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, das Extranet 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 der Kundschaft, geeignet angebunden werden.

Um ein hohes Sicherheitsniveau zu gewährleisten, sind zusätzliche sicherheitsrelevante Aspekte zu berücksichtigen. Beispiele hierfür sind eine sichere Trennung verschiedener Mandanten und Mandantinnen sowie 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 zugrundeliegende 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

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen 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 stillstehen.

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 Angreifende 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. Angreifende können so leichter Sicherheitslücken finden, ins interne Netz der Institution eindringen und dort Informationen stehlen, Daten manipulieren oder auch ganze Produktionssysteme stören. Auch bleiben Angreifende in einem fehlerhaft aufgebauten Netz, das die Sicherheitssysteme nur eingeschränkt überwachen können, länger unerkannt.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.1.1 *Netzarchitektur und -design* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Planende
Weitere Zuständigkeiten	IT-Betrieb

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

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

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 Benutzendengruppen bzw. Mandanten und Mandantinnen 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 Mitarbeitenden 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 oder der 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 (B) [IT-Betrieb]

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 (Allowlist).

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 Benutzende 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 diesen Baustein. 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 und Innentäterinnen 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 (S) [IT-Betrieb]

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 diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen 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 Dienstleistende 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 -partnerinnen sowie 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.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.1.2 Netzmanagement

1. Beschreibung

1.1. Einleitung

Ein zuverlässiges Netzmanagement 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.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil des Netzmanagements zu etablieren.

1.3. Abgrenzung und Modellierung

Der Baustein NET.1.2 *Netzmanagement* ist auf jedes Netzmanagement-System (Management-System und zu verwaltende IT-System) anzuwenden, das im Informationsverbund eingesetzt wird. Bei den zu verwaltenden IT-Systemen handelt es sich üblicherweise um einzelne Clients, Server oder aktive Netzkomponenten (Netzkoppelelemente).

Dieser Baustein betrachtet die notwendigen Komponenten und konzeptionellen Aufgaben zum Netzmanagement. Anforderungen zum Systemmanagement für vernetzte Clients und Server werden hier nicht beschrieben.

Der vorliegende Baustein beschreibt, wie das Netzmanagement aufgebaut und abgesichert sowie die zugehörige Kommunikation geschützt werden können. Details bezüglich der Absicherung von Netzkomponenten, insbesondere deren Management-Schnittstellen, werden in den Bausteinen der Schichten NET.2 *Funknetze* und NET.3 *Netzkomponenten* behandelt.

Die in diesem Baustein thematisierte Protokollierung sollte in ein übergreifendes Protokollierungs- und Archivierungskonzept eingebunden sein (siehe OPS.1.1.5 *Protokollierung* und OPS.1.2.2 *Archivierung*).

Die Daten des Netzmanagements müssen im Datensicherungskonzept berücksichtigt werden. Anforderungen dazu sind im Baustein CON.3 *Datensicherungskonzept* enthalten.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.1.2 *Netzmanagement* von besonderer Bedeutung.

2.1. Unberechtigter Zugriff auf zentrale Netzmanagement-Komponenten

Wenn es bei einem Angriff gelingt, auf Netzmanagement-Lösungen zuzugreifen, z. B. durch ungepatchte Sicherheitslücken oder eine ungenügende Netztrennung, können alle dort angeschlossenen Netzkomponenten kontrolliert und neu konfiguriert werden. So kann z. B. auf schützenswerte Informationen zugegriffen, der Netzverkehr umgeleitet oder auch das gesamte Netz nachhaltig gestört werden.

2.2. Unberechtigter Zugriff auf einzelne Netzkomponenten

Wenn es bei einem Angriff gelingt, auf einzelne Netzkomponenten zuzugreifen, kann die jeweilige Komponente kontrolliert und manipuliert werden. Jeder über die Netzkomponente geleitete Datenverkehr kann somit kompromittiert werden. Darüber hinaus können weiterführende Angriffe vorbereitet werden, um tiefer in das Netz der Institution einzudringen.

2.3. Unberechtigte Eingriffe in die Netzmanagement-Kommunikation

Wird die Netzmanagement-Kommunikation abgehört und manipuliert, können auf diesem Weg aktive Netzkomponenten fehlkonfiguriert bzw. kontrolliert werden. Dadurch kann die Netzintegrität verletzt und die Verfügbarkeit der Netzinfrastruktur eingeschränkt werden. Außerdem können die übertragenen Daten mitgeschnitten und eingesehen werden.

2.4. Unzureichende Zeitsynchronisation der Netzmanagement-Komponenten

Wird die Systemzeit der Netzmanagement-Komponenten unzureichend synchronisiert, können die Protokollierungsdaten eventuell nicht miteinander korreliert werden. Auch kann die Korrelation eventuell zu fehlerhaften Aussagen führen, da die unterschiedlichen Zeitstempel von Ereignissen keine gemeinsame Basis aufweisen. So kann nicht geeignet auf Ereignisse reagiert werden. Probleme können zudem nicht beseitigt werden. Dadurch können beispielsweise Sicherheitsvorfälle und Datenabflüsse unerkannt bleiben.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.1.2 *Netzmanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Planende, Vorgesetzte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.1.2.A1 Planung des Netzmanagements (B)

Die Netzmanagement-Infrastruktur MUSS geeignet geplant werden. Dabei SOLLTEN alle in der Sicherheitsrichtlinie und Anforderungsspezifikation für das Netzmanagement genannten Punkte berücksichtigt werden. Es MÜSSEN mindestens folgende Themen berücksichtigt werden:

- zu trennende Bereiche für das Netzmanagement,
- Zugriffsmöglichkeiten auf die Management-Server,
- Kommunikation für den Managementzugriff,
- eingesetzte 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 sowie
- korrespondierende Anforderungen an die einzubindenden Netzkomponenten.

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

Ausgehend von NET.1.2.A1 *Planung des Netzmanagements* MÜSSEN Anforderungen an die Netzmanagement-Infrastruktur und -Prozesse spezifiziert werden. Dabei MÜSSEN alle wesentlichen Elemente für das Netzmanagement berücksichtigt werden. Auch SOLLTE die Richtlinie für das Netzmanagement beachtet werden.

NET.1.2.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.1.2.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.1.2.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.1.2.A6 Regelmäßige Datensicherung (B)

Bei der Datensicherung des Netzmanagements MÜSSEN mindestens die Systemdaten für die Einbindung der zu verwaltenden Komponenten bzw. Objekte, Ereignismeldungen, Statistikdaten sowie vorgehaltene Daten für das Konfigurationsmanagement gesichert werden.

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

Mindestens folgende Ereignisse MÜSSEN protokolliert werden:

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

NET.1.2.A8 Zeit-Synchronisation (B)

Alle Komponenten des Netzmanagements, inklusive der eingebundenen Netzkomponenten, MÜSSEN eine synchrone Uhrzeit nutzen. Die Uhrzeit SOLLTE an jedem Standort innerhalb des lokalen Netzes mittels NTP-Service synchronisiert werden. Ist ein separates Managementnetz eingerichtet, SOLLTE eine NTP-Instanz in diesem Managementnetz positioniert werden.

NET.1.2.A9 Absicherung der Netzmanagement-Kommunikation und des Zugriffs auf Netz-Management-Werkzeuge (B)

Erfolgt die Netzmanagement-Kommunikation über die produktive Infrastruktur, MÜSSEN dafür sichere Protokolle verwendet werden. Ist dies nicht möglich, MUSS ein eigens dafür vorgesehenes Administrationsnetz (Out-of-Band-Management) verwendet werden (siehe NET.1.1 *Netzarchitektur und -design*).

Falls von einem Netz außerhalb der Managementnetze auf Netzmanagement-Werkzeuge zugegriffen wird, MÜSSEN als sicher geltende Authentisierungs- und Verschlüsselungsmethoden realisiert werden.

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

Grundsätzlich DÜRFEN im Netzmanagement KEINE unsicheren Versionen des Simple Network Management Protocol (SNMP) eingesetzt werden. Werden dennoch unsichere Protokolle verwendet und nicht über andere sichere Netzprotokolle (z. B. VPN oder TLS) abgesichert, MUSS ein separates Managementnetz genutzt werden. Grundsätzlich SOLLTE über SNMP nur mit den minimal erforderlichen Zugriffsrechten zugegriffen werden. Die Zugangsberechtigung SOLLTE auf dedizierte Management-Server eingeschränkt werden.

3.2. Standard-Anforderungen

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

NET.1.2.A11 Festlegung einer Sicherheitsrichtlinie für das Netzmanagement (S)

Für das Netzmanagement SOLLTE eine Sicherheitsrichtlinie erstellt und nachhaltig gepflegt werden. Die Sicherheitsrichtlinie SOLLTE allen Personen, die am Netzmanagement beteiligt sind, bekannt sein. Die Sicherheitsrichtlinie SOLLTE zudem grundlegend für ihre Arbeit sein. Es SOLLTE regelmäßig und nachvollziehbar überprüft werden, dass die in der Sicherheitsrichtlinie geforderten Inhalte umgesetzt werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

Die Sicherheitsrichtlinie SOLLTE festlegen, welche Bereiche des Netzmanagements über zentrale Management-Werkzeuge und -Dienste realisiert werden. Auch SOLLTE sie definieren, inwieweit Aufgaben im Netzmanagement der Institution automatisiert realisiert werden sollen.

Darüber hinaus SOLLTEN Rahmenbedingungen und Vorgaben für die Netztrennung, die Zugriffskontrolle, die Protokollierung sowie für den Schutz der Kommunikation spezifiziert werden. Auch für das eingesetzte Netzmanagement-Werkzeug und für die operativen Grundregeln des Netzmanagements SOLLTEN Rahmenbedingungen und Vorgaben spezifiziert werden.

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

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

Der so dokumentierte Ist-Zustand der Management-Infrastruktur SOLLTE mit der Dokumentation der Netz-Infrastruktur abgeglichen werden (siehe Baustein NET.1.1 *Netz-Architektur- und Design).*

Die Dokumentation SOLLTE vollständig und immer aktuell sein.

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

Ausgehend von der Sicherheitsrichtlinie für das Netzmanagement SOLLTE ein Netzmanagement-Konzept erstellt und nachhaltig gepflegt werden. Dabei SOLLTEN mindestens folgende Aspekte bedarfsgerecht berücksichtigt werden:

- Methoden, Techniken und Werkzeuge für das Netzmanagement,
- Absicherung des Zugangs und der Kommunikation,
- Netztrennung, insbesondere Zuordnung von Netzmanagement-Komponenten zu Zonen,
- 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 sowie
- Einbindung des Netzmanagements in die Notfallplanung.

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

Es SOLLTE eine Fein- und Umsetzungsplanung für die Netzmanagement-Infrastruktur erstellt werden. Dabei SOLLTEN alle in der Sicherheitsrichtlinie und im Netzmanagement-Konzept adressierten Punkte berücksichtigt werden.

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

Ausgehend von der Sicherheitsrichtlinie für das Netzmanagement und dem Netzmanagement-Konzept SOLLTE ein Konzept für den sicheren Betrieb der Netzmanagement-Infrastruktur erstellt werden. Darin SOLLTE der Anwendungs- und Systembetrieb für die Netzmanagement-Werkzeuge berücksichtigt werden. Auch SOLLTE geprüft werden, wie sich die Leistungen anderer operativer Einheiten einbinden und steuern lassen.

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

Lösungen für das Netzmanagement SOLLTEN anhand der Sicherheitsrichtlinie, der spezifizierten Anforderungen (siehe NET1.2.A2 *Anforderungsspezifikation für das Netzmanagement*) und der Fein- und Umsetzungsplanung aufgebaut, sicher konfiguriert und in Betrieb genommen werden. Danach SOLLTEN die spezifischen Prozesse für das Netzmanagement eingerichtet werden.

NET.1.2.A17 Regelmäßiger Soll-Ist-Vergleich im Rahmen des Netzmanagements (S)

Es SOLLTE regelmäßig und nachvollziehbar geprüft werden, inwieweit die Netzmanagement-Lösung dem Sollzustand entspricht. Dabei SOLLTE geprüft werden, ob die bestehende Lösung noch die Sicherheitsrichtlinie und Anforderungsspezifikation erfüllt. Auch SOLLTE geprüft werden, inwieweit die umgesetzte Management-Struktur und die genutzten Prozesse dem aktuellen Stand entsprechen. Weiter SOLLTE verglichen werden, ob die Management-Infrastruktur aktuell ist.

NET.1.2.A18 Schulungen für Management-Lösungen (S) [Vorgesetzte]

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

NET.1.2.A19 ENTFALLEN (S)

Diese Anforderung ist entfallen.

NET.1.2.A20 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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

Direkte Management-Zugriffe von Administrierenden von einem IT-System außerhalb der Managementnetze auf eine Netzkomponente SOLLTEN vermieden werden. Ist ein solcher Zugriff ohne zentrales Management-Werkzeug notwendig, SOLLTE die Kommunikation entkoppelt werden. Solche Sprungserver SOLLTEN im Management-Netz integriert und in einem getrennten Zugangssegment positioniert sein.

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

Es SOLLTEN NUR die benötigten Management-Funktionen aktiviert werden.

NET.1.2.A23 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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

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

NET.1.2.A25 Statusüberwachung der Netzkomponenten (S)

Die grundlegenden Performance- und Verfügbarkeitsparameter der zentralen Netzkomponenten SOLLTEN kontinuierlich überwacht werden. Dafür SOLLTEN vorab die jeweiligen Schwellwerte ermittelt werden (Baselining).

NET.1.2.A26 Alarming und Logging (S)

Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-Werkzeugen SOLLTEN automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden (siehe OPS.1.1.5 *Protokollierung*). Das zuständige Personal SOLLTE zusätzlich automatisch benachrichtigt werden. Das Alarming und Logging SOLLTE mindestens folgende Punkte beinhalten:

- Ausfall bzw. Nichterreichbarkeit von Netz- oder Management-Komponenten,
- Hardware-Fehlfunktionen,
- fehlerhafte Anmeldeversuche sowie
- kritische Zustände oder Überlastung von IT-Systemen.

Ereignismeldungen bzw. Logging-Daten SOLLTEN einem zentralen Management-System entweder kontinuierlich oder gebündelt übermittelt werden. Alarmmeldungen SOLLTEN sofort wenn sie auftreten übermittelt werden.

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

Die Netzmanagement-Lösungen SOLLTEN in die Notfallplanung der Institution eingebunden werden. Dazu SOLLTEN die Netzmanagement-Werkzeuge und die Konfigurationen der Netzkomponenten gesichert und in die Wiederanlaufpläne integriert sein.

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

Für die Administration sowohl der internen als auch der externen IT-Systeme SOLLTEN dedizierte Management-Clients eingesetzt werden. Dafür SOLLTE mindestens ein Management-Client am äußeren Netzbereich (für die Administration am Internet anliegender IT-Systeme) und ein weiterer im internen Bereich (für die Administration interner IT-Systeme) platziert werden.

NET.1.2.A29 Einsatz von VLANs im Management-Netz (S)

Werden Managementnetze durch VLANs getrennt, SOLLTE darauf geachtet werden, dass der äußere Paketfilter sowie die daran angeschlossenen Geräte in einem eigenen Teilnetz stehen. Zudem SOLLTE sichergestellt werden, dass das ALG dabei nicht umgangen wird.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

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

Zentrale Management-Lösungen SOLLTEN hochverfügbar betrieben werden. Dazu SOLLTEN die Server bzw. Werkzeuge inklusive der Netzanbindungen redundant ausgelegt sein. Auch die einzelnen Komponenten SOLLTEN hochverfügbar bereitgestellt werden.

NET.1.2.A31 Grundsätzliche Nutzung von sicheren Protokollen (H)

Für das Netzmanagement SOLLTEN ausschließlich sichere Protokolle benutzt werden. Es SOLLTEN alle Sicherheitsfunktionen dieser Protokolle verwendet werden.

NET.1.2.A32 Physische Trennung des Managementnetzes (H) [Planende]

Das Managementnetz SOLLTE physisch von den produktiven Netzen getrennt werden.

NET.1.2.A33 Physische Trennung von Management-Segmenten (H) [Planende]

Es SOLLTEN physisch getrennte Zonen mindestens für das Management von LAN-Komponenten, Sicherheitskomponenten und Komponenten zur Außenanbindung eingerichtet werden.

NET.1.2.A34 ENTFALLEN (H)

Diese Anforderung ist entfallen.

NET.1.2.A35 Festlegungen zur Beweissicherung (H)

Die erhobenen Protokollierungsdaten SOLLTEN für forensische Analysen gesetzeskonform und revisionssicher archiviert werden (siehe auch DER.2.2 *Vorsorge für die IT-Forensik*).

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

Die Protokollierung des Netzmanagements SOLLTE in eine Security-Information-and-Event-Management (SIEM)-Lösung eingebunden werden. Dazu SOLLTEN die Anforderungskataloge zur Auswahl von Netzmanagement-Lösungen hinsichtlich der erforderlichen Unterstützung von Schnittstellen und Übergabeformaten angepasst werden (siehe NET.1.2.A2 *Anforderungsspezifikation für das Netzmanagement*).

NET.1.2.A37 Standortübergreifende Zeitsynchronisation (H)

Die Zeitsynchronisation SOLLTE über alle Standorte der Institution sichergestellt werden. Dafür SOLLTE eine gemeinsame Referenzzeit benutzt werden.

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

Für eine schnelle Wiederherstellung der Sollzustände von Software bzw. Firmware sowie der Konfiguration der Komponenten in der Netzmanagement-Infrastruktur SOLLTEN hinreichend gute Ersatzlösungen festgelegt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) formuliert 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.

Das BSI hat das weiterführende Dokument „Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)“ zum Themenfeld Netzmanagement veröffentlicht.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.2.1 WLAN-Betrieb

1. Beschreibung

1.1. Einleitung

Über Wireless LANs (WLANs) können drahtlose lokale Netze aufgebaut oder bestehende drahtgebundene Netze erweitert werden. Bis heute basieren fast alle am Markt verfügbaren WLAN-Komponenten auf dem Standard IEEE 802.11 und seinen Ergänzungen. Eine besondere Rolle nimmt dabei das Firmenkonsortium „Wi-Fi Alliance“ ein, das basierend auf dem Standard IEEE 802.11 mit „Wi-Fi“ einen Industriestandard geschaffen hat. Dabei bestätigt die Wi-Fi Alliance mit dem Wi-Fi-Gütesiegel, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat.

Innerhalb von Institutionen können WLANs eingesetzt werden, um flexibel mit mobilen Geräten zu arbeiten und diesen den Zugang zum Netz der Institution zu ermöglichen. Hierfür werden innerhalb der Institution Netzzugänge über so genannten Access Points aufgebaut. Aufgrund der meist einfachen und schnellen Installation werden WLANs auch dazu eingesetzt, um temporär Netze einzurichten, beispielsweise auf Messen oder kleineren Veranstaltungen. Darüber hinaus können an öffentlichen Plätzen, wie Flughäfen oder Bahnhöfen, Netzzugänge über so genannte Hotspots angeboten werden. Dadurch werden den mobilen Benutzenden Verbindungen in das Internet oder ihr Institutionsnetz ermöglicht. Die Kommunikation findet dann generell zwischen einem zentralen Zugangspunkt, dem Access Point, und der WLAN-Komponente des Endgeräts statt.

1.2. Zielsetzung

In diesem Baustein wird systematisch aufgezeigt, wie WLANs sicher in einer Institution aufgebaut und betrieben werden können.

1.3. Abgrenzung und Modellierung

Der Baustein NET.2.1 *WLAN-Betrieb* ist auf alle Kommunikationsnetze anzuwenden, die gemäß der Standard-Reihe IEEE 802.11 und deren Erweiterungen aufgebaut und betrieben werden.

Der Baustein enthält grundsätzliche Anforderungen, die beachtet und erfüllt werden müssen, wenn WLANs in Institutionen aufgebaut und betrieben werden. Anforderungen für eine sichere Nutzung von WLANs sind jedoch nicht Gegenstand dieses Bausteins. Die sichere Nutzung von WLANs wird im Baustein NET.2.2 *WLAN-Nutzung* behandelt.

WLANs können entsprechend den Bedürfnissen der betreibenden Institution und der Hardware-Ausstattung, die zur Verfügung steht, in zwei verschiedenen Modi betrieben werden. Im Ad-hoc-

Modus kommunizieren zwei oder mehr WLAN-Clients direkt miteinander. WLANs im Ad-hoc-Modus können sich selbstständig, also ohne feste Infrastruktur, aufbauen und konfigurieren. Somit können sie eine vollvermaschte parallele Netz-Infrastruktur etablieren. Dadurch ist der Ad-hoc-Modus in einer zu schützenden Umgebung ungeeignet und wird deshalb im Folgenden nicht weiter betrachtet. In den meisten Fällen werden WLANs im Infrastruktur-Modus betrieben, d. h. die Kommunikation der WLAN-Clients und die Verbindung in kabelgebundene LAN-Segmente erfolgt über Access Points.

Werden für die Authentisierung am WLAN entsprechende Dienste (z. B. RADIUS) eingesetzt, so müssen die entsprechenden IT-Systeme, auf denen die Dienste betrieben werden, gesondert abgesichert werden. Hierfür können die Bausteine der Schicht SYS.1, wie zum Beispiel SYS.1.1 *Allgemeiner Server,* herangezogen werden.

Wird ein WLAN betrieben, sollte dieses grundsätzlich mit berücksichtigt werden, wenn die Bausteine NET.1.1 *Netzarchitektur und -design*, NET.1.2 *Netzmanagement* und DER.2.1 *Behandlung von Sicherheitsvorfällen* umgesetzt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.2.1 *WLAN-Betrieb* von besonderer Bedeutung.

2.1. Ausfall oder Störung eines Funknetzes

In Funknetzen werden Informationen mittels elektromagnetischer Funkwellen übertragen. Strahlen andere elektromagnetische Quellen im selben Frequenzspektrum Energie ab, können diese die drahtlose Kommunikation stören und im Extremfall den Betrieb des WLANs verhindern. Dies kann durch andere Funksysteme und Geräte, wie beispielsweise Bluetooth, Mikrowellenherde oder andere WLAN-Netze hervorgerufen werden. Darüber hinaus sind auch Denial-of-Service-Angriffe möglich. Werden beispielsweise bestimmte Steuer- und Managementsignale wiederholt gesendet, kann dies dazu führen, dass das Funknetz nicht mehr verfügbar ist.

2.2. Fehlende oder unzureichende Planung des WLAN-Einsatzes

Fehler in der Planung stellen sich oft als besonders schwerwiegend heraus, weil dadurch leicht flächendeckende Sicherheitslücken geschaffen werden können. Wird der Einsatz von WLANs nicht oder nur unzureichend geplant, kann sich eine Vielzahl von Problemen ergeben, beispielsweise:

- Vertrauliche Daten könnten mitgelesen werden, etwa wenn WLAN-Standards eingesetzt werden, die nicht mehr dem Stand der Technik entsprechen (z. B. WEP zur Verschlüsselung).
- Die Übertragungskapazität könnte unzureichend sein. Dadurch können bandbreitenintensive Anwendungen nicht mit der erforderlichen Dienstgüte genutzt werden.
- Die Abdeckung des WLANs könnte nicht ausreichend sein, sodass an bestimmten Orten kein Netz verfügbar ist.

2.3. Fehlende oder unzureichende Regelungen zum WLAN-Einsatz

Bei einer WLAN-Infrastruktur, die nicht zentral administriert wird, sind die Access Points in der Standard-Einstellung meist ohne oder nur mit unzureichenden Sicherheitsmechanismen vorkonfiguriert. Schließen Mitarbeitende beispielsweise aufgrund fehlender Regelungen einen ungenehmigten bzw. ungesicherten Access Point an ein internes Netz der Institution an, kann dies zu schwerwiegenden Problemen führen. Denn sie untergraben damit praktisch sämtliche innerhalb des

LANs ergriffenen Sicherheitsmaßnahmen, wie z. B. die Firewall zum Schutz gegen unberechtigte externe Zugriffe.

2.4. Ungeeignete Auswahl von Authentisierungsverfahren

Wenn Authentisierungsverfahren und -mechanismen fehlen oder unzureichend sind, können Sicherheitslücken entstehen. Beispielsweise wird im Standard IEEE 802.1X (Port Based Network Access Control) das Extensible Authentication Protocol (EAP) definiert. In einigen der beschriebenen EAP-Methoden sind aber Schwachstellen enthalten. So ist EAP-MD5 etwa anfällig gegenüber Man-in-the-Middle- und Wörterbuchangriffen. Wird EAP-MD5 eingesetzt, können Passwörter erraten werden. Außerdem kann die Kommunikation abgehört werden.

2.5. Fehlerhafte Konfiguration der WLAN-Infrastruktur

Access Points und andere WLAN-Komponenten (z. B. WLAN Controller) bieten eine Vielzahl von Konfigurationseinstellungen, die insbesondere auch Sicherheitsfunktionen betreffen. Werden diese falsch konfiguriert, ist entweder keine Kommunikation über einen Access Point möglich oder die Kommunikation erfolgt ungeschützt bzw. mit einem zu geringen Schutzniveau.

2.6. Unzureichende oder fehlende WLAN-Sicherheitsmechanismen

Im Auslieferungszustand sind WLAN-Komponenten häufig so konfiguriert, dass keine oder nur wenige Sicherheitsmechanismen aktiviert sind. Einige der Mechanismen sind darüber hinaus unzureichend und bieten somit keinen ausreichenden Schutz. Auch heute werden noch diverse WLAN-Komponenten eingesetzt, die lediglich unzureichende Sicherheitsmechanismen wie z. B. WEP unterstützen. Teilweise können diese Geräte nicht einmal auf stärkere Sicherheitsmechanismen aufgerüstet werden. Werden solche Geräte eingesetzt, können Angreifende leicht die gesamte Kommunikation abhören und damit vertrauliche Informationen einsehen.

2.7. Abhören der WLAN-Kommunikation

Da es sich bei Funk um ein Medium handelt, das sich mehrere Benutzende teilen können („Shared Medium“), können die über WLANs übertragenen Daten problemlos mitgehört und aufgezeichnet werden. Wenn die Daten nicht oder nur unzureichend verschlüsselt werden, können die übertragenen Nutzdaten leicht eingesehen werden. Zudem überschreiten Funknetze bzw. die ausgesendeten Funkwellen häufig die Grenzen der selbst genutzten Räumlichkeiten. So werden Daten auch noch in Bereiche ausgestrahlt, die nicht von den Benutzenden oder einer Institution kontrolliert und gesichert werden können.

2.8. Vortäuschung eines gültigen Access Points (Rogue Access Point)

Angreifende können sich als Teil der WLAN-Infrastruktur ausgeben, indem sie einen eigenen Access Point mit einem geeignet gewählten Namen (SSID) in der Nähe eines WLAN-Clients installiert. Dieser vorgetäuschte Access Point wird als „Rogue Access Point“ bezeichnet. Bietet dieser dem WLAN-Client eine stärkere Sendeleistung als der echte Access Point, wird der Client diesen als Basisstation nutzen, falls diese sich nicht gegenseitig authentisieren. Zusätzlich könnte auch der echte Access Point durch einen Denial-of-Service-Angriff ausgeschaltet werden. Die Benutzenden melden sich an einem Netz an, das nur vorgibt, das Zielnetz zu sein. Dadurch ist es Angreifenden möglich, die Kommunikation abzuhören. Auch durch Poisoning- oder Spoofing-Methoden können Angreifende eine falsche Identität vortäuschen bzw. den Netzverkehr zu ihren IT-Systemen umlenken. So können sie die Kommunikation belauschen und kontrollieren. Besonders in öffentlichen Funknetzen (sogenannten Hotspots) ist ein Rogue Access Point ein beliebtes Angriffsmittel.

2.9. Ungeschützter LAN-Zugang am Access Point

Sind Access Points sichtbar und ohne physischen Schutz montiert, können sich Angreifende zwischen die Access Points und die Switch-Infrastruktur schalten, um den gesamten Netzverkehr abzuhören. Selbst wenn die drahtlose Kommunikation mit WPA2 verschlüsselt wird, stellt dies eine Gefährdung dar, weil diese Methoden nur die Luftschnittstelle absichern, die Ethernet-Anbindung aber nicht weiter berücksichtigen.

2.10. Hardware-Schäden

Hardware-Schäden können dazu führen, dass der Funkverkehr gestört wird. Im schlimmsten Fall kann das WLAN sogar komplett ausfallen. Dies betrifft insbesondere WLAN-Geräte, die außerhalb von geschützten Räumen angebracht werden, z. B. um offene Plätze abzudecken. Sie sind zusätzlichen Gefährdungen ausgesetzt, wie beispielsweise vorsätzlichen Beschädigungen durch Angreifende oder umweltbedingten Schäden durch Witterung oder Blitzeinschlag.

2.11. Diebstahl eines Access Points

Werden WLAN Access Points ungesichert in öffentlichen Bereichen installiert, können sie gestohlen werden. Dadurch lässt sich beispielsweise ein Shared-Secret Key für die Authentisierung am RADIUS-Server oder der verwendete Schlüssel (beispielsweise für WPA2-Personal) auslesen. Mit diesen Informationen kann dann unberechtigt auf das WLAN zugegriffen werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.2.1 *WLAN-Betrieb* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Planende, Haustechnik

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.2.1.A1 Festlegung einer Strategie für den Einsatz von WLANs (B)

Bevor in einer Institution WLANs eingesetzt werden, MUSS festgelegt sein, welche generelle Strategie die Institution im Hinblick auf die Kommunikation über WLANs plant. Insbesondere MUSS geklärt und festgelegt werden, in welchen Organisationseinheiten, für welche Anwendungen und zu welchem Zweck WLANs eingesetzt und welche Informationen darüber übertragen werden dürfen. Ebenso MUSS der Abdeckungsbereich des WLAN festgelegt werden.

Außerdem MUSS schon in der Planungsphase festgelegt sein, wer für die Administration der unterschiedlichen WLAN-Komponenten zuständig ist, welche Schnittstellen es zwischen den am Betrieb beteiligten Verantwortlichen gibt und wann welche Informationen zwischen den Zuständigen ausgetauscht werden müssen.

NET.2.1.A2 Auswahl eines geeigneten WLAN-Standards (B) [Planende]

Im Rahmen der WLAN-Planung MUSS zuerst ermittelt werden, welche der von der Institution betriebenen Geräte (z. B. Mikrowellengeräte, Bluetooth-Geräte) in das ISM-Band bei 2,4 GHz sowie in das 5 GHz-Band abstrahlen.

Außerdem MÜSSEN die vorhandenen Sicherheitsmechanismen der einzelnen WLAN-Standards gegeneinander abgewogen werden. Generell MUSS sichergestellt sein, dass nur als allgemein sicher anerkannte Verfahren zur Authentisierung und Verschlüsselung eingesetzt werden. Die Entscheidungsgründe MÜSSEN dokumentiert werden.

Geräte, die von anerkannt sicheren Verfahren auf unsichere zurückgreifen müssen, DÜRFEN NICHT mehr eingesetzt werden.

NET.2.1.A3 Auswahl geeigneter Kryptoverfahren für WLAN (B) [Planende]

Die Kommunikation über die Luftschnittstelle MUSS komplett kryptografisch abgesichert werden. Kryptografische Verfahren, die unsicherer als WPA2 sind, DÜRFEN NICHT mehr eingesetzt werden.

Wird WPA2 mit Pre-Shared Keys (WPA2-PSK) verwendet, dann MUSS ein komplexer Schlüssel mit einer Mindestlänge von 20 Zeichen verwendet werden.

NET.2.1.A4 Geeignete Aufstellung von Access Points (B) [Haustechnik]

Access Points MÜSSEN zugriffs- und diebstahlsicher montiert werden. Wenn sie aufgestellt werden, MÜSSEN die erforderlichen Bereiche ausreichend abgedeckt werden. Darüber hinaus MUSS darauf geachtet werden, dass sich die Funkwellen in Bereichen, die nicht durch das WLAN versorgt werden sollen, möglichst nicht ausbreiten. Außeninstallationen MÜSSEN vor Witterungseinflüssen und elektrischen Entladungen geeignet geschützt werden.

NET.2.1.A5 Sichere Basis-Konfiguration der Access Points (B)

Access Points DÜRFEN NICHT in der Konfiguration des Auslieferungszustandes verwendet werden. Voreingestellte SSIDs (Service Set Identifiers), Zugangskennwörter oder kryptografische Schlüssel MÜSSEN vor dem produktiven Einsatz geändert werden. Außerdem MÜSSEN unsichere Administrationszugänge abgeschaltet werden. Access Points DÜRFEN NUR über eine geeignet verschlüsselte Verbindung administriert werden.

NET.2.1.A6 Sichere Konfiguration der WLAN-Infrastruktur (B)

Es MUSS sichergestellt sein, dass mittels der WLAN-Kommunikation keine Sicherheitszonen gekoppelt werden und hierdurch etablierte Schutzmaßnahmen umgangen werden.

NET.2.1.A7 Aufbau eines Distribution Systems (B) [Planende]

Bevor ein kabelgebundenes Distribution System aufgebaut wird, MUSS prinzipiell entschieden werden, ob physisch oder logisch durch VLANs auf den Access Switches des kabelbasierten LANs getrennt wird.

NET.2.1.A8 Verhaltensregeln bei WLAN-Sicherheitsvorfällen (B)

Bei einem Sicherheitsvorfall MUSS der IT-Betrieb passende Gegenmaßnahmen einleiten:

- Am Übergabepunkt der WLAN-Kommunikation ins interne LAN SOLLTE bei einem Angriff auf das WLAN die Kommunikation selektiv pro SSID, Access Point oder sogar für die komplette WLAN-Infrastruktur gesperrt werden.

- Wurden Access Points gestohlen, MÜSSEN festgelegte Sicherheitsmaßnahmen umgesetzt werden, damit der Access Point oder hierauf abgespeicherte Informationen nicht missbraucht werden können.
- Wurden WLAN-Clients entwendet und wird eine zertifikatsbasierte Authentisierung verwendet, MÜSSEN die Client-Zertifikate gesperrt werden.

Es MUSS ausgeschlossen werden, dass entwendete Geräte unberechtigt verwendet werden, um auf das Netz der Institution zuzugreifen.

3.2. Standard-Anforderungen

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

NET.2.1.A9 Sichere Anbindung von WLANs an ein LAN (S) [Planende]

Werden WLANs an ein LAN angebunden, SOLLTE der Übergang zwischen WLANs und LAN abgesichert werden, beispielsweise durch einen Paketfilter. Der Access Point SOLLTE unter Berücksichtigung der Anforderung NET.2.1.A7 *Aufbau eines Distribution Systems* eingebunden sein.

NET.2.1.A10 Erstellung einer Sicherheitsrichtlinie für den Betrieb von WLANs (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die wesentlichen Kernaspekte für einen sicheren Einsatz von WLANs konkretisiert werden. Die Richtlinie SOLLTE allen Verantwortlichen bekannt sein, die an Aufbau und Betrieb von WLANs beteiligt sind. Sie SOLLTE zudem Grundlage für ihre Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Werden die Inhalte der Richtlinie nicht umgesetzt, MUSS geeignet reagiert werden. Die Ergebnisse SOLLTEN geeignet dokumentiert werden.

NET.2.1.A11 Geeignete Auswahl von WLAN-Komponenten (S)

Anhand der Ergebnisse der Planungsphase SOLLTE eine Anforderungsliste erstellt werden, mithilfe derer die am Markt erhältlichen Produkte bewertet werden können. Werden WLAN-Komponenten beschafft, SOLLTE neben Sicherheit auch auf Datenschutz und Kompatibilität der WLAN-Komponenten untereinander geachtet werden.

NET.2.1.A12 Einsatz einer geeigneten WLAN-Management-Lösung (S)

Eine zentrale Managementlösung SOLLTE eingesetzt werden. Der Leistungsumfang der eingesetzten Lösung SOLLTE im Einklang mit den Anforderungen der WLAN-Strategie sein.

NET.2.1.A13 Regelmäßige Sicherheitschecks in WLANs (S)

WLANs SOLLTEN regelmäßig daraufhin überprüft werden, ob eventuell Sicherheitslücken existieren. Zusätzlich SOLLTE regelmäßig nach unbefugt installierten Access Points innerhalb der bereitgestellten WLANs gesucht werden. Weiterhin SOLLTEN die Performance und Abdeckung gemessen werden. Die Ergebnisse von Sicherheitschecks SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTEN untersucht werden.

NET.2.1.A14 Regelmäßige Audits der WLAN-Komponenten (S)

Bei allen Komponenten der WLAN-Infrastruktur SOLLTE regelmäßig überprüft werden, ob alle festgelegten Sicherheitsmaßnahmen umgesetzt sind. Außerdem SOLLTE überprüft werden ob alle Komponenten korrekt konfiguriert sind. Öffentlich aufgestellte Access Points SOLLTEN regelmäßig stichprobenartig daraufhin geprüft werden, ob es gewaltsame Öffnungs- oder Manipulationsversuche gab. Die Auditergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTEN untersucht werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.2.1.A15 Verwendung eines VPN zur Absicherung von WLANs (H)

Es SOLLTE ein VPN eingesetzt werden, um die Kommunikation über die WLAN-Infrastruktur zusätzlich abzusichern.

NET.2.1.A16 Zusätzliche Absicherung bei der Anbindung von WLANs an ein LAN (H)

Wird eine WLAN-Infrastruktur an ein LAN angebunden, SOLLTE der Übergang zwischen WLANs und LAN entsprechend des höheren Schutzbedarfs zusätzlich abgesichert werden.

NET.2.1.A17 Absicherung der Kommunikation zwischen Access Points (H)

Die Kommunikation zwischen den Access Points über die Funkschnittstelle und das LAN SOLLTE verschlüsselt erfolgen.

NET.2.1.A18 Einsatz von Wireless Intrusion Detection/Wireless Intrusion Prevention Systemen (H)

Es SOLLTEN Wireless Intrusion Detection Systeme bzw. Wireless Intrusion Prevention Systeme eingesetzt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld WLAN veröffentlicht:

- BSI-Standard zur Internet-Sicherheit (ISi-Reihe): Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

Das National Institute of Standards and Technology (NIST) hat folgende weiterführende Dokumente zum Themenfeld WLAN veröffentlicht:

- NIST Special Publication 800-153 „Guidelines for Securing Wireless Local Area Network (WLANs)“
- NIST Special Publication 800-97 „Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11“

Bundesamt
für Sicherheit in der
Informationstechnik

NET.2.2 WLAN-Nutzung

1. Beschreibung

1.1. Einleitung

Über Wireless LANs (WLANs) können drahtlose lokale Netze aufgebaut oder bestehende drahtgebundene Netze erweitert werden. Bis heute basieren fast alle am Markt verfügbaren WLAN-Komponenten auf dem Standard IEEE 802.11 und seinen Ergänzungen. Eine besondere Rolle nimmt dabei das Firmenkonsortium „Wi-Fi Alliance“ ein, das basierend auf dem Standard IEEE 802.11 mit „Wi-Fi“ einen Industriestandard geschaffen hat. Dabei bestätigt die Wi-Fi Alliance mit dem Wi-Fi-Gütesiegel, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat.

WLANs bieten einen Gewinn an Komfort und Mobilität. Jedoch birgt die Nutzung auch zusätzliches Gefährdungspotenzial für die Sicherheit der Informationen, da drahtlos kommuniziert wird. Daher ist es wichtig, dass neben dem IT-Betrieb auch die Benutzenden für die möglichen Gefahren sensibilisiert werden, die entstehen können, wenn WLANs unsachgemäß verwendet werden. So müssen die Benutzenden über die erforderlichen Kenntnisse verfügen, um Sicherheitsmaßnahmen richtig verstehen und anwenden zu können. Insbesondere müssen sie wissen, was von ihnen in Hinblick auf Informationssicherheit erwartet wird und wie sie in bestimmten Situationen reagieren sollten, wenn sie WLANs nutzen.

1.2. Zielsetzung

In diesem Baustein soll aufgezeigt werden, wie WLANs sicher genutzt werden können.

1.3. Abgrenzung und Modellierung

Der Baustein NET.2.2 *WLAN-Nutzung* ist auf alle IT-Systeme (WLAN-Clients) anzuwenden, die WLANs nutzen.

Der Baustein enthält grundsätzliche Anforderungen, die bei der Nutzung von WLANs zu beachten und zu erfüllen sind, um den spezifischen Gefährdungen entgegenwirken zu können. Anforderungen, mit deren Hilfe WLANs sicher betrieben werden können, sind dagegen nicht Gegenstand dieses Bausteins, sondern sind im Baustein NET.2.1 *WLAN-Betrieb* beschrieben. Darüber hinaus geht der Baustein nicht auf allgemeine Aspekte von Clients ein. Solche Aspekte werden im Baustein SYS2.1 *Allgemeiner Client* sowie in den betriebssystemspezifischen Bausteinen der Schicht SYS *IT-Systeme* behandelt. Der Baustein NET.2.2 *WLAN-Nutzung* sollte grundsätzlich mit berücksichtigt werden, wenn die Bausteine ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* und DER.2.1 *Behandlung von Sicherheitsvorfällen* umgesetzt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.2.2 *WLAN-Nutzung* von besonderer Bedeutung.

2.1. Unzureichende Kenntnis über Regelungen

Kennen die Benutzenden die Regelungen für den korrekten Umgang mit WLANs nicht oder nicht gut genug, können sie sich auch nicht daran halten. Werden Clients zum Beispiel gedankenlos mit fremden drahtlosen Netzen verbunden, können darüber unverschlüsselt übertragenen Informationen abgehört werden. Außerdem können durch den Betreibenden des drahtlosen Netzes Informationen über die Benutzenden wie zum Beispiel besuchte Webseiten, gesammelt werden.

2.2. Nichtbeachtung von Sicherheitsmaßnahmen

Durch Nachlässigkeit und fehlende Kontrollen kommt es immer wieder vor, dass Personen die ihnen empfohlenen oder angeordneten Sicherheitsmaßnahmen nicht oder nur teilweise umsetzen. Wird beispielsweise ein WLAN-Client im Ad-hoc-Modus genutzt, obwohl dies in der Nutzungsrichtlinie ausdrücklich verboten ist, kann ein anderer Client direkt mit dem WLAN-Client kommunizieren. So kann er z. B. unberechtigt auf vertrauliche Dokumente zugreifen, die eventuell auf dem Client freigegeben sind.

2.3. Abhören der WLAN-Kommunikation

Da es sich bei Funk um ein Medium handelt, das sich mehrere Benutzende teilen können („Shared Medium“), können die über WLANs übertragenen Daten problemlos mitgehört und aufgezeichnet werden. Werden die Daten nicht oder nur unzureichend verschlüsselt, können die übertragenen Nutzdaten leicht mitgelesen werden. Zudem überschreiten Funknetze bzw. die ausgesendeten Funkwellen nicht selten die Grenzen der genutzten Räumlichkeiten. So werden Daten auch noch in Bereiche ausgestrahlt, die nicht von den Benutzenden oder der Institution kontrolliert und gesichert werden können.

2.4. Auswertung von Verbindungsdaten bei der drahtlosen Kommunikation

Bei WLANs auf Basis von IEEE 802.11 wird die MAC-Adresse einer WLAN-Karte bei jeder Datenübertragung mit versendet. Da sie unverschlüsselt übertragen wird, können Bewegungsprofile über mobile Benutzende erstellt werden, z. B. wenn diese sich in öffentliche Hotspots einbuchen.

2.5. Vortäuschung eines gültigen Access Points (Rogue Access Point)

Angreifende können sich als Teil der WLAN-Infrastruktur ausgeben, indem sie einen eigenen Access Point mit einem geeignet gewählten WLAN-Namen (SSID) in der Nähe eines WLAN-Clients installieren. Dieser vorgetäuschte Access Point wird als „Rogue Access Point“ bezeichnet. Bietet dieser dem WLAN-Client eine stärkere Sendeleistung als der echte Access Point, wird der Client diesen als Basisstation nutzen, falls diese sich nicht gegenseitig authentisieren. Zusätzlich könnte auch der echte Access Point durch einen Denial-of-Service-Angriff ausgeschaltet werden. Die Benutzenden melden sich an einem Netz an, das nur vorgibt, das Zielnetz zu sein. Dadurch ist es den Angreifenden möglich, die Kommunikation abzuhören. Auch durch Poisoning- oder Spoofing-Methoden können Angreifende eine falsche Identität vortäuschen bzw. den Netzverkehr zu ihren IT-Systemen umlenken. So können

sie die Kommunikation belauschen und kontrollieren. Besonders in öffentlichen Funknetzen (sogenannten Hotspots) ist ein Rogue Access Point ein beliebtes Angriffsmittel.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.2.2 *WLAN-Nutzung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Benutzende
Weitere Zuständigkeiten	IT-Betrieb, Vorgesetzte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.2.2.A1 Erstellung einer Nutzungsrichtlinie für WLAN (B) [IT-Betrieb]

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MÜSSEN die wesentlichen Kernaspekte für eine sichere WLAN-Nutzung in einer WLAN-Nutzungsrichtlinie konkretisiert werden. In einer solchen Nutzungsrichtlinie MÜSSEN die Besonderheiten bei der WLAN-Nutzung beschrieben sein, z. B. ob, wie und mit welchen Geräten Hotspots genutzt werden dürfen.

Die Richtlinie MUSS Angaben dazu enthalten, welche Daten im WLAN genutzt und übertragen werden dürfen und welche nicht.

Es MUSS beschrieben sein, wie mit clientseitigen Sicherheitslösungen umzugehen ist. Die Nutzungsrichtlinie MUSS ein klares Verbot enthalten, ungenehmigte Access Points an das Netz der Institution anzuschließen. Außerdem MUSS in der Richtlinie darauf hingewiesen werden, dass die WLAN-Schnittstelle deaktiviert werden muss, wenn sie über einen längeren Zeitraum nicht genutzt wird.

Es MUSS regelmäßig überprüft werden, ob die in der Richtlinie geforderten Inhalte richtig umgesetzt werden. Ist dies nicht der Fall, MUSS geeignet reagiert werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

NET.2.2.A2 Sensibilisierung und Schulung der WLAN-Benutzenden (B) [Vorgesetzte, IT-Betrieb]

Die Benutzenden von WLAN-Komponenten, vornehmlich von WLAN-Clients, MÜSSEN sensibilisiert und zu den in der Nutzungsrichtlinie aufgeführten Maßnahmen geschult werden. Hierfür MÜSSEN geeignete Schulungsinhalte identifiziert und festgelegt werden. Den Benutzenden MUSS genau erläutert werden, was die WLAN-spezifischen Sicherheitseinstellungen bedeuten und warum sie wichtig sind. Außerdem MÜSSEN die Benutzenden auf die Gefahren hingewiesen werden, die drohen, wenn diese Sicherheitseinstellungen umgangen oder deaktiviert werden.

Die Schulungsinhalte MÜSSEN immer entsprechend den jeweiligen Einsatzszenarien angepasst werden. Neben der reinen Schulung zu WLAN-Sicherheitsmechanismen MÜSSEN den Benutzenden

jedoch auch die WLAN-Sicherheitsrichtlinie ihrer Institution und die darin enthaltenen Maßnahmen vorgestellt werden. Ebenso MÜSSEN die Benutzenden für die möglichen Gefahren sensibilisiert werden, die von fremden WLANs ausgehen.

NET.2.2.A3 Absicherung der WLAN-Nutzung an Hotspots (B) [IT-Betrieb]

Dürfen Hotspots genutzt werden, MUSS Folgendes umgesetzt werden:

- Jede(r) Benutzende eines Hotspots MUSS seine oder ihre Sicherheitsanforderungen kennen und danach entscheiden, ob und unter welchen Bedingungen ihm oder ihr die Nutzung des Hotspots erlaubt ist.
- Werden Hotspots genutzt, dann SOLLTE sichergestellt werden, dass die Verbindung zwischen Hotspot-Access Point und IT-Systemen der Benutzenden nach dem Stand der Technik kryptografisch abgesichert wird.
- WLANs, die nur sporadisch genutzt werden, SOLLTEN von den Benutzenden aus der Historie gelöscht werden.
- Die automatische Anmeldung an WLANs SOLLTE deaktiviert werden.
- Wenn möglich, SOLLTEN separate Konten mit einer sicheren Grundkonfiguration und restriktiven Berechtigungen verwendet werden.
- Es SOLLTE sichergestellt sein, dass sich keine Benutzenden mit administrativen Berechtigungen von ihren Clients aus an externen WLANs anmelden können.
- Sensible Daten DÜRFEN NUR übertragen werden, wenn allen notwendigen Sicherheitsmaßnahmen auf den Clients, vor allem eine geeignete Verschlüsselung, aktiviert sind.
- Wird die WLAN-Schnittstelle über einen längeren Zeitraum nicht genutzt, MUSS diese deaktiviert werden.
- Über öffentlich zugängliche WLANs DÜRFEN die Benutzenden NUR über ein Virtual Private Network (VPN) auf interne Ressourcen der Institution zugreifen.

3.2. Standard-Anforderungen

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

NET.2.2.A4 Verhaltensregeln bei WLAN-Sicherheitsvorfällen (S)

Bei WLAN-Sicherheitsvorfällen SOLLTEN die Benutzenden Folgendes umsetzen:

- Sie SOLLTEN ihre Arbeitsergebnisse sichern.
- Sie SOLLTEN den WLAN-Zugriff beenden und die WLAN-Schnittstelle ihres Clients deaktivieren.
- Fehlermeldungen und Abweichungen SOLLTEN durch sie genau dokumentiert werden. Ebenso SOLLTEN sie dokumentieren, was sie gemacht haben, bevor bzw. während der Sicherheitsvorfall eingetreten ist.
- Sie SOLLTEN über eine geeignete Eskalationsstufe (z. B. User Help Desk) den IT-Betrieb benachrichtigen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld WLAN veröffentlicht:

- BSI-Standard zur Internet-Sicherheit (ISi-Reihe): Sichere Anbindung von lokalen Netzen an das Internet (Isi-LANA)
- Das National Institute of Standards and Technology (NIST) hat folgende weiterführende Dokumente zum Themenfeld WLAN veröffentlicht:
    - NIST Special Publication 800-153 „Guidelines for Securing Wireless Local Area Network (WLANs)“
    - NIST Special Publication 800-97 „Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11“

Bundesamt
für Sicherheit in der
Informationstechnik

NET.3.1 Router und Switches

1. Beschreibung

1.1. Einleitung

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

Router arbeiten auf der 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. Sie werden verwendet, um lokale Netze zu segmentieren oder um lokale Netze über Weitverkehrsnetze 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 OSI-Schicht 2, mittlerweile sind sie jedoch mit unterschiedlichen Funktionen erhältlich. Firmen kennzeichnen die Geräte 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 werden somit heute oft auf einem Gerät vereint.

1.2. Zielsetzung

Der Baustein beschreibt, wie Router und Switches sicher eingesetzt werden können.

1.3. Abgrenzung und Modellierung

Der Baustein NET.3.1 *Router und Switches* ist auf jeden im Informationsverbund eingesetzten Router und Switch anzuwenden.

Es ist eine große Auswahl von unterschiedlichen Routern und Switches von verschiedenen Firmen am Markt verfügbar. Der Baustein beschreibt keine spezifischen Anforderungen für bestimmte Produkte. Er ist so weit wie möglich unabhängig von einzelnen Produkten gehalten.

Durch die Verschmelzung der Funktionen von Routern und Switches kann der Großteil der Anforderungen sowohl auf Router als auch auf Switches angewendet werden. Der vorliegende Baustein unterscheidet hier weitgehend nicht zwischen den Gerätearten.

Heute bieten auch nahezu alle Betriebssysteme von Servern und auch Clients eine Routing-Funktionalität an. Dieser Baustein benennt keine Anforderungen für aktivierte Routing-Funktionen in Betriebssystemen von Servern und Clients.

Darüber hinaus werden Aspekte der infrastrukturellen Sicherheit nicht in diesem Baustein aufgeführt, wie z. B. die geeignete Aufstellung, Stromversorgung oder Verkabelung. Sicherheitsanforderungen zu diesen Themen finden sich in den jeweiligen Bausteinen der Schicht INF *Infrastruktur*.

Der vorliegende Baustein beschreibt keine Anforderungen, wie virtuelle Router und Switches abgesichert werden können. Ebenso wird nicht auf eventuell vorhandene Firewall-Funktionen von Routern und Switches eingegangen. Dazu muss zusätzlich der Baustein NET.3.2 *Firewall* umgesetzt werden. Einige Aspekte des Netzdesigns und -managements sind auch für den Einsatz von Routern und Switches von Bedeutung und werden im Rahmen der entsprechenden Anforderungen erwähnt. Weitere Informationen für den Aufbau, das Design und das Management eines Netzes sind in den Bausteinen NET.1.1 *Netzarchitektur und -design* bzw. NET.1.2 *Netzmanagement* zu finden.

Router und Switches sollten grundsätzlich mit berücksichtigt werden, wenn die Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement*, CON.3 *Datensicherungskonzept* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* umgesetzt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.3.1 *Router und Switches* von besonderer Bedeutung.

2.1. Distributed Denial of Service (DDoS)

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

2.2. Manipulation

Gelingt es Angreifenden, unberechtigt auf einen Router oder Switch zuzugreifen, können sie die Geräte neu konfigurieren oder auch zusätzliche Dienste starten. Die Konfiguration lässt sich beispielsweise so verändern, dass Dienste, Clients oder ganze Netzsegmente geblockt werden. Gleichzeitig kann so Netzverkehr am Switch abgefangen, gelesen oder manipuliert werden.

2.3. Fehlerhafte Konfiguration eines Routers oder Switches

Router und Switches werden mit einer Standardkonfiguration ausgeliefert, in der viele Dienste aktiviert sind. Auch verraten Login-Banner beispielsweise die Modell- und Versionsnummer des Gerätes. Werden Router und Switches mit unsicheren Werkseinstellungen produktiv eingesetzt, kann einfacher unberechtigt auf sie zugegriffen werden. Im schlimmsten Fall sind dadurch interne Dienste für Angreifende erreichbar.

2.4. Fehlerhafte Planung und Konzeption

Viele Institutionen planen und konzipieren den Einsatz von Routern und Switches fehlerhaft. So werden unter anderem Geräte beschafft, die nicht ausreichend dimensioniert sind, z. B. hinsichtlich der Port-Anzahl oder der Leistung. In der Folge kann ein Router oder Switch bereits überlastet sein, wenn

er zum ersten Mal eingesetzt wird. Dadurch sind eventuell Dienste oder ganze Netze nicht erreichbar und der Fehler muss aufwendig korrigiert werden.

2.5. Inkompatible aktive Netzkomponenten

Kompatibilitätsprobleme können insbesondere dann entstehen, wenn bestehende Netze um aktive Netzkomponenten anderer Firmen ergänzt oder wenn Netze mit Netzkomponenten unterschiedlicher Firmen betrieben werden. Werden aktive Netzkomponenten mit unterschiedlichen Implementierungen desselben Kommunikationsverfahrens gemeinsam in einem Netz betrieben, können einzelne Teilbereiche des Netzes, bestimmte Dienste oder sogar das gesamte Netz ausfallen.

2.6. MAC-Flooding

Beim MAC-Flooding schicken Angreifende viele Anfragen mit wechselnden Quell-MAC-Adressen an einen Switch. Sobald der Switch dann die Limits der MAC-Adressen, die er speichern kann, erreicht hat, fängt er an, sämtliche Anfragen an alle IT-Systeme im Netz zu schicken. Dadurch können Angreifende den Netzverkehr einsehen.

2.7. Spanning-Tree-Angriffe

Bei Spanning-Tree-Angriffen versenden Angreifende sogenannte Bridge Protocol Data Units (BPDUs) mit dem Ziel, die Switches dazu zu bringen, einen eigenen (bösartigen) Switch als Root Bridge anzusehen. Dadurch wird der Netzverkehr über den Switch der Angreifenden umgeleitet, sodass sie alle über ihn versendeten Informationen mitschneiden können. In der Folge können sie DDoS-Attacken initiieren und durch falsche BPDUs das Netz dazu zwingen, die Spanning-Tree-Topologie neu aufzubauen, wodurch das Netz ausfallen kann.

2.8. GARP-Attacken

Bei Gratuitous-ARP (GARP)-Attacken senden Angreifende unaufgeforderte ARP-Antworten an bestimmte Opfer oder an alle IT-Systeme im selben Subnetz. In dieser gefälschten ARP-Antwort tragend die Angreifenden ihre MAC-Adresse als Zuordnung zu einer fremden IP-Adresse ein und bringt das Opfer dazu, seine ARP-Tabelle so zu verändern, dass der Netzverkehr nun zu den Angreifenden, anstatt zum validen Ziel gesendet wird. Dadurch können sie die Kommunikation zwischen den Opfern mitschneiden oder sie manipulieren.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.3.1 *Router und Switches* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

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

Bevor ein Router oder Switch eingesetzt wird, MUSS er sicher konfiguriert werden. Alle Konfigurationsänderungen SOLLTEN nachvollziehbar dokumentiert sein. Die Integrität der Konfigurationsdateien MUSS in geeigneter Weise geschützt werden. Bevor Zugangspasswörter abgespeichert werden, MÜSSEN sie mithilfe eines zeitgemäßen kryptografischen Verfahrens abgesichert werden.

Router und Switches MÜSSEN so konfiguriert sein, dass nur zwingend erforderliche Dienste, Protokolle und funktionale Erweiterungen genutzt werden. Nicht benötigte Dienste, Protokolle und funktionale Erweiterungen MÜSSEN deaktiviert oder ganz deinstalliert werden. Ebenfalls MÜSSEN nicht benutzte Schnittstellen auf Routern und Switches deaktiviert werden. Unbenutzte Netzports MÜSSEN nach Möglichkeit deaktiviert oder zumindest einem dafür eingerichteten *Unassigned-VLAN* zugeordnet werden.

Wenn funktionale Erweiterungen benutzt werden, MÜSSEN die Sicherheitsrichtlinien der Institution weiterhin erfüllt sein. Auch SOLLTE begründet und dokumentiert werden, warum solche Erweiterungen eingesetzt werden.

Informationen über den internen Konfigurations- und Betriebszustand MÜSSEN nach außen verborgen werden. Unnötige Auskunftsdienste MÜSSEN deaktiviert werden.

NET.3.1.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.1.A4 Schutz der Administrationsschnittstellen (B)

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

Um Router und Switches zu administrieren bzw. zu überwachen, SOLLTEN geeignet verschlüsselte Protokolle eingesetzt werden. Sollte dennoch auf unverschlüsselte Protokolle zurückgegriffen werden, MUSS für die Administration ein eigenes Administrationsnetz (Out-of-Band-Management) genutzt werden. Die Managementschnittstellen und die Administrationsverbindungen MÜSSEN durch eine separate Firewall geschützt werden. Für die Schnittstellen MÜSSEN geeignete Zeitbeschränkungen für z. B. Timeouts vorgegeben werden.

Alle für das Management-Interface nicht benötigten Dienste MÜSSEN deaktiviert werden. Verfügt eine Netzkomponente über eine dedizierte Hardwareschnittstelle, MUSS der unberechtigte Zugriff darauf in geeigneter Weise unterbunden werden.

NET.3.1.A5 Schutz vor Fragmentierungsangriffen (B)

Am Router und Layer-3-Switch MÜSSEN Schutzmechanismen aktiviert sein, um IPv4- sowie IPv6-Fragmentierungsangriffe abzuwehren.

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

Es MUSS für die Administrierenden immer möglich sein, direkt auf Router und Switches zuzugreifen, sodass diese weiterhin lokal administriert werden können, auch wenn das gesamte Netz ausfällt.

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

Ein Router oder Switch MUSS so konfiguriert werden, dass er unter anderem folgende Ereignisse protokolliert:

- Konfigurationsänderungen (möglichst automatisch),
- Reboot,
- Systemfehler,
- Statusänderungen pro Interface, System und Netzsegment sowie
- Login-Fehler

NET.3.1.A8 Regelmäßige Datensicherung (B)

Die Konfigurationsdateien von Routern und Switches MÜSSEN regelmäßig gesichert werden. Die Sicherungskopien MÜSSEN so abgelegt werden, dass im Notfall darauf zugegriffen werden kann.

NET.3.1.A9 Betriebsdokumentationen (B)

Die wichtigsten betrieblichen Aufgaben eines Routers oder Switches MÜSSEN geeignet dokumentiert werden. Es SOLLTEN alle Konfigurationsänderungen sowie sicherheitsrelevante Aufgaben dokumentiert werden. Die Dokumentation SOLLTEN vor unbefugten Zugriffen geschützt werden.

3.2. Standard-Anforderungen

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

NET.3.1.A10 Erstellung einer Sicherheitsrichtlinie (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTE eine spezifische Sicherheitsrichtlinie erstellt werden. In der Sicherheitsrichtlinie SOLLTEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie Router und Switches sicher betrieben werden können. Die Richtlinie SOLLTE allen Administrierenden bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den festgelegten Anforderungen abgewichen, SOLLTE das mit dem oder der ISB abgestimmt und dokumentiert werden. Es SOLLTE regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse SOLLTEN geeignet dokumentiert werden.

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

Bevor Router oder Switches beschafft werden, SOLLTE basierend auf der Sicherheitsrichtlinie eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Es SOLLTE darauf geachtet werden, dass das von der Institution angestrebte Sicherheitsniveau mit den zu beschaffenden Geräten erreicht werden kann. Grundlage für die Beschaffung SOLLTEN daher die Anforderungen aus der Sicherheitsrichtlinie sein.

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

Es SOLLTE eine Konfigurations-Checkliste erstellt werden, anhand derer die wichtigsten sicherheitsrelevanten Einstellungen auf Routern und Switches geprüft werden können. Da die sichere Konfiguration stark vom Einsatzzweck abhängt, SOLLTEN die unterschiedlichen Anforderungen der Geräte in der Konfigurations-Checkliste berücksichtigt werden.

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

Router und Switches SOLLTEN ausschließlich über ein separates Managementnetz (Out-of-Band-Management) administriert werden. Eine eventuell vorhandene Administrationsschnittstelle über das

eigentliche Datennetz (In-Band) SOLLTE deaktiviert werden. Die verfügbaren Sicherheitsmechanismen der eingesetzten Managementprotokolle zur Authentisierung, Integritätssicherung und Verschlüsselung SOLLTEN aktiviert werden. Alle unsicheren Managementprotokolle SOLLTEN deaktiviert werden.

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

Die Protokolle ICMP und ICMPv6 SOLLTEN restriktiv gefiltert werden.

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

Es SOLLTE verhindert werden, dass Angreifende mithilfe gefälschter, reservierter oder noch nicht zugewiesener IP-Adressen in die Router und Switches eindringen können.

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

Beim Einsatz von IPv6 SOLLTEN Mechanismen eingesetzt werden, die Angriffe auf den Routing-Header des Type-0 erkennen und verhindern.

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

Es SOLLTEN Mechanismen eingesetzt werden, die hochvolumige Angriffe sowie TCP-State-Exhaustion-Angriffe erkennen und abwehren.

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

Der Zugriff auf Router und Switches SOLLTE mithilfe von Access Control Lists (ACLs) definiert werden. In der ACL SOLLTE anhand der Sicherheitsrichtlinie der Institution festgelegt werden, über welche IT-Systeme oder Netze mit welcher Methode auf einen Router oder Switch zugegriffen werden darf. Für den Fall, dass keine spezifischen Regeln existieren, SOLLTE generell der restriktivere Allowlist-Ansatz bevorzugt werden.

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

Die Ports eines Switches SOLLTEN vor unberechtigten Zugriffen geschützt werden.

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

Router SOLLTEN sich authentisieren, wenn sie Routing-Informationen austauschen oder Updates für Routing-Tabellen verschicken. Es SOLLTEN ausschließlich Routing-Protokolle eingesetzt werden, die dies unterstützen.

Dynamische Routing-Protokolle SOLLTEN ausschließlich in sicheren Netzen verwendet werden. Sie DÜRFEN NICHT in demilitarisierten Zonen (DMZs) eingesetzt werden. In DMZs SOLLTEN stattdessen statische Routen eingetragen werden.

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

Router und Switches SOLLTEN an ein zentrales Identitäts- und Berechtigungsmanagement angebunden werden.

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

Es SOLLTE geplant und vorbereitet werden, welche Fehler bei Routern oder Switches in einem Notfall diagnostiziert werden könnten. Außerdem SOLLTE geplant und vorbereitet werden, wie die identifizierten Fehler behoben werden können. Für typische Ausfallszenarien SOLLTEN entsprechende Handlungsanweisungen definiert und in regelmäßigen Abständen aktualisiert werden.

Die Notfallplanungen für Router und Switches SOLLTEN mit der übergreifenden Störungs- und Notfallvorsorge abgestimmt sein. Die Notfallplanungen SOLLTEN sich am allgemeinen Notfallvorsorgekonzept orientieren. Es SOLLTE sichergestellt sein, dass die Dokumentationen zur

Notfallvorsorge und die darin enthaltenen Handlungsanweisungen in Papierform vorliegen. Das im Rahmen der Notfallvorsorge beschriebene Vorgehen SOLLTE regelmäßig geprobt werden.

NET.3.1.A23 Revision und Penetrationstests (S)

Router und Switches SOLLTEN regelmäßig auf bekannte Sicherheitsprobleme hin überprüft werden. Auch SOLLTEN regelmäßig Revisionen durchgeführt werden. Dabei SOLLTE unter anderem geprüft werden, ob der Ist-Zustand der festgelegten sicheren Grundkonfiguration entspricht. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.3.1.A24 Einsatz von Netzzugangskontrollen (H)

Eine Port-based Access Control SOLLTE nach IEEE 802.1x auf Basis von EAP-TLS implementiert werden. Es SOLLTE KEINE Implementierung nach den Standards IEEE 802.1x-2001 und IEEE 802.1x-2004 erfolgen.

NET.3.1.A25 Erweiterter Integritätsschutz für die Konfigurationsdateien (H)

Stürzt ein Router oder Switch ab, SOLLTE sichergestellt werden, dass bei der Wiederherstellung bzw. beim Neustart keine alten oder fehlerhaften Konfigurationen (unter anderem ACLs) benutzt werden.

NET.3.1.A26 Hochverfügbarkeit (H)

Die Realisierung einer Hochverfügbarkeitslösung SOLLTE den Betrieb der Router und Switches bzw. deren Sicherheitsfunktionen NICHT behindern oder das Sicherheitsniveau senken. Router und Switches SOLLTEN redundant ausgelegt werden. Dabei SOLLTE darauf geachtet werden, dass die Sicherheitsrichtlinie der Institution eingehalten wird.

NET.3.1.A27 Bandbreitenmanagement für kritische Anwendungen und Dienste (H)

Router und Switches SOLLTEN Funktionen enthalten und einsetzen, mit denen sich die Applikationen erkennen und Bandbreiten priorisieren lassen.

NET.3.1.A28 Einsatz von zertifizierten Produkten (H)

Es SOLLTEN Router und Switches mit einer Sicherheitsevaluierung nach Common Criteria eingesetzt werden, mindestens mit der Stufe EAL4.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat in den BSI-Standards zur Internet-Sicherheit (ISi-Reihe) weitere Informationen zur Sicherheit bei Routern und Switches veröffentlicht.

Das Institute of Electrical and Electronics Engineers (IEEE) hat in seiner Standard-Reihe die Standards IEEE 802.1Q „IEEE Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks“ und IEEE 802.1AE „IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security“ veröffentlicht.

In den Requests for Comments (RFC) bieten der RFC 6165 „Extensions to IS-IS for Layer-2 Systems“ und der RFC 7348 „Virtual Extensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks“ weiterführende Informationen zu Routern und Switches.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.3.2 Firewall

1. Beschreibung

1.1. Einleitung

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

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

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

1.2. Zielsetzung

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

1.3. Abgrenzung und Modellierung

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

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

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

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

Darüber hinaus wird nicht auf Produkte wie sogenannte Next Generation Firewalls (NGFW) oder Unified Threat Management (UTM)-Firewalls eingegangen, die zusätzlich funktionale Erweiterungen enthalten, z. B. VPN, Systeme zur Intrusion Detection und Intrusion Prevention (IDS/IPS), Virenscanner oder Spam-Filter. Sicherheitsaspekte dieser funktionalen Erweiterungen sind nicht Gegenstand des vorliegenden Bausteins, sondern werden z. B. in den Bausteinen NET.3.3 *VPN* und OPS1.1.4 *Schutz vor Schadprogrammen* behandelt.

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

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

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.3.2 *Firewall* von besonderer Bedeutung.

2.1. Distributed Denial of Service (DDoS)

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

2.2. Manipulation

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

2.3. Umgehung der Firewall-Regeln

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

2.4. Fehlerhafte Konfiguration und Bedienungsfehler einer Firewall

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

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.3.2 *Firewall* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.3.2.A1 Erstellung einer Sicherheitsrichtlinie (B)

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

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

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

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

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

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

Basierend auf den Firewall-Regeln aus NET.3.2.A2 *Festlegen der Firewall-Regeln* MÜSSEN geeignete Filterregeln für den Paketfilter definiert und eingerichtet werden.

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

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

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

NET.3.2.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.2.A6 Schutz der Administrationsschnittstellen (B)

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

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

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

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

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

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

NET.3.2.A9 Protokollierung (B)

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

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

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

Wenn sich Benutzende am Sicherheitsproxy authentisieren, MÜSSEN auch Authentisierungsdaten oder ausschließlich die Information über eine fehlgeschlagene Authentisierung protokolliert werden.

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

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

NET.3.2.A11 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.2.A12 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.2.A13 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.2.A14 Betriebsdokumentationen (B)

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

NET.3.2.A15 Beschaffung einer Firewall (B)

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

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

3.2. Standard-Anforderungen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

NET.3.2.A22 Sichere Zeitsynchronisation (S)

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

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

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

NET.3.2.A24 Revision und Penetrationstests (S)

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

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

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

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

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

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

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

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

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

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

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

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

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

NET.3.2.A29 Einsatz von Hochverfügbarkeitslösungen (H)

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

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

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

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

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

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

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

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld Firewall veröffentlicht:

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

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

Bundesamt
für Sicherheit in der
Informationstechnik

NET.3.3 VPN

1. Beschreibung

1.1. Einleitung

Mithilfe von Virtuellen Privaten Netzen (VPNs) können schutzbedürftige Daten über nicht-vertrauenswürdige Netze, wie das Internet, übertragen werden. Ein VPN ist ein virtuelles Netz, das innerhalb eines anderen Netzes betrieben wird, jedoch logisch von diesem Netz getrennt ist. Das VPN nutzt das Netz hierbei lediglich als Transportmedium, ist aber selber unabhängig von der Struktur und dem Aufbau des verwendeten Netzes. VPNs können mithilfe kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten schützen. VPNs ermöglichen auch dann die sichere Authentisierung der Kommunikationspunkte, wenn mehrere Netze oder IT-Systeme über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

1.2. Zielsetzung

Der Baustein definiert Anforderungen, mit denen sich ein VPN zielgerichtet und sicher planen, umsetzen und betreiben lässt.

1.3. Abgrenzung und Modellierung

Der vorliegende Baustein ist für jede Zugriffsmöglichkeit auf das Netz der Institution über einen VPN-Endpunkt anzuwenden.

Der Baustein geht nicht auf Grundlagen für sichere Netze und deren Aufbau ein (siehe dazu NET.1.1 *Netzarchitektur und -design*). Auch deckt dieser Baustein nicht alle mit dem Betrieb eines VPN zusammenhängenden Prozesse ab. VPNs sollten grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement*, OPS.1.2.5 *Fernwartung*, OPS.1.1.2 *Ordnungsgemäße IT-Administration* sowie CON.1 *Kryptokonzept* mit berücksichtigt werden.

Empfehlungen, wie die Betriebssysteme der VPN-Endpunkte konfiguriert werden können, sind ebenfalls nicht Bestandteil dieses Bausteins. Entsprechende Anforderungen sind im Baustein SYS.1.1 *Allgemeiner Server* beziehungsweise SYS.2.1 *Allgemeiner Client* sowie in den jeweiligen betriebssystemspezifischen Bausteinen des IT-Grundschutz-Kompendiums zu finden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.3.3 *VPN* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Planung des VPN-Einsatzes

Bei einem nicht sorgfältig geplanten, aufgebauten oder konfigurierten VPN können Sicherheitslücken entstehen, die alle IT-Systeme betreffen könnten, die mit dem VPN verbunden sind. Angreifenden kann es so möglich sein, auf vertrauliche Informationen der Institution zuzugreifen.

So ist es durch eine unzureichende VPN-Planung beispielsweise möglich, dass die Benutzenden nicht ordnungsgemäß geschult wurden. Dadurch könnten sie das VPN in einer unsicheren Umgebung benutzen oder sich von unsicheren Clients aus einwählen. Dies ermöglicht es Angreifenden eventuell, auf das gesamte Institutionsnetz zuzugreifen.

Auch wenn die regelmäßige Kontrolle der Zugriffe auf das VPN unzureichend geplant wurde, könnten Angriffe nicht rechtzeitig erkannt werden. Somit kann nicht zeitnah reagiert werden und Angreifende unbemerkt Daten stehlen oder ganze Prozesse sabotieren.

2.2. Unsichere VPN-Dienstleistende

Hat eine Institution seine VPN-Dienstleistenden nicht sorgfältig ausgewählt, könnte dadurch das gesamte Netz der Institution unsicher werden. So könnte beispielsweise ein von den Dienstleistenden unsicher angebotener VPN-Zugang für Angriffe genutzt werden, um gezielt Informationen zu stehlen.

2.3. Unsichere Konfiguration der VPN-Clients für den Fernzugriff

Wird ein VPN-Client nicht sicher konfiguriert, könnten die Benutzenden dessen Sicherheitsmechanismen falsch oder gar nicht benutzen. Auch verändern sie eventuell die Konfiguration des VPN-Clients. Ebenso ist es durch eine unsichere Konfiguration möglich, dass von den Benutzenden installierte Software auch die Sicherheit des VPN-Clients gefährdet.

2.4. Unsichere Standard-Einstellungen auf VPN-Komponenten

In der Standard-Einstellung sind VPN-Komponenten meist ohne oder nur mit unzureichenden Sicherheitsmechanismen vorkonfiguriert. Oft wird mehr auf Nutzungsfreundlichkeit und problemlose Integration in bestehende IT-Systeme als auf Sicherheit geachtet. Werden VPN-Komponenten nicht oder nur mangelhaft an die konkreten Sicherheitsbedürfnisse der Institution angepasst, können Schwachstellen und somit gefährliche Angriffspunkte entstehen. Werden beispielsweise werksseitig voreingestellte Passwörter nicht geändert, könnte das gesamte VPN und damit das interne Netz der Institution angegriffen werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.3.3 *VPN* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte Grundsätzlich zuständig sein. Darüber hinaus kann es noch Weitere Zuständigkeiten geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.3.3.A1 Planung des VPN-Einsatzes (B)

Die Einführung eines VPN MUSS sorgfältig geplant werden. Dabei MÜSSEN die Verantwortlichkeiten für den VPN-Betrieb festgelegt werden. Es MÜSSEN für das VPN zudem Benutzendengruppen und deren Berechtigungen geplant werden. Ebenso MUSS definiert werden, wie erteilte, geänderte oder entzogene Zugriffsberechtigungen zu dokumentieren sind.

NET.3.3.A2 Auswahl von VPN-Dienstleistenden (B)

Falls VPN-Dienstleistende eingesetzt werden, MÜSSEN mit diesen Service Level Agreements (SLAs) ausgehandelt und schriftlich dokumentiert werden. Es MUSS regelmäßig kontrolliert werden, ob die VPN-Dienstleistenden die vereinbarten SLAs einhalten.

NET.3.3.A3 Sichere Installation von VPN-Endgeräten (B)

Wird eine Appliance eingesetzt, die eine Wartung benötigt, MUSS es dafür einen gültigen Wartungsvertrag geben. Es MUSS sichergestellt werden, dass nur qualifiziertes Personal VPN-Komponenten installiert. Die Installation der VPN-Komponenten sowie eventuelle Abweichungen von den Planungsvorgaben SOLLTEN dokumentiert werden. Die Funktionalität und die gewählten Sicherheitsmechanismen des VPN MÜSSEN vor Inbetriebnahme geprüft werden.

NET.3.3.A4 Sichere Konfiguration eines VPN (B)

Für alle VPN-Komponenten MUSS eine sichere Konfiguration festgelegt werden. Diese SOLLTE geeignet dokumentiert werden. Auch MUSS die für die Administration zuständige Person regelmäßig kontrollieren, ob die Konfiguration noch sicher ist und sie eventuell für alle IT-Systeme anpassen.

NET.3.3.A5 Sperrung nicht mehr benötigter VPN-Zugänge (B)

Es MUSS regelmäßig geprüft werden, ob ausschließlich berechtigte IT-Systeme und Benutzende auf das VPN zugreifen können. Nicht mehr benötigte VPN-Zugänge MÜSSEN zeitnah deaktiviert werden. Der VPN-Zugriff MUSS auf die benötigten Benutzungszeiten beschränkt werden.

3.2. Standard-Anforderungen

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

NET.3.3.A6 Durchführung einer VPN-Anforderungsanalyse (S)

Eine Anforderungsanalyse SOLLTE durchgeführt werden, um für das jeweilige VPN die Einsatzszenarien zu bestimmen und daraus Anforderungen an die benötigten Hard- und Software-Komponenten ableiten zu können. In der Anforderungsanalyse SOLLTEN folgende Punkte betrachtet werden:

- Geschäftsprozesse beziehungsweise Fachaufgaben,

- Zugriffswege,
- Identifikations- und Authentisierungsverfahren,
- Benutzende und ihre Berechtigungen,
- Zuständigkeiten sowie
- Meldewege.

NET.3.3.A7 Planung der technischen VPN-Realisierung (S)

Neben der allgemeinen Planung (siehe NET.3.3.A1 *Planung des VPN-Einsatzes*) SOLLTEN die technischen Aspekte eines VPN sorgfältig geplant werden. So SOLLTEN für das VPN die Verschlüsselungsverfahren, VPN-Endpunkte, erlaubten Zugangsprotokolle, Dienste und Ressourcen festgelegt werden. Zudem SOLLTEN die Teilnetze definiert werden, die über das VPN erreichbar sind. (siehe NET.1.1 *Netzarchitektur und -design).*

NET.3.3.A8 Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung (S)

Eine Sicherheitsrichtlinie zur VPN-Nutzung SOLLTE erstellt werden. Diese SOLLTE allen Mitarbeitenden bekannt gegeben werden. Die in der Sicherheitsrichtlinie beschriebenen Sicherheitsmaßnahmen SOLLTEN im Rahmen von Schulungen erläutert werden. Wird für Mitarbeitende ein VPN-Zugang eingerichtet, SOLLTE diesen ein Merkblatt mit den wichtigsten VPN-Sicherheitsmechanismen ausgehändigt werden. Alle VPN-Benutzende SOLLTEN verpflichtet werden, die Sicherheitsrichtlinien einzuhalten.

NET.3.3.A9 Geeignete Auswahl von VPN-Produkten (S)

Bei der Auswahl von VPN-Produkten SOLLTEN die Anforderungen der Institutionen an die Vernetzung unterschiedlicher Standorte und die Anbindung von mobilen Mitarbeitenden oder Telearbeitsplätzen berücksichtigt werden.

NET.3.3.A10 Sicherer Betrieb eines VPN (S)

Für VPNs SOLLTE ein Betriebskonzept erstellt werden. Darin SOLLTEN die Aspekte Qualitätsmanagement, Überwachung, Wartung, Schulung und Autorisierung beachtet werden.

NET.3.3.A11 Sichere Anbindung eines externen Netzes (S)

Es SOLLTE sichergestellt werden, dass VPN-Verbindungen NUR zwischen den dafür vorgesehenen IT-Systemen und Diensten aufgebaut werden. Die dabei eingesetzten Tunnel-Protokolle SOLLTEN für den Einsatz geeignet sein.

NET.3.3.A12 Konten- und Zugriffsverwaltung bei Fernzugriff-VPNs (S)

Für Fernzugriff-VPNs SOLLTE eine zentrale und konsistente Konten- und Zugriffsverwaltung gewährleistet werden.

NET.3.3.A13 Integration von VPN-Komponenten in eine Firewall (S)

Die VPN-Komponenten SOLLTEN in die Firewall integriert werden. Dies SOLLTE dokumentiert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27033-5:2013 „Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)“ Vorgaben für den Einsatz von VPNs.

Das National Institute of Standards and Technology (NIST) macht in seiner Special Publication 800-77 „Guide to IPsec VPNs“ generelle Vorgaben zum Einsatz von VPNs.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.3.4 Network Access Control

1. Beschreibung

1.1. Einleitung

Eine Netzzugangskontrolle (engl. Network Access Control, NAC) sichert Netzzugänge im Endgerätebereich durch Identitätsprüfung (Authentisierung) und Reglementierung (Autorisierung) ab. Unter Endgeräten werden in diesem Baustein alle IT-Systeme verstanden, die am Access Layer eines Campus-Netzes angeschlossen werden. NAC kann sowohl in kabelgebundenen als auch in drahtlosen Netzen eingesetzt werden. Eine Identität kann zum Beispiel über Konten mit Zertifikaten sicher geprüft werden. Durch die folgende Autorisierung werden den Endgeräten über Autorisierungsregeln passende Netzsegmente und Berechtigungen zugewiesen und damit Zugriffsregeln festgelegt. Ebenso kann Endgeräten der Netzzugang verweigert werden.

Beispielsweise kann ein Drucker über NAC als solcher identifiziert und mit einem validen Zertifikat sicher authentisiert werden. Wurde der Drucker erfolgreich authentisiert, wird er dann mittels NAC-Autorisierung dem für den Drucker vorgesehenen Netzsegment zugewiesen.

NAC-Lösungen nutzen dabei entweder die im Standard IEEE 802.1X (Port Based Network Access Control) beschriebenen Techniken oder die sogenannte MAC-Adress-Authentisierung. Bei IEEE 802.1X erfolgt die Authentisierung über das Extensible Authentication Protocol (EAP) zwischen einer Software auf dem Endgerät, dem sogenannten Supplicant, und dem sogenannten Authenticator, der von einem Access-Switch, WLAN Access Point oder WLAN Controller realisiert wird. Für die Authentisierung wird zusätzlich ein zentraler RADIUS-Server (Remote Authentication Dial-In User Service) genutzt. Der RADIUS-Server wird auch als Authentication Server oder AAA-Server (Authentication, Authorization, Accounting) bezeichnet. Bei der MAC-Adress-Authentisierung wird das Endgerät über seine MAC-Adresse authentisiert.

Eine NAC-Lösung nach IEEE 802.1X umfasst also folgende Komponenten:

- Authentication Server oder RADIUS-Server
- Supplicant auf einem Endgerät
- Authenticator auf einem Access-Switch oder einer WLAN-Komponente (WLAN Access Point oder WLAN Controller)
- zentrale NAC-Identitätsverwaltung, die als integrierte Identitätsverwaltung auf dem Server realisiert sein kann oder auf bestehende Verzeichnisdienste zurückgreift

Eine NAC-Lösung umfasst in diesem Baustein alle zuvor beschriebenen Komponenten. Ist eine einzelne Komponente der NAC-Lösung gemeint, z. B. der RADIUS-Server, dann wird diese

Komponente tatsächlich auch als solche benannt. Als zentrale Komponenten einer NAC-Lösung gelten in diesem Baustein der RADIUS-Server und die NAC-Identitätsverwaltung.

Damit eine NAC-Lösung sinnvoll eingesetzt werden kann und die Netzzugänge geeignet abgesichert werden können, müssen viele Punkte festgelegt und die genannten Komponenten der Lösung aufeinander abgestimmt werden. Weiterhin sind NAC-spezifische Prozesse (z. B. Maßnahmen, um Störungen zu beheben) zu definieren und bestehende Prozesse (z. B. Inbetriebnahme von Endgeräten) anzupassen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei NAC zu etablieren. Eine NAC-Lösung soll sicherstellen, dass der Zugang zum Netz durch identitätsabhängige Autorisierungsregeln reglementiert wird. Dadurch werden Informationen geschützt, die über Netze verarbeitet, gespeichert und übertragen werden.

1.3. Abgrenzung und Modellierung

Der Baustein NET.3.4 *Network Access Control* ist auf die Elemente einer NAC-Lösung anzuwenden. Dies beinhaltet betroffene Netze, Clients und zentrale Komponenten.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt NAC-Lösungen, die auf dem Standard IEEE 802.1X und MAC-Adress-Authentisierung via RADIUS basieren. Dabei liegt der Fokus auf folgende Teilaspekte einer NAC-Lösung:

- allgemeine Festlegungen für NAC sowohl für die zentralen Komponenten als auch für die Endgeräte
- Anforderungen an Authentisierung und Autorisierung
- Festlegungen für Management und Betrieb einer NAC-Lösung

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Verzeichnisdienste (siehe APP.2.1 *Allgemeiner Verzeichnisdienst*)
- Netzarchitektur und -design (siehe NET.1.1 *Netzarchitektur und -design*)
- WLAN-spezifische Aspekte (siehe NET.2.1 *WLAN-Betrieb* und NET.2.2 *WLAN-Nutzung*)
- allgemeine Betriebsaspekte (siehe Bausteine der Schicht OPS *Betrieb*)

Dieser Baustein behandelt **nicht** die folgenden Inhalte:

- Port Security sowie allgemeine Aspekte für Netzkomponenten (siehe NET.3.1 *Router und Switches*)
- proprietäre NAC-Implementierungen, die nicht auf IEEE 802.1X basieren
- die Implementierung eines RADIUS-Servers auf Netzkomponenten (Access-Switch, WLAN Access Point oder WLAN Controller)
- administrative Authentisierung an Netzkomponenten mittels RADIUS
- allgemeine Aspekte für Endgeräte (siehe Bausteine der Schichten SYS.2 *Desktop-Systeme*, SYS.3 *Mobile Devices* und SYS.4 *Sonstige Systeme*)
- allgemeine Aspekte für Server (siehe SYS.1.1 *Allgemeiner Server*) und Virtualisierung (siehe SYS.1.5 *Virtualisierung*)

- allgemeine Aspekte für Identitäts- und Berechtigungsmanagement (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*)

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.3.4 *Network Access Control* von besonderer Bedeutung.

2.1. Unzureichende Planung der NAC-Lösung

Sind nicht alle für NAC relevanten IT-Systeme und Informationen in einem IT-Asset-Management erfasst, kann eine NAC-Lösung nicht ausreichend geplant werden. Endgeräte erhalten dann gegebenenfalls keinen Zugang zum Netz oder einen Zugang zu einem falschen Netzsegment.

Wurden die Anforderungen an die NAC-Lösung nicht ausreichend erfasst und analysiert, kann auch dies zu einer unzureichenden Planung führen. Beispielsweise ist es dann möglich, dass eingesetzte Switches die Anforderungen an die geplante NAC-Lösung nicht erfüllen können oder der geplante RADIUS-Server falsch dimensioniert wird. Eine weitere Folge könnten auch zu harte oder zu weiche Vorgaben für die genutzten Authentisierungs- und Autorisierungsverfahren sein. Dadurch könnte Endgeräten entweder der Zugang zum Netz verweigert oder unsichere Authentisierungsverfahren könnten genutzt werden, obwohl sichere Verfahren möglich wären. Möglicherweise könnten dadurch auch zu weitreichende Kommunikationsberechtigungen erlangt werden.

2.2. Unzureichend abgestimmte Integration von Endgeräten in die NAC-Lösung

Fehlende oder unzureichend umgesetzte Orchestrierungswerkzeuge, Sicherheitsrichtlinien, Anforderungskataloge und Ressourcen für die Erfassung aller Endgeräte können dazu führen, dass Endgeräte unzureichend abgestimmt in die NAC-Lösung integriert werden. Dies erschwert es, ein sicheres und betriebsfreundliches Authentisierungsverfahren je Endgerätegruppe umzusetzen und ein entsprechendes Inbetriebnahmeverfahren zu konzipieren. Dadurch könnten die Kommunikationsmöglichkeiten der Endgeräte negativ beeinträchtigt werden. Außerdem kann es sein, dass zu schützende Geräte versehentlich in falschen Netzsegmenten positioniert werden.

Sind die Endgeräte unzureichend standardisiert oder werden NAC-spezifische Endgeräteanforderungen unzureichend unterstützt, kann dies auch dazu führen, dass unsichere Authentisierungsverfahren eingesetzt werden, obwohl eine starke Authentisierung grundsätzlich möglich wäre.

2.3. Nutzung unzureichend sicherer Protokolle bei NAC

Werden sichere EAP-Authentisierungsverfahren technisch nicht unterstützt, kann es passieren, dass unsichere Authentisierungsprotokolle wie EAP-MD5 oder MAC-Authentisierung eingesetzt werden müssen. In diesem Fall sind Spoofing-, Replay- oder Man-in-the-Middle-Angriffe leichter möglich und es kann nicht ausgeschlossen werden, dass unberechtigte IT-Systeme in das Netz gelangen. Wird für Endgeräte mit schwachen Authentisierungsprotokollen nicht eingeschränkt, mit welchen Zielen und über welche Protokolle sie kommunizieren dürfen, können auch unberechtigte IT-Systeme, die durch einen der oben genannten Angriffe Zugang erhalten, weitreichende Kommunikationsmöglichkeiten erlangen.

2.4. Fehlerhafte Konfiguration der NAC-Lösung

Durch menschliche Fehler, unzureichende Prozesse oder unzureichende Personalkapazitäten und den dadurch bedingten Zeitmangel kann es passieren, dass die NAC-spezifischen Parameter an Endgeräten, Access-Switches oder RADIUS-Servern (NAC-Regelwerk) fehlerhaft konfiguriert werden. Dies kann dazu führen, dass sich die gesamte NAC-Lösung ungewollt falsch verhält, wodurch z. B. Endgeräte benötigte Ressourcen nicht erreichen können oder keinen Netzzugang erhalten.

Werden MAC-Adressen bewusst falsch registriert, können dadurch zu viele Ressourcen freigeschaltet werden, indem falsche Netzsegmente oder andere falsche Autorisierungsparameter zugewiesen werden.

2.5. Unzureichende Validierung von Konfigurationsänderungen

Unzureichende Änderungsprozesse, die Konfigurationsänderungen nicht oder nur unzureichend validieren, begünstigen Fehler in der Konfiguration. Hierdurch kann es passieren, dass für Endgeräte zu viel oder zu wenig schützenswerte Ressourcen erreichbar sind oder es ihnen gänzlich verwehrt wird, auf das Netz zuzugreifen. Wird z. B. NAC an Switch-Ports ohne zwingenden Grund abgeschaltet, können gegebenenfalls unberechtigte Endgeräte uneingeschränkt auf das Netz zugreifen. Wird neue Software auf Endgeräten unzureichend validiert, kann dies z. B. zu Interferenzen zwischen Software-Komponenten führen und die Funktionalität des Supplicants beeinflussen.

2.6. Unzureichend geschützter Netzzugang

Wird NAC an Switch-Ports temporär oder dauerhaft abgeschaltet, ist der Netzzugang unzureichend geschützt. Dadurch ist es möglich, dass unautorisierte Personen auf das Netz zugreifen können oder unsichere IT-Systeme zu weitgehende Kommunikationsberechtigungen erhalten. In der Folge kann unberechtigt auf Informationen zugegriffen und Informationen können manipuliert oder gelöscht werden. Außerdem kann auf diese Weise Schadsoftware eingeschleust werden.

Wird die Endgeräte-Compliance unzureichend geprüft, kann dies auch zu einem unzureichend geschützten Netzzugang führen, wenn das Endgerät z. B. über unzureichenden Virenschutz verfügt und dadurch Schadsoftware eingeschleust wird.

2.7. Ausfall oder unzureichende Erreichbarkeit der zentralen NAC-Komponenten

Ein unzureichendes oder unzureichend umgesetztes NAC-Konzept, gestörte NAC-Komponenten oder ein gestörtes Netz, unzureichende Anforderungsanalyse, mangelnde Prozesse oder Denial-of-Service-Angriffe (DoS-Angriffe) können dazu führen, dass die zentralen NAC-Komponenten ausfallen oder nicht erreichbar sind. Dies hat Auswirkungen auf die Fähigkeit der Endgeräte zu kommunizieren. Zum Beispiel haben, abhängig von der Switch-Konfiguration, Endgeräte bei Ausfall aller RADIUS-Server entweder keinen oder einen uneingeschränkten Netzzugang.

2.8. Nachverfolgung von Benutzenden

Ein unzureichendes Administrationskonzept, eine unzureichende Umsetzung der Konzeptionierung, zu lange Speicherzeiten oder eine mangelnde Abstimmung mit Betriebsrat und Datenschutzbeauftragten könnten dazu führen, dass personenrelevante Log-Daten unzureichend geschützt sind. Dadurch könnten Benutzendenprofile erstellt werden, die es ermöglichen, dass Mitarbeitende zeitlich nachverfolgt werden können.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.3.4 *Network Access Control* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Institution

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.3.4.A1 Begründete Entscheidung für den Einsatz von NAC (B) [Institution]

Die Institution MUSS grundsätzlich entscheiden, ob und in welchem Umfang NAC eingesetzt wird. Die getroffene Entscheidung MUSS zusammen mit einer Begründung an geeigneter Stelle dokumentiert werden.

Wird NAC eingesetzt, MÜSSEN folgende Punkte geeignet thematisiert werden:

- Netzbereiche und Netzkomponenten, für die NAC realisiert werden soll
- Umgang mit internen Endgeräten und Fremdendgeräten
- Berücksichtigung von NAC bei der Beschaffung von neuen IT-Systemen

3.2. Standard-Anforderungen

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

NET.3.4.A2 Planung des Einsatzes von NAC (S)

Der Einsatz von NAC SOLLTE umfassend und detailliert geplant werden. Die Planung SOLLTE dabei mindestens folgende Aspekte beinhalten:

- Erstellung von Anforderungskatalogen für Endgeräte, Access-Switches und RADIUS-Server
- Prüfung und gegebenenfalls Ergänzung des IT-Asset-Managements
- Erstellung eines spezifischen NAC-Konzepts
- Festlegung von Beschaffungs-, Betriebs-, und Incident-Prozessen für NAC-Komponenten
- Migrationsplanung
- Monitoring und Logging der NAC-Lösung

- Anbindung an sicherheitsrelevante Komponenten (z. B. Firewalls, Virenschutz, Schwachstellen-Scanner, System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen)
- Zusatzfunktionen wie Profiling, Endgerätekonformitätsprüfung und Integritätsprüfung sowie Verschlüsselung auf Layer 2 mit MACsec

NET.3.4.A3 Erstellung eines Anforderungskatalogs für NAC (S)

Die Anforderungen an die NAC-Lösung SOLLTEN in einem Anforderungskatalog erhoben werden. Der Anforderungskatalog SOLLTE dabei die grundlegenden funktionalen Anforderungen umfassen und alle NAC-Komponenten (z. B. Endgeräte, Access-Switches und RADIUS-Server) adressieren.

Der Anforderungskatalog SOLLTE mit allen betroffenen Fachabteilungen, den zuständigen Gremien und den Richtlinien der Institution abgestimmt werden. Der Anforderungskatalog SOLLTE regelmäßig und bei Bedarf aktualisiert werden.

Wenn NAC-Komponenten beschafft werden, SOLLTEN zugehörige Anforderungen berücksichtigt werden.

Die NAC-Lösung SOLLTE auf Basis des Anforderungskatalogs getestet werden.

NET.3.4.A4 Erstellung eines NAC-Konzepts (S)

Ausgehend von der Entscheidung aus NET.3.4.A1 *Begründete Entscheidung für den Einsatz von NAC* und den Anforderungen an die NAC-Lösung SOLLTE ein NAC-Konzept erstellt werden. Das NAC-Konzept SOLLTE mit dem Segmentierungskonzept gemäß NET.1.1 *Netzarchitektur und -design* abgestimmt werden. Darüber hinaus SOLLTEN im NAC-Konzept mindestens folgende Aspekte festgelegt werden:

- Netzbereiche, in denen NAC eingeführt wird
- Authentisierung und Autorisierung
- Nutzung von Zusatzfunktionen
- Konfigurationsvorgaben für betroffene Endgerätetypen, Access-Switches und WLAN Access Points sowie WLAN Controller
- Aufbau der RADIUS-Infrastruktur und das grundlegende Regelwerk für NAC
- Anbindung an externe Sicherheitskomponenten wie Firewalls oder Virenschutz
- Anbindung an Verzeichnisdienste

Das NAC-Konzept SOLLTE alle technischen und organisatorischen Vorgaben beschreiben. Insbesondere SOLLTEN alle relevanten Prozesse und die Migration thematisiert werden.

Das NAC-Konzept SOLLTE regelmäßig geprüft und bei Bedarf aktualisiert werden.

NET.3.4.A5 Anpassung von Prozessen für Endgeräte bezüglich NAC (S)

Für die Endgeräte, die in die NAC-Lösung eingebunden werden, SOLLTE NAC in allen relevanten Prozessen angemessen berücksichtigt werden. Insbesondere SOLLTEN die Prozesse zu Inbetriebnahme, Austausch, Änderungen und Störungen angepasst werden.

Für Supplicant-Software, Konfiguration und Identitätsmerkmale (z. B. Zertifikate), die für NAC auf den Endgeräten erforderlich sind, SOLLTE ein Prozess festgelegt werden, um die Endgeräte zentral zu verwalten.

NET.3.4.A6 Festlegung von Notfallprozessen für NAC (S)

Wird die Wirkkette bei NAC gestört, SOLLTE erwogen werden, die Sicherheitsmechanismen von NAC temporär in angemessenem Umfang zu deaktivieren.

Bei den Notfallmaßnahmen, die im Notfallprozess festgelegt werden, SOLLTEN Produktivität und Informationssicherheit gegeneinander abgewogen werden. Dabei SOLLTEN die folgenden Optionen von Notfallmaßnahmen (RADIUS-down-Policies) betrachtet werden:

- Die bestehenden Verbindungen werden durch Mechanismen wie temporäre Aussetzung der Reauthentisierung beibehalten, jedoch werden alle neuen Anmeldeversuche abgelehnt, so dass das vorgesehene Sicherheitsniveau erhalten bleibt.
- Die dynamische Zuordnung wird für neue Anmeldeversuche ausgesetzt und stattdessen eine feste, vordefinierte Zuweisung von Netzsegmenten durch Access-Switches vorgenommen, so dass zumindest grundlegend kommuniziert werden kann.
- NAC wird auf den Access-Switches oder auf einzelnen Ports eines Access-Switches deaktiviert, so dass weiterhin uneingeschränkt kommuniziert werden kann.

RADIUS-down-Policies SOLLTEN mit den relevanten Sicherheitsrichtlinien der Institution abgestimmt werden.

NET.3.4.A7 Nutzung sicherer Authentisierungsverfahren (S)

Endgeräte SOLLTEN sichere Authentisierungsverfahren nach dem Stand der Technik verwenden. Endgeräte SOLLTEN automatisiert auf Basis von Zertifikaten oder Zugangskonten authentisiert werden.

Unsichere Authentisierungsverfahren SOLLTEN nur in begründeten Ausnahmefällen genutzt und die Entscheidung dokumentiert werden.

NET.3.4.A8 Festlegung der NAC-spezifischen Rollen und Berechtigungen für den RADIUS-Server (S)

Im Rollen- und Berechtigungskonzept für den RADIUS-Server SOLLTEN die verschiedenen Gruppen berücksichtigt werden, die wegen NAC auf einen RADIUS-Server zugreifen müssen, um diesen zu administrieren. Dies SOLLTE insbesondere dann sorgfältig geplant werden, wenn ein zentraler RADIUS-Server für die gesamte Institution bereitgestellt wird. Mindestens SOLLTEN die folgenden Gruppen mit NAC-spezifischem Zugriff auf den RADIUS-Server zusätzlich zum allgemeinen IT-Betrieb berücksichtigt werden:

- die jeweiligen Organisationseinheiten, die Access-Switches (RADIUS-Clients) für ihren Netzbereich administrieren
- die jeweiligen Zuständigen für Endgerätegruppen, die Identitäten (z. B. MAC-Adressen) ihrer entsprechenden Gruppen verwalten
- der First-Level-Support, der fehlerhafte RADIUS-Freigaben analysiert und gegebenenfalls die entsprechenden Freischaltungen anpasst

NET.3.4.A9 Festlegung eines angepassten NAC-Regelwerkes (S)

Für die NAC-Lösung SOLLTE ein NAC-Regelwerk definiert werden, das das NAC-Konzept umsetzt und festlegt, wie die Endgeräte auf das Netz zugreifen dürfen. Hierin SOLLTE für jedes Endgerät bzw. für jede Endgerätegruppe festgelegt werden, ob uneingeschränkt auf das Netz zugegriffen werden darf, ob der Zugriff verweigert wird oder ob nur Segmente mit eingeschränkten Kommunikationsmöglichkeiten erreichbar sind.

Im NAC-Regelwerk SOLLTE auch festgelegt werden, auf welcher Basis die Zugangskontrolle erfolgt. Hierfür SOLLTEN für alle Endgeräte die genutzten Authentisierungsmethoden und die Bedingungen für eine erfolgreiche Authentisierung festgelegt werden.

NET.3.4.A10 Sichere Nutzung von Identitäten (S)

Für die NAC-Authentisierung SOLLTEN individuelle Identitäten genutzt werden. Identitäten, die von mehr als einem Endgerät verwendet werden, SOLLTEN nur in begründeten Ausnahmefällen genutzt werden.

Alle Informationen, die für eine erfolgreiche Authentisierung benötigt werden, SOLLTEN nach aktuellem Stand der Technik vor unberechtigtem Zugriff abgesichert werden.

NET.3.4.A11 Sichere Konfiguration der NAC-Lösung (S)

Alle Komponenten der NAC-Lösung SOLLTEN sicher nach dem Stand der Technik konfiguriert werden. Hierfür SOLLTEN entsprechende Standard-Konfigurationen und Betriebshandbücher entwickelt und bereitgestellt werden.

Die vorgegebenen und umgesetzten Konfigurationen für die Komponenten der NAC-Lösung SOLLTEN regelmäßig überprüft und gegebenenfalls angepasst werden.

Auf Endgeräten SOLLTEN die Berechtigungen für die Benutzenden derart eingeschränkt werden, dass diese die Konfigurationsparameter für den Supplicant nicht manipulieren, den Supplicant nicht deaktivieren und die Schlüssel oder Passwörter für NAC nicht auslesen können.

Für Access-Switches oder für einzelne Ports von Access-Switches SOLLTE die NAC-Authentisierung nur in begründeten und zuvor festgelegten Ausnahmefällen deaktiviert werden. Hierfür SOLLTEN technische Maßnahmen genutzt werden, die gegebenenfalls durch organisatorische Maßnahmen ergänzt werden.

NET.3.4.A12 Monitoring der NAC-Lösung (S)

Die zentralen RADIUS-Server und alle Access-Switches mit Authenticator sowie alle weiteren zentralen Dienste, die für die NAC-Lösung essentiell sind, SOLLTEN in ein möglichst umfassendes und einheitliches Monitoring eingebunden werden. Ergänzend zum allgemeinen Monitoring gemäß OPS.1.1.1 *Allgemeiner IT-Betrieb* SOLLTEN alle NAC-spezifischen Parameter überwacht werden, die die Funktionalität der NAC-Lösung oder der entsprechenden Dienste sicherstellen.

Insbesondere SOLLTE die Verfügbarkeit des RADIUS-Protokolls überprüft werden. Hierfür SOLLTEN RADIUS-Anfragen an aktive Konten erzeugt werden, um die gesamte NAC-Wirkkette inklusive der externen Verzeichnisdienste zu prüfen.

Für die Access-Switches SOLLTE der Status von NAC in das Monitoring einbezogen werden, um ein Deaktivieren von NAC zu erkennen.

Abweichungen von definierten Zuständen und Grenzwerten SOLLTEN dem IT-Betrieb gemeldet werden.

NET.3.4.A13 Erstellung von Validierungsvorgaben für die NAC-Konfiguration (S)

Für die NAC-Lösung SOLLTEN Validierungsvorgaben erstellt werden, um sicherzustellen, dass die NAC-Komponenten das NAC-Konzept angemessen umsetzen. Die Validierungsvorgaben SOLLTEN insbesondere die unterschiedlichen Funktionsdetails für die verschiedenen NAC-Komponenten berücksichtigen.

Die Validierung SOLLTE als Soll-Ist-Vergleich regelmäßig sowie bei Bedarf für die zentralen NAC-Komponenten und die Access-Switches durchgeführt werden.

NET.3.4.A14 Umsetzung weiterer Maßnahmen bei Verwendung von MAC-Adress-Authentisierung (S)

Endgeräte, die nicht über eine sichere EAP-Methode authentisiert werden können und anhand ihrer MAC-Adresse identifiziert werden, SOLLTEN NICHT als vertrauenswürdige Endgeräte eingestuft werden. Der Netzzugang SOLLTE auf das notwendige Minimum beschränkt werden.

Hierfür SOLLTEN weitere Maßnahmen wie Nutzung von Kommunikationsbeschränkungen oder nachgelagertes Endgeräte-Profiling der Endgeräte-Aktivitäten umgesetzt werden.

NET.3.4.A15 Anbindung Virenschutz an NAC-Lösung (S)

Jedes Endgerät SOLLTE auf Schadsoftware geprüft werden, bevor es an das Netz der Institution angebunden wird und bevor es auf IT-Systeme der Institution zugreift. Hierfür SOLLTE für die NAC-Endgeräte ein geeigneter Virenschutz mit der NAC-Authentisierung und Autorisierung gekoppelt werden.

Falls das Virenschutzprogramm Schadsoftware meldet, SOLLTE die NAC-Lösung mit geeigneten Maßnahmen reagieren.

NET.3.4.A16 Protokollierung der Ereignisse (S)

Ergänzend zu OPS.1.1.5 *Protokollierung* SOLLTEN Statusänderungen an NAC-Komponenten sowie alle relevanten NAC-spezifischen, gegebenenfalls sicherheitskritischen Ereignisse protokolliert werden. Zusätzlich SOLLTEN alle schreibenden Konfigurationszugriffe auf die zentralen NAC-Komponenten protokolliert werden.

Es SOLLTE festgelegt werden, welche Protokollierungsdaten mit welchen Details erfasst und welche Daten auf einer zentralen Protokollierungsinstanz zusammengeführt werden.

Protokollierungsdaten SOLLTEN NUR über sichere Kommunikationswege übertragen werden.

Sicherheitskritische Ereignisse wie RADIUS-down oder eine ungewöhnliche Anzahl von RADIUS-Anfragen SOLLTEN zu einem automatischen Alarm führen.

NET.3.4.A17 Positionierung des RADIUS-Servers im Management-Bereich (S)

Der RADIUS-Server SOLLTE in einem geschützten Netzsegment innerhalb des Management-Bereichs (siehe NET.1.1 *Netzarchitektur und -design*) positioniert werden. Kommunikationsanfragen an den RADIUS-Server SOLLTEN nur von vertrauenswürdigen Quellen zugelassen werden. Diese SOLLTEN auf ein Minimum eingeschränkt werden.

Der RADIUS-Server SOLLTE NICHT direkt mit Endgeräten kommunizieren, sondern ausschließlich über den Authenticator auf den Access-Switches. Anfragen der Access-Switches SOLLTEN nur aus dem gemeinsamen Management-Netzsegment akzeptiert werden.

NET.3.4.A18 Dokumentation der NAC-Lösung (S)

Die NAC-Lösung mit allen NAC-Komponenten SOLLTE geeignet dokumentiert werden.

Aus der Dokumentation SOLLTE mindestens hervorgehen, auf welchen Komponenten und Endgeräten NAC mit welchen Parametern genutzt wird und welche Abhängigkeiten zwischen den Komponenten existieren. Auch SOLLTE das Regelwerk für Authentisierung und Autorisierung, das in Software-Code vorliegt, ergänzend in vereinfachter, verständlicher Form dokumentiert werden. Darüber hinaus SOLLTE die Konfiguration aller NAC-Komponenten, gegebenenfalls kategorisiert, umfassend dokumentiert werden.

Die Dokumentation SOLLTE bei jeder Änderung fortgeschrieben und stets aktuell gehalten werden. Die Aktualität der Dokumentation SOLLTE regelmäßig und bei Bedarf geprüft werden.

NET.3.4.A19 Ordnungsgemäße Verwaltung von Identitäten zur Authentisierung (S)

Alle Identitäten, die via NAC einen Zugang zum Netz der Institution ermöglichen, SOLLTEN geeignet geschützt und verwaltet werden. Hierzu SOLLTEN mindestens die folgenden Punkte festgelegt werden:

- Handhabung und Schutz von Zertifikaten
- Prüfen, Sperren und Löschen von nicht mehr genutzten Identitäten

- Prozess und Schnittstellen zur Sperrung einer Identität

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.3.4.A20 Einsatz von MACsec (H)

Für jedes Datenpaket SOLLTE die Datenintegrität gewährleistet werden. Darüber hinaus SOLLTE erwogen werden, diese Daten zu verschlüsseln. Hierfür SOLLTE MACsec gemäß IEEE 802.1AE genutzt werden.

Access-Switches und Endgeräte, die MACsec nicht unterstützen oder für die MACsec nicht eingerichtet werden soll, SOLLTEN erfasst werden. Für diese SOLLTE regelmäßig überprüft werden, ob die Ausschlussgründe noch gelten.

NET.3.4.A21 Einsatz von Endgerätekonformitätsprüfung (H)

Bevor ein Endgerät an das Netz der Institution angebunden wird und bevor es auf IT-Systeme der Institution zugreift, SOLLTE geprüft werden, ob es den Konformitätsvorgaben der Institution genügt (Compliance Check).

Für jedes Endgerät SOLLTE festgelegt werden, welche Vorgaben das Endgerät einzuhalten hat. Endgeräte, die nicht den Konformitätsvorgaben der Institution genügen, SOLLTEN nur stark eingeschränkt auf das Netz der Institution zugreifen dürfen.

Die NAC-Lösung SOLLTE mit einem Werkzeug zur Konformitätsprüfung verbunden werden, das eine Bewertung des Zustands der Endgeräte vornimmt und an die NAC-Lösung meldet. Auf dieser Basis SOLLTE die NAC-Lösung steuern, wie die Endgeräte auf das Netz zugreifen dürfen.

NET.3.4.A22 NAC-Autorisierung mit Mikrosegmenten (H)

Endgeräte mit ähnlichem Anforderungsprofil und identischem Schutzbedarf SOLLTEN via NAC getrennten Netzsegmenten zugewiesen werden.

Darüber hinaus SOLLTE erwogen werden, ob mit NAC eine Mikrosegmentierung der zu autorisierenden Endgeräte umgesetzt wird.

NET.3.4.A23 Einsatz von autarken RADIUS-Servern für unterschiedliche Netzbereiche und Funktionen (H)

Für NAC SOLLTEN dedizierte und autarke RADIUS-Server eingesetzt werden. Weitere Funktionen wie VPN-Zugriffsregelung SOLLTEN NICHT gemeinsam mit NAC-Funktionen auf einem gemeinsamen RADIUS-Server realisiert werden.

Zusätzlich SOLLTE erwogen werden, dedizierte und autarke RADIUS-Server für unterschiedliche Netze bereitzustellen. Hier SOLLTEN insbesondere getrennte RADIUS-Server erwogen werden, um Office- und Produktions-Endgeräte oder LAN- und WLAN-Endgeräte getrennt abzusichern.

Darüber hinaus SOLLTE erwogen werden, für einzelne Netz- oder Funktionsbereiche eigenständige RADIUS-Server einzurichten.

NET.3.4.A24 Nutzung sicherer Protokolle zwischen NAC-Komponenten (H)

Für die Kommunikation zwischen den zentralen NAC-Komponenten SOLLTEN grundsätzlich Protokolle verwendet werden, die nach dem Stand der Technik als sicher gelten. Für die Kommunikation zwischen dem RADIUS-Server und einem gegebenenfalls genutzten Verzeichnisdienst SOLLTEN nur sichere Protokolle eingesetzt werden.

Darüber hinaus SOLLTE auch geprüft werden, ob für die Kommunikation zwischen dem RADIUS-Server und Access-Switches sichere Protokolle eingesetzt werden sollen.

NET.3.4.A25 Einbindung der NAC-Lösung in ein Sicherheitsmonitoring (H)

Die NAC-Lösung SOLLTE in ein Sicherheitsmonitoring eingebunden werden. Dies SOLLTE zumindest für die zentralen NAC-Komponenten und für die weiteren zentralen Dienste, die von der NAC-Lösung genutzt werden, umgesetzt werden.

NAC-spezifische Sicherheitsereignisse (z. B. häufige Zurückweisung von Anfragen oder die Mehrfachverwendung von Identitäten) SOLLTEN in eine Alarmierung übernommen werden.

Wird für die IT der Institution ein System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen eingesetzt, SOLLTEN die zentralen NAC-Komponenten sowie gegebenenfalls die weiteren zentralen Dienste hierin eingebunden werden.

NET.3.4.A26 Hochverfügbarkeit der zentralen NAC-Komponenten (H)

Die zentralen NAC-Komponenten SOLLTEN redundant ausgelegt werden. Alle weiteren zentralen Dienste, die für die Funktionsfähigkeit der NAC-Lösung essentiell sind, SOLLTEN auch hochverfügbar ausgelegt sein.

Die für die Hochverfügbarkeit relevanten Parameter SOLLTEN in Monitoring und Protokollierung integriert werden. Statusänderungen und Warnmeldungen SOLLTEN regelmäßig kontrolliert und gegebenenfalls in eine Alarmierung einbezogen werden.

Die RADIUS-down-Policies, mit denen eine Kommunikation auch bei ausgefallenem RADIUS-Dienst gewährleistet wird, SOLLTEN das Sicherheitsniveau des Netzes NICHT senken.

NET.3.4.A27 Prüfung der Notwendigkeit für MAC-Adress-Authentisierung (H)

Eine Authentisierung über MAC-Adressen SOLLTE nur dort genutzt werden, wo dies technisch unumgänglich ist und die Sicherheitsrichtlinien dies zulassen.

Es SOLLTE im Vorfeld geprüft werden, ob solche Ausnahmefälle notwendig sind. Ist dies der Fall, SOLLTEN die Ausnahmefälle auf den minimalen Einsatzbereich eingeschränkt werden.

Die Begründung und das Ergebnis der Prüfung SOLLTEN dokumentiert werden. Sie SOLLTEN regelmäßig und bei Bedarf nochmals verifiziert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein NET.3.4 *Network Access Control* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.4.1 TK-Anlagen

1. Beschreibung

1.1. Einleitung

Mit einer Telekommunikationsanlage, kurz TK-Anlage, können die Telefone einer Institution intern verbunden und extern an ein öffentliches Telefonnetz angeschlossen werden. Durch die zunehmende Verzahnung von IT und Telekommunikation können TK-Anlagen dabei sowohl analog als auch IP-basiert aufgebaut sein. Hybrid-Anlagen sind eine Kombination aus einer klassischen Telekommunikationslösung und einem VoIP-System. Mit einer Hybrid-Anlage können klassische digitale und analoge Telefonie sowie VoIP gleichzeitig betrieben werden.

Neben der Sprachtelefonie können, abhängig von den angeschlossenen Endgeräten, weitere Dienste genutzt werden. So ist es möglich, mittels TK-Anlagen Daten, Texte, Grafiken und Bewegtbilder zu übertragen. Die Informationen können dabei analog oder digital über drahtgebundene oder drahtlose Übertragungsmedien weitergeleitet werden. Je nach Anbindung und genutzten Datennetzen können in einer Institution verschiedenste Telekommunikationsanlagen eingesetzt werden.

1.2. Zielsetzung

In diesem Baustein werden die für die TK-Anlagen sowie die entsprechenden Anteile von Hybrid-Anlagen spezifischen Gefährdungen und Anforderungen betrachtet. Das Ziel des Bausteins ist der Schutz der Informationen, die über TK-Anlagen übermittelt werden sowie der Schutz der Anlage vor Fremdeingriffen und Manipulationen.

1.3. Abgrenzung und Modellierung

Der Baustein NET.4.1 *TK-Anlagen* ist auf jede TK-Anlage anzuwenden.

Dieser Baustein behandelt die Gefährdungen und Anforderungen, die spezifisch für eine TK-Anlage sowie die entsprechenden Teile einer Hybrid-Anlage sind. Themen, die über die TK-Anlage hinausgehen, wie zum Beispiel Gefährdungen und Anforderungen für einzelne VoIP-Implementierungen, sowie extern bereitgestellte Dienste werden in den entsprechenden Bausteinen des IT-Grundschutz-Kompendiums gesondert behandelt.

Die Sicherheitsaspekte von VoIP-Komponenten und der Sprachübertragung über VoIP werden im Baustein NET.4.2 *VoIP* näher betrachtet.

TK-Anlagen sollten grundsätzlich mit berücksichtigt werden, wenn die Bausteine ORP.4 *Identitäts- und Berechtigungsmanagemen*t, OPS.1.2.5 *Fernwartung*, CON.3 *Datensicherungskonzept* und OPS.1.1.5 *Protokollierung* umgesetzt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.4.1 *TK-Anlagen* von besonderer Bedeutung.

2.1. Abhören von TK-Anlagen

Wenn Telefongespräche oder Daten über eine TK-Anlage unverschlüsselt übertragen werden, besteht grundsätzlich die Gefahr, dass Angreifende Informationen mithören oder mitlesen. So könnten sie beispielsweise die Telefonkabel direkt anzapfen oder an einer zwischen den Gesprächsteilnehmenden vermittelnden TK-Anlage lauschen.

Bei vielen TK-Anlagen können Anrufende Empfangenden Nachrichten hinterlassen, wenn diese zum Zeitpunkt des Anrufs telefonisch nicht erreichbar sind. Einige Anrufbeantworter, vor allem bei VoIP-Anlagen, verschicken diese Informationen als Audio-Datei in einer E-Mail. Der Inhalt dieser E-Mail könnte direkt von Angreifenden abgefangen und angehört werden.

Des Weiteren könnten Gespräche durch das Aktivieren von gesperrten, in Deutschland zum Teil unzulässigen, Leistungsmerkmalen von Dritten mitgehört werden. Ein Beispiel hierfür ist die Zeugenschaltung. Eine derartige Aktivierung erfordert zwar genauere Systemkenntnisse, ist aber aufgrund vieler frei verfügbarer Hinweise im Internet häufig kein großes Hindernis.

2.2. Abhören von Räumen über TK-Anlagen

Über Mikrofone in Endgeräten können grundsätzlich auch Räume abgehört werden. Dabei werden zwei Varianten unterschieden:

Bei der ersten Variante können Endgeräte, wenn entsprechende Funktionen implementiert sind, aus dem öffentlichen Netz oder über das LAN dazu veranlasst werden, die eingebauten Mikrofone zu aktivieren. Ein bekanntes Beispiel hierfür ist die sogenannte „Baby-Watch-Funktion“ von Telefonen oder Anrufbeantwortern.

Bei der zweiten Variante kann das Leistungsmerkmal „direktes Ansprechen“ in Kombination mit der Option „Freisprechen“ missbraucht werden. Die auf diese Weise realisierbare Funktion einer Wechselsprechanlage kann unter gewissen Umständen auch zum Abhören eines Raumes ausgenutzt werden.

2.3. Gebührenbetrug

Gebührenbetrug im Zusammenhang mit Daten- oder Telekommunikationsdiensten hat das Ziel, die Kosten für geführte Telefonate oder Datentransfers auf Dritte zu übertragen. Eine TK-Anlage lässt sich auf verschiedene Weise von außen manipulieren. Zum einen können Angreifende versuchen, vorhandene Leistungsmerkmale für den Gebührenbetrug zu missbrauchen. Zu diesen Leistungsmerkmalen zählen beispielsweise aus der Ferne umprogrammierbare Rufumleitungen oder Dial-in-Optionen. Zum anderen können die Berechtigungen so vergeben werden, dass kommende „Amtsleitungen“ abgehende „Amtsleitungen“ belegen. Auf diese Weise können Anrufenden bei Anwahl einer bestimmten Rufnummer auf Kosten des TK-Anlagenbetreibenden von außen automatisch wieder mit dem „Amt“ verbunden werden.

Darüber hinaus können nicht nur Angreifende von außen, sondern auch die Beschäftigten innerhalb einer Institution mit den Gebühren betrügen. So können sie etwa versuchen, auf Kosten der Institution oder der anderen Beschäftigten zu telefonieren, indem sie z. B. von fremden Apparaten telefonieren, fremde Berechtigungscodes (Passwörter) auslesen oder persönliche Berechtigungen verändern.

2.4. Missbrauch frei zugänglicher Telefonanschlüsse

Oft werden Telefone betrieben, die keinen Benutzenden persönlich zugeordnet sind. Einige dieser Telefone, wie zum Beispiel solche in Druckerräumen, sind nur einem eingeschränkten Personenkreis zugänglich. Andererseits sind Telefone häufig in Bereichen zu finden, die für Besuchende frei zugänglich sind. Dazu zählen beispielsweise Parkhäuser oder Bereiche vor Zugangskontrollsystemen. Besitzen diese Telefone ein elektronisches Telefonbuch, in dem interne Telefonnummern gespeichert sind, könnten diese Nummern ungewollt nach außen gelangen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.4.1 *TK-Anlagen* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Fachverantwortliche
Weitere Zuständigkeiten	IT-Betrieb, Vorgesetzte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.4.1.A1 Anforderungsanalyse und Planung für TK-Anlagen (B) [IT-Betrieb]

Vor der Beschaffung oder Erweiterung einer TK-Anlage MUSS eine Anforderungsanalyse durchgeführt werden. Im Rahmen dieser Analyse MUSS festgelegt werden, welche Funktionen die TK-Anlage bieten soll. Hierbei MÜSSEN neben der Ausprägung der TK-Anlage auch die Anzahl der benötigten Verbindungen und Anschlüsse festgelegt werden. Auch eine mögliche Erweiterbarkeit und grundlegenden Sicherheitsfunktionen MÜSSEN bei der Planung betrachtet werden. Darüber hinaus MÜSSEN je nach Bedarf Support- und Wartungsverträge für die TK-Anlage berücksichtigt werden. Basierend auf den ermittelten Anforderungen MUSS anschließend der Einsatz der TK-Anlage geplant und dokumentiert werden. Die zuvor ermittelten Anforderungen und die Planung MÜSSEN mit den entsprechenden IT-Zuständigen abgestimmt werden.

NET.4.1.A2 Auswahl von TK-Diensteanbietenden (B) [IT-Betrieb]

Um mit Personen telefonieren zu können, deren Telefone nicht an die institutionseigene TK-Anlage angeschlossen sind, MUSS ein TK-Diensteanbieter oder TK-Diensteanbieterin beauftragt werden. Dabei MÜSSEN die Anforderungen an die TK-Anlage, die Sicherheitsrichtlinie sowie vertragliche und finanzielle Aspekte berücksichtigt werden. Alle vereinbarten Leistungen MÜSSEN eindeutig schriftlich festgehalten werden.

NET.4.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.4.1.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.4.1.A5 Protokollierung bei TK-Anlagen (B)

Bei TK-Anlagen MÜSSEN geeignete Daten erfasst und bei Bedarf ausgewertet werden. Protokolliert werden MÜSSEN zusätzlich alle systemtechnischen Eingriffe, die Programmveränderungen beinhalten, sowie Auswertungsläufe, Datenübermittlungen und Datenzugriffe. Alle Administrationsarbeiten an der TK-Anlage MÜSSEN ebenfalls protokolliert werden. Die protokollierten Informationen SOLLTEN regelmäßig kontrolliert werden.

3.2. Standard-Anforderungen

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

NET.4.1.A6 Erstellung einer Sicherheitsrichtlinie für TK-Anlagen (S) [IT-Betrieb]

Basierend auf der institutionsweiten Sicherheitsrichtlinie SOLLTE eine eigene Sicherheitsrichtlinie für die TK-Anlage erstellt werden. Diese Sicherheitsrichtlinie für die TK-Anlage SOLLTE grundlegende Aussagen zur Vertraulichkeit, Verfügbarkeit und Integrität beinhalten. Sie SOLLTE allen Personen, die an der Beschaffung, dem Aufbau, der Umsetzung und dem Betrieb der TK-Anlage beteiligt sind, bekannt sein und die Grundlage für deren Arbeit darstellen. Die zentralen sicherheitstechnischen Anforderungen an die TK-Anlage sowie das zu erreichende Sicherheitsniveau SOLLTEN in der institutionsweite Sicherheitsrichtlinie aufgenommen werden.

NET.4.1.A7 Geeignete Aufstellung der TK-Anlage (S)

Die TK-Anlage SOLLTE in einem geeigneten Raum untergebracht sein. Die Schnittstellen an der TK-Anlage, besonders nicht genutzte Schnittstellen, SOLLTEN geeignet geschützt werden.

NET.4.1.A8 Einschränkung und Sperrung nicht benötigter oder sicherheitskritischer Leistungsmerkmale (S)

Der Umfang der verfügbaren Leistungsmerkmale SOLLTE auf das notwendige Minimum beschränkt werden. Nur die benötigten Leistungsmerkmale SOLLTEN freigeschaltet werden. Die nicht benötigten oder wegen ihres Missbrauchspotenzials als kritisch eingestuften Leistungsmerkmale SOLLTEN so weit wie möglich an der zentralen Anlage abgeschaltet werden. Zusätzliche Schutzmaßnahmen SOLLTEN für die auf den Endgeräten gespeicherten und abrufbaren vertraulichen Daten ergriffen werden.

NET.4.1.A9 Schulung zur sicheren Nutzung von TK-Anlagen (S) [Vorgesetzte]

Die Benutzenden der TK-Anlage SOLLTEN in die korrekte Verwendung von Diensten und Geräten eingewiesen werden. Den Benutzenden der TK-Anlage SOLLTEN alle notwendigen Unterlagen zur Bedienung der entsprechenden Endgeräte zur Verfügung gestellt werden. Sämtliche Auffälligkeiten und Unregelmäßigkeiten der TK-Anlage SOLLTEN den entsprechenden Verantwortlichen gemeldet werden.

NET.4.1.A10 Dokumentation und Revision der TK-Anlagenkonfiguration (S) [IT-Betrieb]

Die TK-Anlagenkonfiguration SOLLTE geeignet dokumentiert und fortgeschrieben werden. Die TK-Anlagenkonfiguration SOLLTE in regelmäßigen Abständen überprüft werden. Das Ergebnis der

Prüfung SOLLTE zumindest den Informationssicherheitsbeauftragten, den Fachverantwortlichen und anderen verantwortlichen Mitarbeitenden vorgelegt werden.

NET.4.1.A11 Außerbetriebnahme von TK-Anlagen und -geräten (S) [IT-Betrieb]

Die Aussonderung von TK-Anlagen und angeschlossenen TK-Geräten SOLLTE in der Sicherheitsrichtlinie berücksichtigt werden. Alle Daten, die auf TK-Anlagen oder Endgeräten gespeichert sind, SOLLTEN vor der Aussonderung sicher gelöscht werden.

NET.4.1.A12 Datensicherung der Konfigurationsdateien (S)

Die Konfigurations- und Anwendungsdaten der eingesetzten TK-Anlage SOLLTEN bei der Ersteinrichtung und anschließend regelmäßig gesichert werden, insbesondere nachdem sich diese geändert haben. Es SOLLTE regelmäßig geprüft und dokumentiert werden, ob die Sicherungen der TK-Anlagen auch tatsächlich als Basis für eine Systemwiederherstellung genutzt werden können.

Es SOLLTE ein Datensicherungskonzept für TK-Anlagen erstellt und mit den allgemeinen Konzepten der Datensicherung für Server und Netzkomponenten abgestimmt werden.

NET.4.1.A13 Beschaffung von TK-Anlagen (S)

Bei der Beschaffung von TK-Anlagen SOLLTEN die Ergebnisse der Anforderungsanalyse und der Planung miteinbezogen werden. Bei der Beschaffung einer TK-Anlage SOLLTE beachtet werden, dass sie neben digitalen auch analoge Teilnehmeranschlüsse anbieten sollte. Darüber hinaus SOLLTEN vorhandene Kommunikationssysteme und -komponenten bei der Beschaffung berücksichtigt werden.

NET.4.1.A14 Notfallvorsorge für TK-Anlagen (S)

Es SOLLTE ein Notfallplan für die TK-Anlage erstellt werden. Dieser SOLLTE in das Notfallkonzept der Institution integriert werden. Es SOLLTEN regelmäßig Notfallübungen bezüglich der TK-Anlagen durchgeführt werden.

NET.4.1.A15 Notrufe bei einem Ausfall der TK-Anlage (S)

Es SOLLTE sichergestellt werden, dass auch bei einem Ausfall der TK-Anlage Notrufe aus der Institution abgesetzt werden können. Die Notrufmöglichkeiten SOLLTEN von allen Räumen aus auf ausreichend kurzen Wegen erreichbar sein.

NET.4.1.A16 Sicherung von Endgeräten in frei zugänglichen Räumen (S)

Der Funktionsumfang der Endgeräte, die in frei zugänglichen Räumen aufgestellt werden sollen, SOLLTE eingeschränkt werden. Ist dies nicht möglich, SOLLTE das Endgerät in geeigneter Weise vor unbefugtem Zugriff geschützt werden.

NET.4.1.A17 Wartung von TK-Anlagen (S)

Die Geräte zur Wartung und Konfiguration der TK-Anlage SOLLTEN mit Passwörtern bzw. PINs abgesichert sein.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.4.1.A18 Erhöhter Zugangsschutz (H)

Die TK-Anlage SOLLTE in einem separaten sowie geeignet gesicherten Raum untergebracht sein. Der Zutritt und Zugang zur TK-Anlage SOLLTE nur einem eingeschränkten Personenkreis möglich sein. Externe SOLLTEN NUR beaufsichtigt Zugang zur Anlage erhalten.

NET.4.1.A19 Redundanter Anschluss (H)

Der Anschluss der TK-Anlage SOLLTE redundant ausgelegt sein. Bei IP-basierten TK-Anlagen SOLLTE ein zusätzlicher PSTN-Anschluss vorhanden sein.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat im Rahmen der Technischen Leitlinien die „BSI-TL-02013 für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf“ veröffentlicht.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.4.2 VoIP

1. Beschreibung

1.1. Einleitung

Voice over IP (VoIP) bezeichnet das Telefonieren über Datennetze, insbesondere über das Internet. Um Signalisierungsinformationen zu übertragen, beispielsweise bei einem Anruf, werden spezielle Signalisierungsprotokolle eingesetzt. Die eigentlichen Nutzdaten wie Sprache oder Video werden mit Hilfe eines Medientransportprotokolls übermittelt. Beide Protokolle werden jeweils benötigt, um eine Multimediaverbindung aufzubauen und aufrechtzuerhalten. Bei einigen Verfahren wird nur ein Protokoll sowohl für die Signalisierung als auch für den Medientransport benötigt.

1.2. Zielsetzung

Dieser Baustein betrachtet die Sicherheitsaspekte der Endgeräte und Vermittlungseinheiten (Middleware) von VoIP. Die hier beschriebenen Komponenten gleichen hinsichtlich ihrer Funktionalität den im Baustein NET 4.1 *TK-Anlagen* beschriebenen Telekommunikationsanlagen.

1.3. Abgrenzung und Modellierung

Der Baustein NET.4.2 *VoIP* ist auf alle Kommunikationsnetze anzuwenden, in denen VoIP eingesetzt wird. Da VoIP über Datennetze betrieben wird, sind zusätzlich zu diesem Baustein die Anforderungen der Bausteine NET.1.1 *Netzarchitektur- und Design* oder NET.3.2 *Firewall* geeignet mit zu berücksichtigen.

In diesem Baustein werden die Sicherheitsaspekte von VoIP-Komponenten und der Sprachübertragung über VoIP betrachtet. Tauschen leitungsvermittelnde TK-Anlagen Informationen untereinander über ein Datennetz aus, ist dieser Baustein ebenfalls anzuwenden.

Die spezifischen Gefährdungen und Anforderungen von klassischen TK-Anlagen sowie Hybrid-Anlagen werden in dem Baustein NET 4.1 *TK-Anlagen* betrachtet.

Oft wird VoIP-Software nicht auf eigens dafür vorgesehene Hardware betrieben, sondern auf Standard-IT. Werden Softphones auf Clients installiert, sollten die Anforderungen des Bausteins SYS.2.1 *Allgemeiner Client* sowie der betriebssystemspezifischen Bausteine berücksichtigt werden. Wird Software für VoIP auf Servern betrieben, sollten neben den Anforderungen der betriebssystemspezifischen Bausteine die Anforderungen des Bausteins SYS.1.1 *Allgemeiner Server* erfüllt werden.

VoIP sollte grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement*, OPS.1.1.5 *Protokollierung*, sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* mit berücksichtigt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.4.2 *VoIP* von besonderer Bedeutung.

2.1. Fehlerhafte Konfiguration der VoIP-Middleware

Eine VoIP-basierte Telefonanlage kann in ähnlicher Weise von Fehlkonfigurationen betroffen sein wie eine leitungsvermittelnde Telefonlösung. So könnten beispielsweise Telefonbenutzenden falsche Telefonnummern zugeordnet werden oder die gesamte Telefoninfrastruktur könnte ausfallen. Auch tendenziell unkritische Fehler, wie ein falsch geschriebener Name im Telefonbuch, können nicht ausgeschlossen werden.

Wird mittels VoIP kommuniziert, sind in der Regel mehrere IT-Systeme beteiligt. Wird SIP als Initialisierungsprotokoll eingesetzt, werden meist Systeme wie *Registrare*, *SIP-Proxy-Server* und *Location-Server* für die Kommunikation benötigt. Ändert sich die VoIP-Infrastruktur, müssen alle IT-Systeme angepasst werden. Dadurch können leicht Konfigurationsfehler entstehen. Auch wenn sich alle Dienste auf einem Server befinden, müssen diese häufig einzeln konfiguriert werden. Wird nur ein System fehlerhaft geändert, kann die gesamte Telefoninfrastruktur möglicherweise nicht mehr genutzt werden.

2.2. Fehlerhafte Konfiguration der VoIP-Komponenten

Unabhängig davon, ob es sich bei VoIP-Komponenten um dedizierte Hardware („Appliances“) oder softwarebasierte Systeme handelt, ist die Konfiguration entscheidend für die fehlerfreie Funktion des Systems. Neben den Einstellungen zur Signalisierung, die bei der Planung festgelegt wurden, spielt das Übertragungsverfahren für die Medienströme eine wichtige Rolle. Durch ein Kompressionsverfahren kann die Größe der Datenpakete mit den Sprachinformationen verkleinert werden.

Durch die fehlerhafte Konfiguration des Übertragungsverfahrens können Probleme bei der Übertragung auftreten. Wird ein ungeeignetes Verfahren eingesetzt und werden Sprachinformationen zu stark komprimiert, verschlechtert sich oft die Sprachqualität. Wird hingegen ein Verfahren gewählt, das eine zu geringe Kompression vornimmt, wird der Nachrichtenstrom nicht ausreichend vermindert und das Datennetz kann überlastet werden.

2.3. Abhören von Telefongesprächen

Wenn Telefongespräche oder Daten unverschlüsselt übertragen werden, könnten Angreifende grundsätzlich Informationen mithören oder mitlesen. So könnten sie beispielsweise die Telefonkabel direkt anzapfen oder an einer zwischen den Gesprächsteilnehmern vermittelnden TK-Anlage lauschen. Bei VoIP können Telefongespräche und Datenübertragungen sogar einfacher als bei klassischen TK-Anlagen abgehört werden. Alle Sprachinformationen werden innerhalb eines Medienstroms, beispielsweise mit dem Realtime Transport Protocol (RTP), übertragen. Durch Techniken wie Spoofing und Sniffing stehen bei VoIP den Angreifenden auch alle Möglichkeiten von Angriffen in Datennetzen zur Verfügung.

Bei vielen TK-Anlagen können Anrufende den Empfangenden Nachrichten hinterlassen, wenn diese zum Zeitpunkt des Anrufs telefonisch nicht erreichbar sind. Einige Anrufbeantworter, vor allem bei VoIP-Anlagen, verschicken diese Informationen als Audio-Datei in einer E-Mail. Der Inhalt dieser E-Mail könnte direkt von einem Angreifenden abgefangen und angehört werden.

2.4. Missbrauch frei zugänglicher Telefonanschlüsse

Oft werden Telefone betrieben, die keinen Benutzenden persönlich zugeordnet sind. Einige dieser Telefone, wie zum Beispiel solche in Druckerräumen, sind nur einem eingeschränkten Personenkreis zugänglich. Andererseits sind Telefone häufig in Bereichen zu finden, die für Besuchende frei zugänglich sind. Dazu zählen beispielsweise Parkhäuser oder Bereiche vor Zugangskontrollsystemen. Besitzen diese Telefone ein elektronisches Telefonbuch, in dem interne Telefonnummern gespeichert sind, könnten diese Nummern ungewollt nach außen gelangen.

Beim Einsatz von VoIP-Telefonen in frei zugänglichen Bereichen können weitere Aspekte relevant sein. Denn sie haben einen hohen Software-Anteil und werden häufig in Datennetzen betrieben, die auch für andere IT-Anwendungen genutzt werden. Angreifende könnten deshalb durch den direkten Zugriff auf Geräteinformationen versuchen, Schwachstellen in der VoIP-Software auszunutzen oder selbst schädliche Software zu installieren.

VoIP-Telefone müssen an ein Datennetz angeschlossen sein. Angreifende könnten an diesen Netzanschluss ein mobiles IT-System anschließen und so unter Umständen auf das von außen durch eine Firewall geschützte interne Netz zugreifen. Diesen Zugang können sie möglicherweise für Angriffe auf die Vertraulichkeit, Integrität und Verfügbarkeit ausnutzen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.4.2 *VoIP* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.4.2.A1 Planung des VoIP-Einsatzes (B)

Die Bedingungen, unter denen VoIP eingesetzt werden soll, MÜSSEN festgelegt werden. Es MUSS unter anderem entschieden werden, ob vollständig oder partiell auf VoIP umgestiegen werden soll. Besondere Anforderungen an die Verfügbarkeit von VoIP oder an die Vertraulichkeit und Integrität der Telefonate bzw. der Signalisierungsinformationen SOLLTEN vorab ermittelt werden. Geeignete Signalisierungs- und Medientransportprotokolle MÜSSEN vor dem Einsatz ausgewählt werden.

Es SOLLTE entschieden werden, ob und wie die VoIP-Infrastruktur an öffentliche (Daten-)Netze angebunden werden soll. Die Kapazitäten und das Design von vorhandenen Datennetzen SOLLTEN bei der Planung berücksichtigt werden.

NET.4.2.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.4.2.A3 Sichere Administration und Konfiguration von VoIP-Endgeräten (B)

Nicht benötigte Funktionen der Endgeräte MÜSSEN deaktiviert werden. Die Konfigurationseinstellungen DÜRFEN NICHT unberechtigt geändert werden. Alle Sicherheitsfunktionen der Endgeräte SOLLTEN vor dem produktiven Einsatz getestet werden. Die eingesetzten Sicherheitsmechanismen und die verwendeten Parameter SOLLTEN dokumentiert werden.

NET.4.2.A4 Einschränkung der Erreichbarkeit über VoIP (B)

Es MUSS entschieden werden, wie externe Gesprächspartner und -partnerinnen auf die VoIP-Architektur zugreifen können. Es MUSS verhindert werden, dass IT-Systeme aus unsicheren Netzen direkte Datenverbindungen auf die VoIP-Komponenten der Institution aufbauen können. Wenn alle ein- und ausgehenden Verbindungen über ein zentrales IT-System abgewickelt werden sollen, SOLLTE sichergestellt werden, dass alle Signalisierungs- und Sprachinformationen zwischen dem öffentlichen und dem privaten Datennetz nur über dieses autorisierte IT-System ausgetauscht werden.

NET.4.2.A5 Sichere Konfiguration der VoIP-Middleware (B)

Die VoIP-Komponenten MÜSSEN so konfiguriert sein, dass sie den Schutzbedarf angemessen erfüllen. Die Default-Konfigurationen der VoIP-Middleware MÜSSEN vor der produktiven Inbetriebnahme angepasst werden. Alle Installations- und Konfigurationsschritte SOLLTEN so dokumentiert werden, dass die Installation und Konfiguration durch sachkundige Dritte anhand der Dokumentation nachvollzogen und wiederholt werden können. Alle nicht benötigten Dienste der VoIP-Middleware MÜSSEN deaktiviert werden.

NET.4.2.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2. Standard-Anforderungen

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

NET.4.2.A7 Erstellung einer Sicherheitsrichtlinie für VoIP (S)

Die zentralen sicherheitstechnischen Anforderungen an VoIP sowie das zu erreichende Sicherheitsniveau SOLLTEN in der institutionsweiten Sicherheitsrichtlinie aufgenommen werden. In dieser Sicherheitsrichtlinie SOLLTEN alle allgemeinen sicherheitstechnischen Vorgaben konkretisiert werden. Außerdem SOLLTEN in der Richtlinie die Vorgaben für den Betrieb und die Nutzung der VoIP-Komponenten geregelt sein. Hierbei SOLLTEN auch die verschiedenen VoIP-Funktionen, wie zum Beispiel Voicemails, betrachtet werden. Die VoIP-Sicherheitsrichtlinie SOLLTE allen beteiligten Personen und Gruppen zugänglich und bekannt sein.

NET.4.2.A8 Verschlüsselung von VoIP (S)

Es SOLLTE entschieden werden, ob und welche Sprach- und Signalisierungsinformationen verschlüsselt werden sollen. Generell SOLLTEN alle VoIP-Datenpakete, die das gesicherte LAN verlassen, durch geeignete Sicherheitsmechanismen geschützt werden. Die Benutzenden SOLLTEN über die Nutzung der VoIP-Verschlüsselung informiert werden.

NET.4.2.A9 Geeignete Auswahl von VoIP-Komponenten (S)

Bevor VoIP-Komponenten beschafft werden, SOLLTE eine Anforderungsliste erstellt werden. Anhand der Anforderungsliste SOLLTEN die am Markt erhältlichen Produkte bewertet werden. Diese Anforderungsliste SOLLTE alle Merkmale zur Erreichung des angestrebten Sicherheitsniveaus umfassen. Es SOLLTE geregelt werden, wie die am Markt erhältlichen Produkte gemäß der Anforderungsliste bewertet werden können.

NET.4.2.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

NET.4.2.A11 Sicherer Umgang mit VoIP-Endgeräten (S) [Benutzende]

Benutzende, die VoIP-Endgeräte einsetzen, SOLLTEN über die grundlegenden VoIP-Gefährdungen und Sicherheitsmaßnahmen informiert sein. Außerdem SOLLTEN sie geeignete Passwörter zur Absicherung von Voicemails auswählen.

NET.4.2.A12 Sichere Außerbetriebnahme von VoIP-Komponenten (S)

Wenn VoIP-Komponenten außer Betrieb genommen oder ersetzt werden, SOLLTEN alle sicherheitsrelevanten Informationen von den Geräten gelöscht werden. Nach dem Löschvorgang SOLLTE überprüft werden, ob die Daten auch tatsächlich erfolgreich entfernt wurden. Vertrauliche Informationen SOLLTEN auch von Backup-Medien gelöscht werden. Alle Beschriftungen, insbesondere der Endgeräte, SOLLTEN vor der Entsorgung entfernt werden. Es SOLLTE frühzeitig mit Herstellenden, Vertreibenden beziehungsweise Service-Unternehmen geklärt werden, welche Maßnahmen zur Löschung sicherheitsrelevanter Informationen mit den Vertrags- und Garantiebedingungen vereinbar sind.

NET.4.2.A13 Anforderungen an eine Firewall für den Einsatz von VoIP (S)

Es SOLLTE überprüft werden, ob die bestehende Firewall für den Einsatz von VoIP angepasst werden kann. Ist dies nicht der Fall, SOLLTE eine zusätzliche Firewall hierfür beschafft und installiert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.4.2.A14 Verschlüsselung der Signalisierung (H)

Die Integrität und Vertraulichkeit der Signalisierungsinformationen SOLLTE durch geeignete kryptografische Verfahren gewährleistet werden. Nicht nur die Nutzdaten, sondern auch die Authentisierungsdaten SOLLTEN durchgängig verschlüsselt werden. Der Zugriff auf das VoIP-Gateway SOLLTE durch VoIP-Adressen und H.323-Identitäten so weit wie möglich eingeschränkt werden. Es SOLLTEN zusätzlich Ende-zu-Ende-Sicherheitsmechanismen für den Medientransport und die Signalisierung benutzt werden. Es SOLLTE dokumentiert werden, wie die Signalisierung geschützt wird.

NET.4.2.A15 Sicherer Medientransport mit SRTP (H)

Mediendaten und Informationen zur Steuerung dieser Daten, die über das Real-Time Transport Protocol (RTP) übertragen werden, SOLLTEN in geeigneter Weise geschützt werden. Die Nutzdaten SOLLTEN durch den Einsatz von Secure Real-Time Transport Protocol (SRTP) beziehungsweise Secure Real-Time Control Protocol (SRTCP) geschützt werden. Die sicherheitsrelevanten Optionen der Implementierung des Protokolls SOLLTEN dokumentiert werden.

NET.4.2.A16 Trennung des Daten- und VoIP-Netzes (H)

Das VoIP-Netz SOLLTE in geeigneter Weise vom Datennetz getrennt werden. Es SOLLTE geregelt werden, wie mit Geräten umzugehen ist, die auf das VoIP- und Datennetz zugreifen müssen. VoIP-Endgeräte in einem VoIP-Netz SOLLTEN NUR die vorgesehenen VoIP-Verbindungen zu anderen IT-Systemen aufbauen können.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat im Rahmen der Technischen Leitlinien die „BSI-TL-02013 für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf" veröffentlicht.

Das National Institute of Standards and Technology (NIST) hat im Rahmen seiner Special Publications die NIST Special Publication 800-5 zu „Security Considerations for Voice Over IP Systems" veröffentlicht.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.4.3 Faxgeräte und Faxserver

1. Beschreibung

1.1. Einleitung

In diesem Baustein werden die Sicherheitsaspekte der Informationsübermittlung über marktübliche Faxgeräte sowie Faxserver betrachtet. Die übermittelten Informationen werden als Fax (Kurzform von Telefax) oder seltener auch als Telefaksimile oder Fernkopie bezeichnet. Bei einem herkömmlichen Faxgerät werden von einer Vorlage die darauf aufgezeichneten Inhalte vom Sendegerät Punkt für Punkt abgetastet und zu den Empfangsgeräten übertragen. Das Empfangsgerät baut diese Inhalte wieder Punkt für Punkt auf und gibt sie in der Regel direkt auf Papier aus.

Ein Faxserver hingegen ist ein Dienst, der auf einem Server installiert wird und so anderen IT-Systemen in einem Datennetz ermöglicht, Faxe zu versenden und zu empfangen. Faxserver werden häufig in bereits bestehende E-Mail- oder Groupware-Systeme integriert. So ist es möglich, dass eingehende Fax-Dokumente durch den Faxserver per E-Mail an die Benutzenden zugestellt werden. Abzusendende Dokumente werden entweder über eine Druckerwarteschlange oder per E-Mail an den Faxserver übergeben. In der Regel wird das Dokument zwischen Faxserver und den Clients im Datennetz als Bild-Datei gesendet oder empfangen. Die übermittelte Bild-Datei kann nicht unmittelbar in Textverarbeitungssystemen weiterverarbeitet werden. Hierzu ist in der Regel zunächst eine Texterkennung (OCR, Optical Character Recognition) erforderlich. Von einem Faxserver empfangene und verarbeitete Dokumente lassen sich für gewöhnlich einfach archivieren, beispielsweise durch den Faxserver-Dienst selber, durch Dokumentenmanagementsysteme oder durch die Groupware, die direkt an den Faxserver-Dienst angebunden sind.

1.2. Zielsetzung

Ein Ziel dieses Bausteins ist der Schutz der Informationen, die mithilfe von Faxsendungen übermittelt und verarbeitet werden. Ein weiteres Ziel ist der Schutz der Faxgeräte und Faxserver vor Manipulationen durch Unbefugte. Das Übertragungsmedium spielt bei der Anwendung des Bausteins keine Rolle, sodass die Anforderungen des Bausteins auch für Fax over IP (FoIP) umgesetzt werden sollten.

1.3. Abgrenzung und Modellierung

Der Baustein NET.4.3 *Faxgeräte und Faxserver* ist für jedes Faxgerät und jeden Faxserver im Informationsverbund anzuwenden.

In diesem Baustein werden als technische Basis des Faxversandes marktübliche Stand-Alone-Faxgeräte und Faxserver betrachtet. Zusätzliche Aspekte zu Faxgeräten, die in einem Multifunktionsgerät (All-in-one-Gerät) zu finden sind, werden gesondert in dem Baustein SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte* behandelt. Zum Schutz der Informationen, die auf Faxservern verarbeitet, angeboten, gespeichert und darüber übertragen werden, sollten der Baustein SYS.1.1 *Allgemeiner Server* sowie die jeweiligen betriebssystemspezifischen Bausteine betrachtet werden. Informationen zur richtigen Archivierung können dem Baustein OPS.1.2.2 *Archivierung* entnommen werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.4.3 *Faxgeräte und Faxserver* von besonderer Bedeutung.

2.1. Unzureichende oder falsche Versorgung mit Verbrauchsgütern

Faxgeräte empfangen Dokumente und drucken diese in der Regel direkt auf Papier aus. Für einen reibungslosen und unterbrechungsfreien Betrieb eines Faxgerätes müssen Verbrauchsgüter wie Papier und Toner in ausreichender Menge vorhanden sein. Ist dies nicht gegeben, können oft keine Fax-Dokumente empfangen werden. Außerdem können keine Sendebestätigungen ausgedruckt werden, die eventuell zwingend benötigt werden.

2.2. Fehlerhafte Faxübertragung

Auf dem Übertragungsweg zwischen Sendegerät und Empfangsgerät eines Fax-Dokuments können zahlreiche Störungen auftreten. Dies kann dazu führen, dass die zu übermittelnden Fax-Dokumente unvollständig oder unlesbar sind oder gar nicht bei den Empfangenden ankommen. Entscheidungen, die von diesen Informationen abhängig sind, können fehlerhaft sein und somit hohe Schäden verursachen.

Zeitverzögerungen, die entstehen, weil die Probleme erst erkannt werden müssen und das Dokument neu gesendet werden muss, können zu weiteren Komplikationen führen. Oft haben die Sendenden oder Empfangenden gar keine Möglichkeiten, den Übertragungsweg zu beeinflussen, sodass sie warten müssen, bis die Störung durch Dritte behoben wurde. Häufig glauben die Absendenden sogar, dass das Fax-Dokument ordnungsgemäß an die gewünschten Adressaten übermittelt wurden und die hierdurch entstehenden Probleme werden erst sehr spät erkannt.

Zusätzlich kann nicht ausgeschlossen werden, dass ein Fax-Dokument an das falsche Empfangsgerät übermittelt wurde, beispielsweise weil eine Fehlschaltung im öffentlichen Telekommunikationsnetz vorliegt. Ebenso ist denkbar, dass bei Faxgeräten Rufnummern falsch gewählt oder Zielwahltasten falsch programmiert werden. Wird ein Faxserver verwendet, können die Rufnummern ebenfalls falsch eingegeben oder falsch im Adressbuch abgespeichert werden. Dadurch können unter Umständen vertrauliche Informationen an unbefugte Personen übermittelt werden.

2.3. Manipulation von Adressbüchern und Verteilerlisten

In Faxgeräten können häufig Adressbücher und Verteilerlisten geführt werden. Wird ein Faxserver genutzt, können in der Regel über die Groupware ähnliche Adressbücher und Verteilerlisten an einer zentralen Stelle geführt werden, die von mehreren Benutzenden verwendet werden können. In den Adressbüchern können Nummern von Empfangenden gespeichert werden, sodass diese nicht bei jedem Faxversand neu eingegeben werden müssen. Zudem ist es möglich, über Verteilerlisten eine Gruppe von Empfangenden anzulegen und so Faxsendungen an mehrere Personen gleichzeitig zu verschicken.

Häufig werden einmal programmierte Nummern von Empfangenden oder Verteilerlisten nicht mehr kontrolliert, wenn ein Fax-Dokument versendet werden soll. Wenn Unbefugte die Adressbücher oder die Verteilerlisten am Faxgerät oder in der Groupware ändern, können so vertrauliche Informationen an die falschen Empfangenden gelangen. Außerdem kann es passieren, dass die vorgesehenen Empfangenden dringend benötigte Informationen nicht erhalten. Beispielsweise könnte eine Faxnummer im Adressbuch ausgetauscht oder weitere Empfangende in die Verteilerliste aufgenommen werden, ohne dass dies von den Verantwortlichen in der jeweiligen Institution bemerkt wird.

2.4. Unbefugtes Lesen von Faxsendungen

In fast allen Fällen ist es am wirtschaftlichsten, wenn sich mehrere Benutzende ein Faxgerät teilen. Daher werden diese in der Regel in Räumen aufgestellt, die alle Mitarbeitenden einer Institution betreten können, wie beispielsweise in Druckerräumen. Da hierdurch die Faxgeräte für alle Mitarbeitenden frei zugänglich sind, können auch alle Mitarbeitenden die empfangenen Faxsendungen lesen und so an vertrauliche Informationen gelangen.

2.5. Auswertung von Restinformationen in Faxgeräten und Faxservern

Abhängig vom technischen Verfahren, mit dem Faxgeräte Informationen speichern, weiterverarbeiten oder drucken, können nach dem Faxversand und -empfang Restinformationen unterschiedlichen Umfangs im Faxgerät verbleiben. Unbefugte, die in den Besitz des Gerätes oder der entsprechenden Bauteile kommen, können diese Informationen unter Umständen wiederherstellen.

Auf der Festplatte eines Faxservers werden Faxsendungen mindestens so lange gespeichert, bis sie an das Ziel zugestellt werden können. Weiterhin arbeiten moderne Betriebssysteme mit Auslagerungsdateien, die auch Restinformationen enthalten können. Diese Informationen könnten beim Zugriff auf diesen Faxserver unerlaubt ausgewertet werden.

2.6. Vortäuschen eines falschen Absendenden bei Faxsendungen

Faxsendungen sind ein beliebtes Medium, um Dokumente, die nur mit einer Unterschrift gültig sind, zu übertragen. Doch auf die gleiche Weise, wie mit einem falschen Namen und einem falschen Briefkopf falsche Absendende vorgetäuscht werden kann, kann auch eine Faxsendung manipuliert werden. So können beispielsweise Unterschriften von anderen Schriftstücken eingescannt und auf das Fax-Dokument kopiert werden. Ein Unterschied, ob es sich um eine tatsächlich getätigte Unterschrift oder um eine reproduzierte Grafikdatei handelt, ist generell nicht zu erkennen. Schäden entstehen dann, wenn Empfangende die darin enthaltenen Informationen als authentisch oder sogar als rechtsverbindlich ansehen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET:4.3 *Faxgeräte und Faxserver* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	Fachverantwortliche
Weitere Zuständigkeiten	Benutzende, Beschaffungsstelle, IT-Betrieb, Haustechnik

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.4.3.A1 Geeignete Aufstellung eines Faxgerätes (B) [Haustechnik]

Faxgeräte MÜSSEN so aufgestellt werden, dass eingegangene Faxsendungen nicht von Unberechtigten eingesehen oder entnommen werden können. Der Aufstellungsort SOLLTE zudem danach ausgewählt werden, dass ausreichend dimensionierte Telekommunikationsleitungen bzw. -kanäle vorhanden sind. Der Aufstellungsort MUSS über einen geeigneten Netzanschluss für das Faxgerät verfügen. Faxgeräte DÜRFTEN NICHT an nicht dafür vorgesehene Netzanschlüsse angeschlossen werden.

NET.4.3.A2 Informationen für Mitarbeitende über die Faxnutzung (B)

Alle Mitarbeitenden MÜSSEN auf die Besonderheiten der Informationsübermittlung per Fax hingewiesen werden. Sie MÜSSEN auch darüber informiert sein, dass die Rechtsverbindlichkeit einer Faxsendung stark eingeschränkt ist. Eine verständliche Bedienungsanleitung MUSS am Faxgerät ausliegen. Die Benutzenden SOLLTEN mindestens eine Kurzanleitung zur eingesetzten Faxclient-Software des Faxservers erhalten. Außerdem MUSS eine Anweisung zur korrekten Faxnutzung ausliegen.

NET.4.3.A3 Sicherer Betrieb eines Faxservers (B) [IT-Betrieb]

Bevor ein Faxserver in Betrieb genommen wird, SOLLTE eine Testphase erfolgen. Konfigurationsparameter sowie alle Änderungen an der Konfiguration eines Faxservers SOLLTEN dokumentiert werden. Die Archivierung und Löschung von Faxdaten SOLLTEN geregelt sein. Außerdem MUSS regelmäßig die Verbindung vom Faxserver zur TK-Anlage beziehungsweise zum öffentlichen Telefonnetz auf ihre Funktion geprüft werden. Es MUSS außerdem sichergestellt werden, dass der Faxserver ausschließlich Fax-Dienste anbietet und nicht für weitere Dienste genutzt wird. Alle nicht benötigten Leistungsmerkmale und Zugänge der eingesetzten Kommunikationsschnittstellen MÜSSEN deaktiviert werden.

3.2. Standard-Anforderungen

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

NET.4.3.A4 Erstellung einer Sicherheitsrichtlinie für die Faxnutzung (S)

Vor der Freigabe eines Gerätes SOLLTE eine Sicherheitsrichtlinie für die Faxnutzung erstellt werden. Dort SOLLTE die Einsatzart festgelegt sein. Außerdem SOLLTE geregelt werden, wie mit Faxeingängen und -ausgängen umzugehen ist. Zudem SOLLTE eine Regelung zur Behandlung von nicht zustellbaren Faxsendungen erstellt werden. Außerdem SOLLTE die Richtlinie Informationen und Anweisungen zur Notfallvorsorge und Ausfallsicherheit des Faxbetriebes enthalten.

NET.4.3.A5 ENTFALLEN (S)

Diese Anforderung ist entfallen.

NET.4.3.A6 Beschaffung geeigneter Faxgeräte und Faxserver (S) [Beschaffungsstelle]

Bevor Faxgeräte oder Faxserver beschafft werden, SOLLTE eine Anforderungsliste erstellt werden. Anhand dieser Liste SOLLTEN die infrage kommenden Systeme oder Komponenten bewertet werden. Die Anforderungsliste für Faxgeräte SOLLTE auch sicherheitsrelevante Aspekte umfassen, wie den Austausch einer Teilnehmererkennung, die Ausgabe von Sendeberichten sowie eine Fehlerprotokollierung und Journalführung. Zudem SOLLTEN angemessene zusätzliche Sicherheitsfunktionen anhand des Schutzbedarfs berücksichtigt werden.

Bei einem Faxserver SOLLTEN alle Anforderungen an das IT-System einschließlich Betriebssystem, Kommunikationskomponenten und Applikationssoftware erhoben und berücksichtigt werden. Die Möglichkeit, dass ein Faxserver in ein bestehendes Datennetz und in ein Groupware-System integriert werden kann, SOLLTE bei Bedarf berücksichtigt werden.

NET.4.3.A7 Geeignete Kennzeichnung ausgehender Faxsendungen (S) [Benutzende]

Quelle und Ziel jeder Faxsendung SOLLTEN auf allen ausgehenden Faxsendungen ersichtlich sein. Wenn diese Informationen nicht aus dem versendeten Dokument ermittelt werden können, SOLLTE ein standardisiertes Faxdeckblatt benutzt werden. Generell SOLLTE das Faxdeckblatt mindestens den Namen der Institution des Absendenden, den Namen des Ansprechpartners bzw. der Ansprechpartnerin, das Datum, die Seitenanzahl sowie einen Dringlichkeitsvermerk auflisten. Außerdem SOLLTE es die Namen und die Institution der Empfangenden enthalten. Wenn notwendig, SOLLTE das Faxdeckblatt für jedes ausgehende Fax angepasst werden.

NET.4.3.A8 Geeignete Entsorgung von Fax-Verbrauchsgütern und -Ersatzteilen (S)

Alle Fax-Verbrauchsgüter, aus denen Informationen über die versendeten und empfangenen Fax-Dokumente gewonnen werden können, SOLLTEN vor der Entsorgung unkenntlich gemacht werden oder durch eine zuverlässige Fachfirma entsorgt werden. Die gleiche Vorgehensweise SOLLTE auch bei ausgetauschten informationstragenden Ersatzteilen erfolgen. Wartungsfirmen, die Faxgeräte überprüfen oder reparieren, SOLLTEN zu einer entsprechenden Handhabung verpflichtet werden. Es SOLLTE regelmäßig kontrolliert werden, ob diese Handhabung eingehalten wird.

NET.4.3.A9 Nutzung von Sende- und Empfangsprotokollen (S)

Die Übertragungsvorgänge ein- und ausgehender Faxsendungen SOLLTEN protokolliert werden. Dazu SOLLTEN die Kommunikationsjournale marktüblicher Faxgeräte genutzt werden. Verfügen die Faxgeräte über Protokollierungsfunktionen, SOLLTEN diese aktiviert werden. Bei einem Faxserver SOLLTE die Protokollierung ebenso aktiviert werden. Auch SOLLTE entschieden werden, welche Informationen protokolliert werden sollen.

Die Kommunikationsjournale der Faxgeräte und die Protokollierungsdateien SOLLTEN regelmäßig ausgewertet und archiviert werden. Sie SOLLTEN stichprobenartig auf Unregelmäßigkeiten geprüft werden. Unbefugte SOLLTEN nicht auf die Kommunikationsjournale sowie die protokollierten Informationen zugreifen können.

NET.4.3.A10 Kontrolle programmierbarer Zieladressen, Protokolle und Verteilerlisten (S)

Programmierbare Kurzwahltasten oder gespeicherte Zieladressen SOLLTEN regelmäßig daraufhin überprüft werden, ob die gewünschte Faxnummer mit der einprogrammierten Nummer übereinstimmt. Nicht mehr benötige Faxnummern SOLLTEN gelöscht werden. Es SOLLTE in geeigneter Weise dokumentiert werden, wenn ein neuer Eintrag aufgenommen oder eine Zielnummer geändert wird.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.4.3.A11 Schutz vor Überlastung des Faxgerätes (H) [IT-Betrieb]

Es SOLLTEN ausreichend Kommunikationsleitungen bzw. -kanäle verfügbar sein. Bei einem Faxserver SOLLTE das voraussichtliche Faxvolumen abgeschätzt werden. Es SOLLTEN entsprechend leistungsfähige Komponenten ausgewählt werden. Die Protokolle von Faxservern SOLLTEN regelmäßig kontrolliert werden, um Engpässen durch Überlastungen rechtzeitig entgegenzuwirken. Nicht mehr benötigte Faxdaten SOLLTEN zeitnah vom Faxserver gelöscht werden.

NET.4.3.A12 Sperren bestimmter Quell- und Ziel-Faxnummern (H)

Unerwünschte Faxadressen, SOLLTEN blockiert werden. Alternativ SOLLTEN nur bestimmte Rufnummern zugelassen werden. Es SOLLTE geprüft werden, welcher Ansatz in welcher Situation geeignet ist.

NET.4.3.A13 Festlegung berechtigter Faxbedienenden (H) [Benutzende]

Es SOLLTEN nur wenige Mitarbeitende ausgewählt werden, die auf das Faxgerät zugreifen dürfen. Diese Mitarbeitenden SOLLTEN ankommende Faxsendungen an die Empfangenden verteilen. Den Mitarbeitenden SOLLTE vermittelt werden, wie sie mit dem Gerät umgehen und wie sie die erforderlichen Sicherheitsmaßnahmen umsetzen können. Jeder berechtigte Benutzende SOLLTE darüber unterrichtet werden, wer das Faxgerät bedienen darf und wer für das Gerät zuständig ist.

NET.4.3.A14 Fertigung von Kopien eingehender Faxsendungen (H) [Benutzende]

Auf Thermopapier gedruckte Faxsendungen, die länger benötigt werden, SOLLTEN auf Normalpapier kopiert oder eingescannt werden. Es SOLLTE berücksichtigt werden, dass auf Thermopapier die Farbe schneller verblasst und somit unkenntlich wird. Die Kopien oder eingescannten Faxsendungen SOLLTEN in geeigneter Weise archiviert werden.

NET.4.3.A15 Ankündigung und Rückversicherung im Umgang mit Faxsendungen (H) [Benutzende]

Wichtige Faxsendungen SOLLTEN den Empfangenden angekündigt werden, bevor sie versendet werden. Dazu SOLLTE festgelegt werden, welche Dokumente vorab angemeldet werden sollen. Mitarbeitende, die vertrauliche Fax-Dokumente versenden möchten, SOLLTEN angewiesen werden, sich den vollständigen Erhalt von den Empfangenden bestätigen zu lassen. Bei wichtigen oder ungewöhnlichen Faxsendungen SOLLTEN sich wiederum Empfangende von den Absendenden bestätigen lassen, dass das Fax-Dokument von ihnen stammt und nicht gefälscht wurde. Es SOLLTE eine geeignete Kommunikationsform ausgewählt werden, mit dem die Fax-Dokumente angekündigt oder bestätigt werden, beispielsweise per Telefon.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein NET:4.3 *Faxgeräte und Faxserver* sind keine weiterführenden Informationen vorhanden.