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.