere aus einem produktiven Netz oder einem unzureichend sicheren Netz, zugegriffen wird.

#### Entkopplung der Netzmanagement-Kommunikation (NET.1.2.A21)

Direkte Management-Zugriffe eines Administrators von einem IT-System außerhalb der Management-Netze auf eine Netzkomponente müssen vermieden werden. Ein solcher Zugriff ohne zentrales Management-Werkzeug darf nur in Notfall-Situation notwendig sein. Es müssen für die Entkopplung des direkten Zuganges auf das zu administrierende Netzsystem Sprungserver im Management-Netz integriert und in einem getrennten Zugangssegment positioniert sein.

#### Beschränkung der Management-Funktionen (NET.1.2.A22)

Es sind nur die benötigten Management-Funktionen aktiviert.

#### Protokollierung der administrativen Zugriffe (NET.1.2.A23)

Im Rahmen des Netzmanagements werden die Sitzungsdaten aller administrativen Zugriffe protokolliert und gespeichert. Hierbei werden die datenschutzrechtlichen Bestimmungen eingehalten.

Die Protokollierungsdaten werden in der Datensicherung ausreichend und gesetzeskonform geschützt. Darüber hinaus muss festgelegt werden, ob und in welchem Umfang Sitzungsdaten für forensische Analysen zu archivieren sind. Wenn Daten archiviert werden, muss darauf geachtet werden, dass dies gesetzeskonform und revisionssicher durchgeführt wird.

#### Zentrale Konfigurationsverwaltung für Netzkomponenten (NET.1.2.A24)

Software bzw. Firmware und Konfigurationsdaten für Netzkomponenten werden automatisch über das Netz verteilt und ohne Betriebsunterbrechung installiert und aktiviert. Die hierfür benötigten Informationen sind an zentraler Stelle sicher verfügbar sowie in die Versionsverwaltung und die Datensicherung eingebunden. Die zentrale Konfigurationsverwaltung ist nachhaltig gepflegt und wird regelmäßig auditiert.

#### Statusüberwachung der Netzkomponenten (NET.1.2.A25)

Die grundlegenden Performance- und Verfügbarkeits-Parameter der zentralen Netzkomponenten werden kontinuierlich überwacht. Hierfür sind vorab die jeweiligen Schwellwerte ermittelt worden (Baselining).

#### Umfassende Protokollierung, Alarmierung und Logging von Ereignissen (NET.1.2.A26)

Wichtige Ereignisse oder Fehlerzustände müssen automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden. Dies gilt sowohl für Ereignisse auf Netzkomponenten als auch für Ereignisse auf den Netzmanagement-Werkzeugen. Das zuständige IT-Personal wird zusätzlich automatisch benachrichtigt. Die Alarmierung und das Logging beinhaltet mindestens folgende Punkte:

* Ausfall bzw. Nichterreichbarkeit von Netz- oder Managementkomponenten
* Hardware-Fehlfunktionen
* Fehlerhafte Anmeldeversuche
* Kritische Zustände oder Überlastung von IT-Systemen

Ereignis-Meldungen bzw. Logging-Daten werden kontinuierlich oder kumuliert einem zentralen Management-System übermittelt. Alarm-Meldungen wird direkt bei Auftreten übermittelt und ausgewertet.

#### Einbindung des Netzmanagements in die Notfallplanung (NET.1.2.A27)

Die Netzmanagement-Lösungen ist in die Notfallplanung eingebunden. Dazu sind die Netzmanagement-Werkzeuge und die Konfigurationen der Netzkomponenten gesichert und in die Wiederanlaufpläne integriert.

#### Platzierung der Management-Clients für das In-Band-Management (NET.1.2.A28)

Für die Administration sowohl der IT-Systeme müssen dedizierte Management-Clients eingesetzt werden.

#### Einsatz von VLANs in der Management-Zone (NET.1.2.A29)

Werden Management Netze durch logische LANs (VLAN/VXLAN) getrennt, muss darauf geachtet werden, dass die Anforderungen aus Kapitel "Anforderungsspezifikation für das Netz" und Kapitel "Netztrennung in Sicherheitszonen" erfüllt 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).

### Netzarchitektur und -design

#### Hochverfügbare Netz- und Sicherheitskomponenten (NET.1.1.A28 - A)

Zentrale Bereiche des internen Netzes sowie die Sicherheitskomponenten sollten hochverfügbar realisiert werden. Hierzu sollten die Komponenten redundant ausgelegt und auch intern hochverfügbar realisiert werden.

#### Hochverfügbare Realisierung von Netzanbindungen (NET.1.1.A29 - A)

Die Netzanbindungen an die Gebäude des Rechenzentrumsverbundes des IT-Dienstleisters sollten vollständig redundant (Kanten und Trassendisjunkt) gestaltet werden. Je nach Verfügbarkeitsanforderung sollten redundante Anbindungen an einen oder verschiedene Anbieter, bedarfsabhängig mit unterschiedlicher Technik und Performance, bedarfsgerecht umgesetzt werden. Auch sollte Wegeredundanz bedarfsgerecht so umgesetzt werden, dass bei einem Ausfall eines Teiles des durch den IT-Dienstleister verwalteten Rechenzentrumsverbundes die Anbindung an öffentliche Netze und an die <Institution> bzw. deren Administrationskomponenten weiterhin gegeben sein. Hierbei sollten mögliche Single Points of Failures (SPoF) und störende Umgebungsbedingungen berücksichtigt werden.

#### Schutz vor Distributed-Denial-of-Service (NET.1.1.A30 - A)

Um DDoS-Angriffe abzuwehren, sollte per Bandbreitenmanagement die verfügbare Bandbreite gezielt zwischen verschiedenen Kommunikationspartnern und Protokollen aufgeteilt werden.

Um DDoS-Angriffe mit sehr hohen Datenraten abwehren zu können, sollten Mitigation-Dienste über größere Internet Service Provider (ISPs) eingekauft und deren Nutzung sollte in Verträgen geregelt werden.

#### Physische Trennung von Sicherheitssegmenten (NET.1.1.A31 - CIA)

Abhängig von den Anforderungen aus Kapitel "Anforderungsspezifikation für das Netz" und Kapitel "Netztrennung in Sicherheitszonen" und den vererbten Anforderungen aus den Verfahren der <Institution> sollten Sicherheitssegmente physisch durch separate Switches getrennt werden. Die physische Separierung der Netzkomponenten darf nicht durch ein darüber liegendes Overlay-Netz überbrückt werden.

#### Physische Trennung von Management-Segmenten (NET.1.1.A32 - CIA)

Abhängig von Sicherheitsrichtlinie und Anforderungsspezifikation sollten Sicherheitssegmente des Management-Bereichs physisch voneinander getrennt werden.

#### Mikrosegmentierung des Netzes (NET.1.1.A33 - CIA)

Um potenzielle Angriffe auf eine geringe Zahl von Endgeräten zu beschränken, sollte das Netz in kleine Segmente bzw. Mikro-Segmente mit sehr ähnlichem Anforderungsprofil und demselben Schutzbedarf unterteilt werden (siehe Kapitel "Anforderungsspezifikation für das Netz" und Kapitel "Netztrennung in Sicherheitszonen"). Insbesondere sollte dies für die DMZ-Segmente berücksichtigt werden.

#### Einsatz kryptografischer Verfahren auf Netzebene (NET.1.1.A34 - CI)

Die Sicherheitssegmente sollten mittels kryptografischer Techniken bereits auf Netzebene realisiert werden. Dafür sollten VPN-Techniken oder IEEE 802.1AE eingesetzt werden.

Wenn über interne Verbindungsstrecken im Rechenzentrumsverbund des IT-Dienstleisters kommuniziert wird, die für einen erhöhten Schutzbedarf nicht ausreichend sicher sind, sollte die Kommunikation angemessen auf Netzebene durch <Institution> zusätzlich verschlüsselt werden.

#### Einsatz von netzbasiertem DLP (NET.1.1.A34 - CI)

Auf Netzebene sollten Systeme zur Data Loss Prevention (DLP) eingesetzt werden, um das Risiko von Datenabflüssen zu verringern.

#### Einsatz von Flow-basiertem Analysen (NET.1.1.A35 - CI)

Auf Netzebene sollten Systeme zur Flow-basierten Analyse eingesetzt werden, um das Risiko von unautorisierten Verbindungen oder den Malware-Verbreitungsweg frühzeitig erkennen oder im Rahmen von Forensik nachgelagert analysieren zu können.

#### Trennung mittels VLAN bei sehr hohem Schutzbedarf (NET.1.1.A36 - CIA)

Bei sehr hohem Schutzbedarf sollten keine logischen LANs (VLAN/VXLAN) eingesetzt werden, sondern physische LAN.

### Netzmanagement

#### Hochverfügbare Realisierung der Management-Lösung (NET.1.2.A30 - A)

Die zentrale Management-Lösung wird hochverfügbar betrieben. Hierzu sind die Server bzw. Werkzeuge inklusive der Netzanbindungen redundant ausgelegt. Auch die einzelnen Komponenten werden hochverfügbar bereitgestellt.

#### Grundsätzliche Nutzung von sicheren Protokollen (NET.1.2.A31 - CIA)

Für das Netzmanagement werden ausschließlich sichere Protokolle benutzt.

#### Physische Trennung des Management-Netzes (NET.1.2.A32 - CIA)

Das Management-Netz sollte physisch getrennt werden.

#### Physische Trennung von Management-Segmenten (NET.1.2.A33 - CIA)

Das Management-Netz sollte in physisch getrennte Sicherheitszonen unterteilt werden. Dabei werden physisch getrennte Sicherheitszonen mindestens für das Management von LAN-Komponenten, Sicherheitskomponenten und Komponenten zur Außenanbindung eingerichtet.

#### Protokollierung von Inhalten administrativer Sitzungen (NET.1.2.A34 - CI)

Ergänzend zur Protokollierung von Sitzungsdaten werden auch die Inhalte von administrativen Zugriffen protokolliert. Alternativ kann nach dem Vier-Augen-Prinzip vorgegangen werden. Auch die protokollierten Inhalte der administrativen Sitzungen sind in der Datensicherung ausreichend und gesetzeskonform geschützt.

#### Festlegungen zur Beweissicherung (NET.1.2.A35 - CIA)

Es sind Vorgehensweisen zur Beweissicherung und zu forensischen Untersuchungen im Rahmen des Netzmanagements festgelegt und dokumentiert worden. Die erhobenen Protokollierungsdaten müssen für forensische Analysen gesetzeskonform und revisionssicher archiviert werden.

#### Einbindung der Protokollierung des Netzmanagements in eine SIEM-Lösung (NET.1.2.A36 - CIA)

Die Protokollierung des Netzmanagements sind in eine Security-Information-and-Event-Management-(SIEM)-Lösung eingebunden. Hierzu müssen die Anforderungskataloge zur Auswahl von Netzmanagement-Lösungen hinsichtlich der erforderlichen Unterstützung von Schnittstellen und Übergabeformaten angepasst werden.

#### Standort-übergreifende Zeitsynchronisation (NET.1.2.A37 - CI)

Die Zeitsynchronisation muss über alle Standorte bzw. Systemen IaaS/PaaS-Providern sichergestellt werden. Zum Zwecke einer übergreifenden Auswertung von Ereignissen muss die Zeit-Synchronisation mit den etablierten bzw. freigegebenen Zeitquellen der <Institution> erfolgen.

Für das separate Management-Netz müssen zur Erkennung eines FalseTickers drei Zeit-Instanz in diesem Netz positioniert und betrieben werden.

#### Festlegung von Notbetriebsformen für die Netzmanagement-Infrastruktur (NET.1.2.A38 - A)

Für eine schnelle Wiederherstellung der Sollzustände von Software bzw. Firmware sowie der Konfiguration der Komponenten in der Netzmanagement-Infrastruktur sind hinreichend gute Ersatzlösungen festzulegen, mit denen die administrativen Tätigkeiten im Notfall durchgeführt werden können.