Bundesamt
für Sicherheit in der
Informationstechnik

# NET.1.1 Netzarchitektur und -design

## 1. Beschreibung

### 1.1. Einleitung

Die meisten Institutionen benötigen heute für ihren Geschäftsbetrieb und für die Erfüllung ihrer Fachaufgaben Datennetze, über die beispielsweise Informationen und Daten ausgetauscht sowie verteilte Anwendungen realisiert werden. An solche Netze werden nicht nur herkömmliche Endgeräte, Netze von Partner-Institutionen und das Internet angeschlossen. Sie integrieren zunehmend auch mobile Endgeräte und Elemente, die dem Internet of Things (IoT) zugerechnet werden. Darüber hinaus werden über Datennetze vermehrt auch Cloud-Dienste sowie Dienste für Unified Communication and Collaboration (UCC) genutzt. Die Vorteile, die sich dadurch ergeben, sind unbestritten. Aber durch die vielen Endgeräte und Dienste steigen auch die Risiken. Deshalb 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. Ebenso müssen nur eingeschränkt vertrauenswürdige externe Netze, z. B. das Internet oder Netze von Kunden, geeignet angebunden werden.

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 eine Firewall. Ein weiteres wichtiges Sicherheitselement, speziell bei Clients, ist außerdem die Netzzugangskontrolle.

### 1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil der Netzarchitektur und des Netzdesigns zu etablieren.

### 1.3. Abgrenzung und Modellierung

Der Baustein NET.1.1 *Netzarchitektur und -design* ist auf das Gesamtnetz einer Institution inklusive aller Teilnetze anzuwenden.

Der Baustein enthält grundsätzliche Anforderungen, die zu beachten und erfüllen sind, wenn Netze geplant, aufgebaut und betrieben werden. Anforderungen für den sicheren Betrieb der entsprechenden

Netzkomponenten, inklusive Sicherheitskomponenten wie z. B. Firewalls, sind nicht Gegenstand des vorliegenden Bausteins. Diese werden in der Bausteingruppe NET.3 *Netzkomponenten* behandelt.

Der Fokus dieses Bausteins liegt auf kabelgebundenen Netzen und der Datenkommunikation. Jedoch müssen allgemeine Anforderungen an die Architektur und das Design, z. B. dass Zonen gegenüber Netzsegmenten immer eine physische Trennung erfordern, für alle Netztechniken beachtet und erfüllt werden.

Weitergehende spezifische Anforderungen für Netzbereiche wie Wireless LAN (WLAN) oder Speichernetze (Storage Area Networks, SAN) werden in der Bausteinschicht NET.2 *Funknetze* bzw. im Baustein SYS.1.8 *Speicherlösungen* behandelt. Darüber hinaus wird auch das Thema Voice over IP (VoIP) sowie die dafür zugrunde liegende Sicherheitsinfrastruktur nicht in diesem Baustein erörtert, sondern in dem entsprechenden Baustein NET.4.2 *VoIP* behandelt.

Spezifische sicherheitstechnische Anforderungen für Virtual Private Clouds und Hybrid Clouds liegen ebenfalls nicht im Fokus dieses Bausteins.

Das Netzmanagement wird im Rahmen der Zonierung und Segmentierung betrachtet, alle weitergehenden Themen des Netzmanagements werden im Baustein NET.1.2 *Netzmanagement* behandelt.

# 2. Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein NET.1.1 *Netzarchitektur und -design* von besonderer Bedeutung.

## 2.1. Ausfall oder unzureichende Performance von Kommunikationsverbindungen

Sind die Kommunikationsverbindungen unzureichend dimensioniert oder reicht ihre Leistung aufgrund eines technischen Ausfalls oder eines Denial-of-Service-(DoS)-Angriffs nicht mehr aus, können z. B. Clients nur noch eingeschränkt mit Servern kommunizieren. Dadurch erhöhen sich die Zugriffszeiten auf interne und externe Dienste. Diese sind so mitunter nur noch eingeschränkt oder gar nicht mehr nutzbar. Auch sind eventuell institutionsrelevante Informationen nicht mehr verfügbar. In der Folge können essenzielle Geschäftsprozesse oder ganze Produktionsprozesse still stehen.

## 2.2. Ungenügend abgesicherte Netzzugänge

Ist das interne Netz mit dem Internet verbunden und der Übergang nicht ausreichend geschützt, z. B. weil keine Firewall eingesetzt wird oder sie falsch konfiguriert ist, können Angreifer auf schützenswerte Informationen der Institution zugreifen und diese kopieren oder manipulieren.

## 2.3. Unsachgemäßer Aufbau von Netzen

Wird ein Netz unsachgemäß aufgebaut oder fehlerhaft erweitert, können unsichere Netztopologien entstehen oder Netze unsicher konfiguriert werden. Angreifer können so leichter Sicherheitslücken finden, ins interne Netz der Institution eindringen und dort Informationen stehlen, Daten manipulieren oder auch ganze Produktionssysteme stören. Auch bleiben Angreifer in einem fehlerhaft aufgebauten Netz, das die Sicherheitssysteme nur eingeschränkt überwachen können, länger unerkannt.

# 3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins aufgeführt. Grundsätzlich ist der Planer für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann

es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

| Zuständigkeiten | Rollen |
|---|---|
| Grundsätzlich zuständig | Planer |
| Weitere Zuständigkeiten | IT-Betrieb |

# 3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein NET.1.1 *Netzarchitektur und -design* vorrangig erfüllt werden:

## NET.1.1.A1 Sicherheitsrichtlinie für das Netz [IT-Betrieb] (B)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für das Netz erstellt werden. Darin MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben werden, wie Netze sicher konzipiert und aufgebaut werden. In der Richtlinie MUSS unter anderem festgelegt werden,

- in welchen Fällen die Zonen zu segmentieren sind und in welchen Fällen Benutzergruppen bzw. Mandanten logisch oder sogar physisch zu trennen sind,
- welche Kommunikationsbeziehungen und welche Netz- und Anwendungsprotokolle jeweils zugelassen werden,
- wie der Datenverkehr für Administration und Überwachung netztechnisch zu trennen ist,
- welche institutionsinterne, standortübergreifende Kommunikation (WAN, Funknetze) erlaubt und welche Verschlüsselung im WAN, LAN oder auf Funkstrecken erforderlich ist sowie
- welche institutionsübergreifende Kommunikation zugelassen ist.

Die Richtlinie MUSS allen im Bereich Netzdesign zuständigen Mitarbeitern bekannt sein. Sie MUSS zudem grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies dokumentiert und mit dem verantwortlichen ISB abgestimmt werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

## NET.1.1.A2 Dokumentation des Netzes [IT-Betrieb] (B)

Es MUSS eine vollständige Dokumentation des Netzes erstellt werden. Sie MUSS einen Netzplan beinhalten. Die Dokumentation MUSS nachhaltig gepflegt werden. Die initiale Ist-Aufnahme, einschließlich der Netzperformance, sowie alle durchgeführten Änderungen im Netz MÜSSEN in der Dokumentation enthalten sein. Die logische Struktur des Netzes MUSS dokumentiert werden, insbesondere, wie die Subnetze zugeordnet und wie das Netz zoniert und segmentiert wird.

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

Ausgehend von der Sicherheitsrichtlinie für das Netz MUSS eine Anforderungsspezifikation erstellt werden. Diese MUSS nachhaltig gepflegt werden. Aus den Anforderungen MÜSSEN sich alle wesentlichen Elemente für Netzarchitektur und -design ableiten lassen.

## NET.1.1.A4 Netztrennung in Zonen (B)

Das Gesamtnetz MUSS mindestens in folgende drei Zonen physisch separiert sein: internes Netz, demilitarisierte Zone (DMZ) und Außenanbindungen (inklusive Internetanbindung sowie Anbindung an andere nicht vertrauenswürdige Netze). Die Zonenübergänge MÜSSEN durch eine Firewall abgesichert werden. Diese Kontrolle MUSS dem Prinzip der lokalen Kommunikation folgen, sodass von Firewalls ausschließlich erlaubte Kommunikation weitergeleitet wird (Whitelisting).

Nicht vertrauenswürdige Netze (z. B. Internet) und vertrauenswürdige Netze (z. B. Intranet) MÜSSEN mindestens durch eine zweistufige Firewall-Struktur, bestehend aus zustandsbehafteten Paketfiltern (Firewall), getrennt werden. Um Internet und externe DMZ netztechnisch zu trennen, MUSS mindestens ein zustandsbehafteter Paketfilter eingesetzt werden.

In der zweistufigen Firewall-Architektur MUSS jeder ein- und ausgehende Datenverkehr durch den äußeren Paketfilter bzw. den internen Paketfilter kontrolliert und gefiltert werden.

Eine P-A-P-Struktur, die aus Paketfilter, Application-Layer-Gateway bzw. Sicherheits-Proxies und Paketfilter besteht, MUSS immer realisiert werden, wenn die Sicherheitsrichtlinie oder die Anforderungsspezifikation dies fordern.

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

Clients und Server MÜSSEN in unterschiedlichen Netzsegmenten platziert werden. Die Kommunikation zwischen diesen Netzsegmenten MUSS mindestens durch einen zustandsbehafteten Paketfilter kontrolliert werden.

Es SOLLTE beachtet werden, dass mögliche Ausnahmen, die es erlauben, Clients und Server in einem gemeinsamen Netzsegment zu positionieren, in den entsprechenden anwendungs- und systemspezifischen Bausteinen geregelt werden.

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

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

Es DÜRFEN NUR Endgeräte in einem Netzsegment positioniert werden, die einem ähnlichen Sicherheitsniveau entsprechen.

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

Schützenswerte Informationen MÜSSEN über nach dem derzeitigen Stand der Technik sichere Protokolle übertragen werden, falls nicht über vertrauenswürdige dedizierte Netzsegmente (z. B. innerhalb des Managementnetzes) kommuniziert wird. Können solche Protokolle nicht genutzt werden, MUSS nach Stand der Technik angemessen verschlüsselt und authentisiert werden (siehe NET.3.3 *VPN).*

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

Der Internetverkehr MUSS über die Firewall-Struktur geführt werden (siehe NET.1.1.A4 *Netztrennung in Zonen*). Die Datenflüsse MÜSSEN durch die Firewall-Struktur auf die benötigten Protokolle und Kommunikationsbeziehungen eingeschränkt werden.

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

Für jedes Netz MUSS festgelegt werden, inwieweit es als vertrauenswürdig einzustufen ist. Netze, die nicht vertrauenswürdig sind, MÜSSEN wie das Internet behandelt und entsprechend abgesichert werden.

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

Die Firewall-Strukur 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 erstellt werden, das die Sicherheitsrichtlinie und die Anforderungsspezifikation nachvollziehbar umsetzt. Abhängig vom Sicherheitsniveau der IT-Systeme MÜSSEN die DMZ-Segmente weitergehend unterteilt werden. Eine externe DMZ MUSS am äußeren Paketfilter angeschlossen werden.

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

Ein IP-basierter Zugriff auf das interne Netz MUSS über einen sicheren Kommunikationskanal erfolgen. Der Zugriff MUSS auf vertrauenswürdige IT-Systeme und Benutzer beschränkt werden (siehe NET.3.3 *VPN*).

Derartige VPN-Gateways SOLLTEN in einer externen DMZ platziert werden. Es SOLLTE beachtet werden, dass hinreichend gehärtete VPN-Gateways direkt aus dem Internet erreichbar sein können. Die über das VPN-Gateway authentisierten Zugriffe ins interne Netz MÜSSEN mindestens die interne Firewall durchlaufen.

IT-Systeme DÜRFEN NICHT via Internet oder externer DMZ auf das interne Netz zugreifen. Es SOLLTE beachtet werden, dass etwaige Ausnahmen zu dieser Anforderung in den entsprechenden anwendungs- und systemspezifischen Bausteinen geregelt werden.

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

Ausgehende Kommunikation aus dem internen Netz zum Internet MUSS an einem Sicherheits-Proxy entkoppelt werden. Die Entkoppelung MUSS außerhalb des internen Netzes erfolgen. Wird eine P-A-P-Struktur eingesetzt, SOLLTE die ausgehende Kommunikation immer durch die Sicherheits-Proxies der P-A-P-Struktur entkoppelt werden.

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

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 und, sofern vorhanden, Standortnetz und Extranet,
- Topologie des Gesamtnetzes und der Netzbereiche, d. h. Zonen und Netzsegmente,
- 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 sowie
- Administration und Überwachung (siehe NET.1.2 *Netzmanagement*).

Die Netzplanung MUSS regelmäßig überprüft werden.

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

Das geplante Netz MUSS fachgerecht umgesetzt werden. Dies MUSS während der Abnahme geprüft werden.

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

Es MUSS regelmäßig geprüft werden, ob das bestehende Netz dem Soll-Zustand entspricht. Dabei MUSS mindestens geprüft werden, inwieweit es die Sicherheitsrichtlinie und Anforderungsspezifikation erfüllt. Es MUSS auch geprüft werden, inwiefern die umgesetzte Netzstruktur dem aktuellen Stand der Netzplanung entspricht. Dafür MÜSSEN zuständige Personen sowie Prüfkriterien bzw. Vorgaben festgelegt werden.

## 3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein NET.1.1 *Netzarchitektur und -design*. Sie SOLLTEN grundsätzlich erfüllt werden.

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

Auf Basis der Sicherheitsrichtlinie und der Anforderungsspezifikation SOLLTE eine Architektur für die Zonen inklusive internem Netz, DMZ-Bereich und Außenanbindungen entwickelt und nachhaltig gepflegt werden. Dabei SOLLTEN je nach spezifischer Situation der Institution alle relevanten Architekturelemente 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, sowie DMZ- und Extranet-Design 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 Private Cloud sowie Absicherung der Anbindungen zu Virtual Private Clouds, Hybrid Clouds und Public Clouds sowie
- Architektur zur sicheren Administration und Überwachung der IT-Infrastruktur.

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

Basierend auf der Netzarchitektur SOLLTE das Netzdesign für die Zonen inklusive internem Netz, DMZ-Bereich und Außenanbindungen entwickelt und nachhaltig gepflegt werden. Dafür SOLLTEN die relevanten Architekturelemente detailliert betrachtet 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 von Private Clouds sowie sichere Anbindung von Virtual Private Clouds, Hybrid Clouds und Public Clouds sowie
- Festlegungen zum Netzdesign für die sichere Administration und Überwachung der IT-Infrastruktur.

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

Das Netz der Institution SOLLTE über eine Firewall mit P-A-P-Struktur an das Internet angeschlossen werden (siehe NET.1.1.A4 *Netztrennung in Zonen*).

Zwischen den beiden Firewall-Stufen MUSS ein proxy-basiertes Application-Layer-Gateway (ALG) realisiert werden. Das ALG MUSS über ein eigenes Transfernetz (dual-homed) sowohl zum äußeren Paketfilter als auch zum internen Paketfilter angebunden werden. Das Transfernetz DARF NICHT mit anderen Aufgaben als denjenigen für das ALG belegt sein.

Falls kein ALG eingesetzt wird, dann MÜSSEN entsprechende Sicherheits-Proxies realisiert werden. Die Sicherheits-Proxies MÜSSEN über ein eigenes Transfernetz (dual-homed) angebunden werden. Das Transfernetz DARF NICHT mit anderen Aufgaben als denjenigen für die Sicherheits-Proxies belegt sein. Es MUSS geprüft werden, ob über die Sicherheits-Proxies gegenseitige Angriffe möglich sind. Ist dies der Fall, MUSS das Transfernetz geeignet segmentiert werden.

Jeglicher Datenverkehr MUSS über das ALG oder entsprechende Sicherheits-Proxies entkoppelt werden. Ein Transfernetz, das beide Firewall-Stufen direkt miteinander verbindet, DARF NICHT konfiguriert werden. Die interne Firewall MUSS zudem die Angriffsfläche des ALGs oder der Sicherheits-Proxies gegenüber Innentätern oder IT-Systemen im internen Netz reduzieren.

Authentisierte und vertrauenswürdige Netzzugriffe vom VPN-Gateway ins interne Netz SOLLTEN NICHT das ALG oder die Sicherheits-Proxies der P-A-P-Struktur durchlaufen.

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

Server, die grundlegende Dienste für die IT-Infrastruktur bereitstellen, SOLLTEN in einem dedizierten Netzsegment positioniert werden. Die Kommunikation mit ihnen SOLLTE durch einen zustandsbehafteten Paketfilter (Firewall) kontrolliert werden.

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

Unterschiedliche IPv4-/IPv6- Endgeräte SOLLTEN je nach verwendetem Protokoll (IPv4-/IPv6- oder IPv4/IPv6-DualStack) dedizierten Subnetzen zugeordnet werden.

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

Um die Infrastruktur zu managen, SOLLTE durchgängig ein Out-of-Band-Management genutzt werden. Dabei SOLLTEN alle Endgeräte, die für das Management der IT-Infrastruktur benötigt werden, in dedizierten Netzsegmenten positioniert werden. Die Kommunikation mit diesen Endgeräten SOLLTE durch einen zustandsbehafteten Paketfilter kontrolliert werden. Die Kommunikation von und zu diesen Management-Netzsegmenten SOLLTE auf die notwendigen Management-Protokolle mit definierten Kommunikations-Endpunkten beschränkt werden.

Der Management-Bereich SOLLTE mindestens die folgenden Netzsegmente umfassen. Diese SOLLTEN abhängig von der Sicherheitsrichtlinie und der Anforderungsspezifikation weiter unterteilt werden in

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

Die verschiedenen Management-Interfaces der IT-Systeme MÜSSEN nach ihrem Einsatzzweck und ihrer Netzplatzierung über einen zustandsbehafteten Paketfilter getrennt werden. Dabei SOLLTEN die IT-Systeme (Management-Interfaces) zusätzlich bei folgender Zugehörigkeit über dedizierte Firewalls getrennt werden:

- IT-Systeme, die aus dem Internet erreichbar sind,
- IT-Systeme im internen Netz sowie
- 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. Eine Überbrückung von Netzsegmenten MUSS ausgeschlossen werden.

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

Auf Basis der Spezifikationen von Netzarchitektur und Netzdesign SOLLTE ein umfassendes Segmentierungskonzept für das interne Netz erstellt werden. Dieses Segmentierungskonzept SOLLTE eventuell vorhandene virtualisierte Netze in Virtualisierungs-Hosts beinhalten. Das Segmentierunskonzept SOLLTE geplant, umgesetzt, betrieben und nachhaltig gepflegt werden. Das Konzept SOLLTE mindestens die folgenden Punkte umfassen, soweit diese in der Zielumgebung vorgesehen sind:

- Initial anzulegende Netzsegmente und Vorgaben dazu, wie neue Netzsegmente zu schaffen sind und wie Endgeräte in den Netzsegmenten zu positionieren sind,
- Festlegung für die Segmentierung von Entwicklungs- und Testsystemen (Staging),
- Netzzugangskontrolle für Netzsegmente mit Clients,

- Anbindung von Netzbereichen, die über Funktechniken oder Standleitung an die Netzsegmente angebunden sind,
- Anbindung der Virtualisierungs-Hosts und von virtuellen Maschinen auf den Hosts an die Netzsegmente,
- Rechenzentrumsautomatisierung sowie
- Festlegungen dazu, wie Endgeräte einzubinden sind, die mehrere Netzsegmente versorgen, z. B. Load Balancer, und Speicher- sowie Datensicherungslösungen.

Abhängig von der Sicherheitsrichtlinie und der Anforderungsspezifikation SOLLTE für jedes Netzsegment konzipiert werden, wie es netztechnisch realisiert werden soll. Darüber hinaus SOLLTE festgelegt werden, welche Sicherheitsfunktionen die Koppelelemente zwischen den Netzsegmenten bereitstellen müssen (z. B. Firewall als zustandsbehafteter Paketfilter oder IDS/IPS).

### NET.1.1.A23 Trennung von Netzsegmenten (S)

IT-Systeme mit unterschiedlichem Schutzbedarf SOLLTEN in verschiedenen Netzsegmenten platziert werden. Ist dies nicht möglich, SOLLTE sich der Schutzbedarf nach dem höchsten vorkommenden Schutzbedarf im Netzsegment richten. Darüber hinaus SOLLTEN die Netzsegmente abhängig von ihrer Größe und den Anforderungen des Segmentierungskonzepts weiter unterteilt werden. Es MUSS sichergestellt werden, dass keine Überbrückung von Netzsegmenten oder gar Zonen möglich ist.

Gehören die virtuellen LANs (VLANs) an einem Switch unterschiedlichen Institutionen an, SOLLTE die Trennung physisch erfolgen. Alternativ SOLLTEN Daten verschlüsselt werden, um die übertragenen Informationen vor unbefugtem Zugriff zu schützen.

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

Falls VLANs eingesetzt werden, dann DARF dadurch KEINE Verbindung geschaffen werden zwischen dem internen Netz und einer Zone vor dem ALG oder den Sicherheits-Proxies.

Generell MUSS sichergestellt werden, dass VLANs nicht überwunden werden können.

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

Eine Fein- und Umsetzungsplanung für die Netzarchitektur und das Netzdesign SOLLTE durchgeführt, dokumentiert, geprüft und nachhaltig gepflegt werden.

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

Betriebsprozesse SOLLTEN bedarfsgerecht erzeugt oder angepasst und dokumentiert werden. Dabei SOLLTE insbesondere berücksichtigt werden, wie sich die Zonierung sowie das Segmentierungskonzept auf den IT-Betrieb auswirken.

### NET.1.1.A27 Einbindung der Netzarchitektur in die Notfallplanung [IT-Betrieb] (S)

Es SOLLTE initial und in regelmäßigen Abständen nachvollziehbar analysiert werden, wie sich die Netzarchitektur und die abgeleiteten Konzepte auf die Notfallplanung auswirken.

## 3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein NET.1.1 *Netzarchitektur und -design* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

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

Zentrale Bereiche des internen Netzes sowie die Sicherheitskomponenten SOLLTEN hochverfügbar ausgelegt sein. Dazu SOLLTEN die Komponenten redundant ausgelegt und auch intern hochverfügbar realisiert werden.

### NET.1.1.A29 Hochverfügbare Realisierung von Netzanbindungen (H)

Die Netzanbindungen, wie z. B. Internet-Anbindung und WAN-Verbindungen, SOLLTEN vollständig redundant 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 innerhalb und außerhalb der eigenen Zuständigkeit bedarfsgerecht umgesetzt werden. Dabei SOLLTEN mögliche Single Points of Failures (SPoF) und störende Umgebungsbedingungen berücksichtigt werden.

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

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 werden. Deren Nutzung SOLLTE in Verträgen geregelt werden.

### NET.1.1.A31 Physische Trennung von Netzsegmenten (H)

Abhängig von Sicherheitsrichtlinie und Anforderungsspezifikation SOLLTEN Netzsegmente physisch durch separate Switches getrennt werden.

### NET.1.1.A32 Physische Trennung von Management-Netzsegmenten (H)

Abhängig von Sicherheitsrichtlinie und Anforderungsspezifikation SOLLTEN Netzsegmente des Management-Bereichs physisch voneinander getrennt werden.

### NET.1.1.A33 Mikrosegmentierung des Netzes (H)

Das Netz SOLLTE in kleine Netzsegmente mit sehr ähnlichem Anforderungsprofil und selbem Schutzbedarf unterteilt werden. Insbesondere SOLLTE dies für die DMZ-Segmente berücksichtigt werden.

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

Die Netzsegmente SOLLTEN im internen Netz, im Extranet und im DMZ-Bereich mittels kryptografischer Techniken bereits auf Netzebene realisiert werden. Dafür SOLLTEN VPN-Techniken oder IEEE 802.1AE eingesetzt werden.

Wenn innerhalb von internem Netz, Extranet oder DMZ über Verbindungsstrecken kommuniziert wird, die für einen erhöhten Schutzbedarf nicht ausreichend sicher sind, SOLLTE die Kommunikation angemessen auf Netzebene verschlüsselt werden.

### NET.1.1.A35 Einsatz von netzbasiertem DLP (H)

Auf Netzebene SOLLTEN Systeme zur Data Lost Prevention (DLP) eingesetzt werden.

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

Bei sehr hohem Schutzbedarf SOLLTEN KEINE VLANs eingesetzt werden.

# 4. Weiterführende Informationen

## 4.1. Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld Netze veröffentlicht:

- Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)
- Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf: BSI-TL-02103 - Version 2.0

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27033 „Information technology – Security techniques — Network security — Part 1: Overview and concepts bis Part 3: Reference networking scenarios – Threats, design techniques and control issues“ Vorgaben für die Absicherung von Netzen.

# 5. Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein NET.1.1 *Netzarchitektur und -design* von Bedeutung.

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.46 Integritätsverlust schützenswerter Informationen