Richtlinie zur Netzarchitektur
Landkreis Teltow-Fläming

LANDKREIS TELTOW-FLÄMING
unverkennbar stark - südlich von Berlin

Inhalt

Präambel....1
§ 1 Begriffsbestimmungen....1
§ 2 Zuständigkeiten....1
§ 3 Schutzniveau....1
§ 4 Netzplanung....2
§ 5 Sicherheitszonen....2
§ 6 Internes Netz....3
§ 7 Demilitarisierte Zone....3
§ 8 Außenanbindungen....4
§ 9 Segmentierung....4
§ 10 Protokolle....5
§ 11 Internet-Protocoll....5
§ 12 Domain-Name-Service (DNS)....5
§ 13 Network-Time-Protocol (NTP)....6
§ 14 Telearbeit....6
§ 15 Sicherheitsgateway....6
§ 16 Zentrale Serverdienste....7
§ 17 Architektur des Managementnetzes....7
§ 18 Virtuelles LAN....8
§ 19 Notfallvorsorge....8
§ 20 Schlussbestimmungen....9
Anlage 1: Referenztabelle....10

Präambel

Diese Richtlinie orientiert sich an den Vorgaben des BSI-Bausteins NET.1.1 Netzarchitektur und Netzdesign aus dem Jahr 2023. Das Ziel dieser Richtlinie ist es die Informationssicherheit als integralen Bestandteil der Netzarchitektur und des Designs zu etablieren. Der Landkreis verwendet für seine Aufgabenerfüllung Datennetze über diese werden Daten und Informationen ausgetauscht. In diesem werden nicht nur Endgeräte wie PCs angeschlossen, sondern auch Server oder externe Netze wie das Internet. Um die Aufgaben zu schützen müssen die Netze sicher aufgebaut werden und der Zugriff entsprechend eingeschränkt werden.

§ 1
Begriffsbestimmungen

(1) Firewall: besteht aus Hard- und Software, die den Datenfluss zwischen Netzwerken kontrolliert. Alle Daten, die ein Netz verlassen werden ebenso überprüft, wie die, die eintreten.

(2) Segmentierung: Bei einer Segmentierung handelt es sich um das Aufteilen von größeren Netzwerken in kleinere Netzwerke (Netzsegmente).

(3) Application-Layer-Gateway (ALG): Das ALG ist eine Sicherheitskomponente welche zwischen Clients und Applikationsservern die Kommunikation kontrolliert. Dieses wird in Form eines Proxies umgesetzt.

(4) Netzwerk: Ein Netzwerk bezeichnet eine Verbindung von mehreren Knotenpunkten über Linien. Dies sind in der IT mehrere Computersysteme, welche mithilfe von Kabeln oder Funk verbunden werden.

§ 2
Zuständigkeiten

(1) Für die Umsetzung dieser Richtlinie ist das Amt für Digitalisierung und Informationstechnik zuständig.

(2) Abweichungen von der Richtlinie müssen im Informationssicherheitsmanagementsystem dokumentiert und mit der*dem Informationssicherheitsbeauftragten abgestimmt werden.

(3) Die*der Informationssicherheitsbeauftragte überprüft die Umsetzung der Richtlinie.

§ 3
Schutzniveau

Das Schutzniveau wurde nach den Vorgaben des für die EU-Zahlstelle zuständigen Ministeriums ermittelt. Wenn aufgrund eines neu festgestellten Schutzbedarfes o.a. eine Änderung notwendig ist, muss die Richtlinie angepasst werden.

§ 4
Netzplanung

(1) Diese Richtlinie gilt als Grundlage für die Planung des Netzwerks und muss bei dieser zuvorderst betrachtet werden.

(2) Der Einsatz eines in-band-Managementnetzwerks ist nicht zulässig.

(3) Die Netzplanung muss jährlich überprüft werden.

(4) Das Netzwerk muss dokumentiert werden. In dieser müssen die aktuellen Kennzahlen festgehalten werden:

(a) IST-Zustand

(b) Netzperformance

(c) Zonierung des Netzwerks

(d) Physische Topologie des Netzwerks

(e) Logische Struktur des Netzes (Segmente, Subnetze, Zonierung)

(f) Dokumentation der Betriebsprozesse

(g) Dokumentation der Änderungen.

(5) Es muss eine Planung für die Dimensionierung und Redundanz der Netz- und Sicherheitskomponenten geben.

(6) Es muss einmal jährlich überprüft werden ob der IST-Zustand der Netzstruktur und Netzdesigns den Anforderungen dieser Richtlinie entspricht. Die Prüfung erfolgt nach den Vorgaben der Dienstanweisung Nr. 70/2024 Interne Revision und Auditierung nach IT-Grundschutz Landkreis Teltow-Fläming.

(7) Auf Basis der Anforderungen aus dieser Richtlinie muss eine Spezifikation der Netzarchitektur und des Netzdesigns erfolgen, wobei sämtliche Architekturelemente berücksichtigt werden müssen.

§ 5
Sicherheitszonen

(1) Das Netzwerk wird übergreifend in mindestens drei physisch separierte Sicherheitszonen getrennt sein:

(a) Internes Netz: ist das nicht öffentliche Netz des Landkreises Teltow-Fläming. Dieses umfasst z.B. Server und Clients.

- In diesem muss eine Sicherheitszone für zentrale Serverdienste vorhanden sein.

(b) Demilitarisierte Zone (DMZ): Bei einer DMZ handelt es ich um das öffentliche Netzwerk des Landkreises Teltow-Fläming. Diese umfasst im allgemeinen Serverdienste, welchen Externen zur Verfügung gestellt werden.

(c) Außenanbindungen: Dabei handelt es sich um nicht vertrauenswürdige Netzwerke wie z. B. das Internet oder das Landesverwaltungsnetz. Ein Netzwerk ist nicht vertrauenswürdig, wenn der Landkreis die Zugriffe in das Netzwerk nicht steuern kann.

(2) Jede ein- und ausgehende Information muss durch sämtliche sie passierenden Firewalls kontrolliert und gefiltert werden.

(3) Ein Ausfall beziehungsweise ein Neustart einer Komponente darf nicht zu einem Abschwächen von Maßnahmen führen.

(4) Weitere Regelungen werden in der Richtlinie zum Einsatz von Firewalls im Landkreis Teltow-Fläming getroffen.

§ 6
Internes Netz

(1) Grundsätzlich sind im internen Netzwerk die Kommunikationsmedien LAN und Richtfunk zulässig.

(2) Verschlüsselung: Es muss mindestens eine Verschlüsselung garantiert werden, welche dem Stand der Technik entspricht.

(3) Ausgehende Kommunikation aus dem internen Netzwerk muss am ALG der Packetfilter-ALG-Packetfilter (P-A-P)-Struktur entkoppelt werden.

(4) Die interne Zone muss über eine P-A-P-Struktur von den DMZ‘s und den Außenanbindungen getrennt sein.

(5) Clients dürfen nur im internen Netz eingesetzt werden. Abweichende Regelungen hiervon sind in der Dienstvereinbarung Nr. 42/2022 zum Arbeiten außerhalb der Diensträume geregelt.

(6) Es dürfen nur Clients im internen Netzwerk betrieben werden, welche zentral vom Amt für Digitalisierung und Informationstechnik betreut werden.

§ 7
Demilitarisierte Zone

(1) Grundsätzlich ist in der DMZ das Kommunikationsmedium LAN erlaubt.

(2) Es sind keine Zugriffe aus der DMZ in das interne Netzwerk erlaubt.

(3) In der DMZ dürfen keine produktiven Systeme eingesetzt werden.

(4) Für jeden Zugriff aus einer Außenanbindung auf die Infrastruktur der Kreisverwaltung wird mindestens eine eigene DMZ eingesetzt.

(5) Es sind nur statische Routen in die DMZ zulässig.

(6) Die Routing-Protokolle müssen die Authentisierung und Integrität sicherstellen.

(7) Es dürfen nur interne IP-Adressen verwendet werden, welche nicht vom Internet adressierbar sind.

(8) Der Zugriff über eine Außenanbindung auf die DMZ muss über einen Proxy erfolgen.

§ 8
Außenanbindungen

(1) Grundsätzlich sind alle Kommunikationsmedien beim Einsatz von Außenanbindungen erlaubt.

(2) Es sind keine Zugriffe von den Außenanbindungen in das interne Netz erlaubt.

(3) Als Außenanbindung und somit nicht vertrauenswürdige Netzwerke gelten das Internet sowie das Landesverwaltungsnetz.

(4) Institutionsfremde Geräte dürfen ausschließlich in einem Gast-Netzwerk untergebracht werden.

§ 9
Segmentierung

(1) Im internen Netzwerk müssen Clients und Server sich in getrennten Netzsegmenten befinden. Die Kommunikation zwischen Clients und Servern muss über eine Firewall mit einer Stateful-Packet-Inspection erfolgen.

(2) Gastzugänge und Netzwerke, für die es keine ausreichende interne Kontrolle über die Endgeräte gibt, müssen in eigene Netzsegmente untergebracht werden.

(3) Es dürfen nur Clients aus dem gleichen Sachgebiet in ein Netzsegment positioniert werden. Wenn ein abweichender Schutzbedarf festgestellt wird, gilt für alle Systeme im Netzsegment der höchste ermittelte Schutzbedarf (gleicher Schutzbedarf).

(4) Für jedes nicht vertrauenswürdige Netzwerk, welches auf Dienste bzw. Anwendungen zugreift, muss es eine DMZ geben. Diese werden an der äußeren Firewall eingerichtet.

§ 10
Protokolle

(1) Es dürfen nur dienstlich notwendige Protokolle verwendet werden.

(2) Die Verwendung von nicht verschlüsselten Protokollen im internen Netzwerk ist nicht zulässig. Die Verschlüsselung muss dem aktuellen Stand der Technik entsprechen.

(3) DHCP ist nur für registrierte MAC-Adressen erlaubt.

(4) Falls über nicht vertrauenswürdige Netzwerke kommuniziert wird, muss mithilfe eines VPN‘s die Verschlüsselung und die Authentizität des Benutzers nachgewiesen werden.

(5) In einem Netzsegment ist nur IPv4 zulässig.

(6) Der Einsatz von SLAAC und Stateless-DHCP ist im Gastnetz erlaubt.

§ 11
Internet-Protocoll

(1) IP-Source-Routing ist zu deaktivieren.

(2) Es muss stets die aktuelle Version des Internet-Protocolls verwendet werden.

(3) Die IP-Adressräume müssen systematisch in den Netzsegmenten vergeben werden.

(4) Das Virtual-Router-Redundancy-Protocol muss deaktiviert werden.

(5) Directed Broadcasts sind zu deaktivieren.

(6) Router-Advertisements von Endgeräten sind nicht zulässig.

(7) Die Wirkung von Router-Advertisements sind nur innerhalb eines Subnetzes wirksam.

(8) IP-Blacklists müssen gegen einen Overflow-Angriff gehärtet werden.

§ 12
Domain-Name-Service (DNS)

(1) Es muss Domain-Name-Service-Security-Extension (DNSSEC) verwendet werden.

(2) Der externe sowie der interne DNS müssen in ihrer Funktionalität getrennt werden.

(3) Ein Zonentransfer ist nur für ausgewählte Server zulässig.

(4) Die List-Funktion des DNS muss deaktiviert werden.

(5) DNS darf nur für vertrauenswürdige Systeme möglich sein.

(6) DNS-Anfragen ohne gesetztes Recursions-Bit müssen verworfen werden.

§ 13
Network-Time-Protocol (NTP)

(1) Alle Komponenten des Netzwerkes müssen eine synchronisierte Uhrzeit nutzen.

(2) Dafür muss ein zentraler NTP-Dienst betrieben werden.

(3) Dieser muss sich mit einem vertrauenswürdigen Anbieter synchronisieren.

(4) NTP muss im Client-Server-Modus betrieben werden und es muss eine Authentisierung stattfinden.

(5) Der NTP-Server muss Out-Of-Band betrieben werden.

(6) Zeitverteilung per Broadcast ist nicht zulässig.

§ 14
Telearbeit

(1) Für die Nutzung von Telearbeit oder mobilem Arbeiten muss eine eigene DMZ verwendet werden. Diese unterliegt nicht den Anforderungen des § 7 dieser Richtlinie.

(2) Der Zugriff in die DMZ darf nur von vertrauenswürdigen Nutzern erfolgen.

(3) Die Hardware und das Betriebssystem der Systeme welche in die DMZ dürfen, werden vom Landkreis bereitgestellt.

(4) Die Nutzung der bereitgestellten Hardware ist auch außerhalb des internen Netzwerks möglich.

(5) Zugriffe aus der DMZ müssen die P-A-P-Struktur durchlaufen und gefiltert werden.

(6) Es sind keine anderen Zugriffe in das interne Netzwerk gestattet.

(7) Außenstellen des Landkreises dürfen nur über eine VPN-Verbindung angebunden werden

§ 15
Sicherheitsgateway

(1) Der proxy-basierte Application-Level-Gateway (ALG) befindet sich im Transfernetzwerk zwischen den beiden Firewalls. Es sind keine weiteren Systeme und Dienste in diesem Netzwerk zulässig. Es sind weitere Sicherheitsproxies zulässig.

(2) Es muss ein Virenschutzprogramm auf einem eigenen Server im Sicherheitsgateway zur Verfügung gestellt werden.

(3) Sämtlicher Datentransfer, welcher durch das Transfernetzwerk läuft, muss von einem ALG entkoppelt werden.

(4) Es darf kein Netzwerk geschaffen werden, welches die beiden Firewalls direkt miteinander verbindet.

(5) Ein Zugriff auf das ALG oder andere Sicherheitsproxies dürfen nur über ein Managementnetzwerk nach § 17 erfolgen.

(6) Zugriffe in das interne Netzwerk nach der Dienstvereinbarung Nr. 42/2022 zum Arbeiten außerhalb der Diensträume müssen nicht das ALG durchlaufen.

(7) Es sind nur statische Routen zulässig.

(8) Auflösung externer Servernamen erfolgt über den DNS-Server, welcher rekursive Anfragen an den DNS-Proxy des ALGs stellt.

(9) Alle Komponenten des Sicherheitsgateways müssen bei Betrieb aktiv sein.

§ 16
Zentrale Serverdienste

(1) Zentrale Serverdienste werden in mindestens einem eigenen Netzbereich zur Verfügung gestellt. Dies umfasst NTP; DNS; internen Mail-Server; Authentifizierungsdienste; DHCP.

(2) Die Datenbankserver müssen in ein eigenes Netz entsprechend ihres Schutzbedarfes betrieben werden. Ein Zugriff darf nur über Fachserver mithilfe einer Schnittstelle ermöglicht werden.

(3) Das Netz befindet sich an der inneren Firewall und die Kommunikation muss über eine Stateful-Packet-Inspection erfolgen.

§ 17
Architektur des Managementnetzes

(1) Es muss ein physisch getrenntes Out-Of-Band-Managementnetz für sämtliche Netzinfrastrukturkomponenten geschaffen werden.

(2) Nur absolut notwendige Administratoren sollen Zugriff auf das Netzwerk und seine Komponenten haben oder erhalten.

(3) Es müssen in den entsprechenden Managementnetzsegmenten Geräte positioniert werden, welche zur Administration unterschiedlicher Netzzonen gedacht sind. Ein Zugriff auf die Geräte ist nur mittels verschlüsselter Protokolle gestattet durch einen Stateful-Packetfilter.

(4) Das Managementnetz muss für jede Sicherheitszone ein physisch getrenntes Segment besitzen, welches durch eine dedizierte Firewall getrennt ist.

(5) Folgende Managementnetze müssen umgesetzt werden:

(a) ein Netzsegment zur Authentisierung und Autorisierung der administrativen Kommunikation,

(b) ein Netzsegment zur Administration der Systeme,

(c) ein Netzsegment für die Überwachung und das Monitoring,

(d) ein Netzsegment für die zentrale Protokollierung inklusive Syslog-Server und SIEM-Server,

(e) ein Netzsegment für grundlegende Dienste des Managementnetzes,

(f) ein Netzsegment für die Management-Interfaces der zu administrierenden IT-Systeme.

(6) Es muss mindestens das Simple-Networt-Management-Protocol-Version-3 verwendet werden.

(7) Alle verwendeten Dienste müssen mindestens eine Transportverschlüsselung auf dem aktuellen Stand anbieten.

(8) Es muss dokumentiert werden von welchen System mit welchen Werkzeugen Administrationsprozesse durchgeführt werden.

§ 18
Virtuelles LAN

(1) Der Einsatz von Virtuellen LAN (VLAN) ist nur im internen Netzwerk gestattet.

(2) VLANs dürfen nicht zur Trennung der Sicherheitszonen verwendet werden.

(3) Trunking an Zugriffs-Ports ist zu sperren.

(4) Wenn ein sehr hoher Schutzbedarf ermittelt wurde, ist der Einsatz von VLANs nur im Ausnahmefall gestattet.

§ 19
Notfallvorsorge

(1) Diagnose und Fehlerbehebungen müssen im Vorfeld geplant und vorbereitet werden. Für typische Ausfallszenarien müssen entsprechende Handlungsanweisungen definiert und in regelmäßigen Abständen aktualisiert werden.

(2) Die Notfallplanungen für die Netzarchitektur muss mit der übergreifenden Störungs-, Notfallvorsorge und Business-Continuity-Management (BCM) abgestimmt sein, nach dem allgemeinen Notfallvorsorgekonzept.

(3) Die Dokumentationen zur Notfallvorsorge und die darin enthaltenen Handlungsanweisungen müssen in Papierform vorliegen.

(4) Im BCM werden weitere Regelungen zur Erprobung des Notfalls getroffen. Wenn das BCM dies nicht regelt, muss einmal jährlich eine Erprobung des Notfalls stattfinden.

§ 20
Schlussbestimmungen

Die Richtlinie zur Netzarchitektur tritt am Tag nach Veröffentlichung im Intranet in Kraft.

Luckenwalde, den 30.Oktober 2024

Wehlan
Landrätin

Anlage 1: Referenztabelle

Bezeichnung	Hinterlegte Anforderung BSI
§ 4 Netzplanung	NET.1.1.A13, NET.1.1.A14, NET.1.1.A15, NET.1.1.A16, NET.1.1.A17, NET.1.1.A26;
§ 5 Sicherheitszonen	NET.1.1.A2, NET.1.1.A4
§ 6 Internes Netz	NET.1.1.A4
§ 7 Demilitarisierte Zone	NET.1.1.A4
§ 8 Außenanbindungen	NET.1.1.A4, NET.1.1.A9
§ 9 Segmentierung	NET.1.1.A5, NET.1.1.A6, NET.1.1.A10, NET.1.1.A19, NET.1.1.A23
§ 10 Protokolle	NET.1.1.A7, NET.1.1.A8, NET.1.1.A20
§ 11 Internet Protocoll	NET.1.1.A7, NET.1.1.A8
§ 12 Domain-Name-Service	NET.1.1.A7, NET.1.1.A8
§ 13 Network-Time-Protocoll	NET.1.1.A7, NET.1.1.A8;
§ 14 Telearbeit	NET.1.1.A11
§ 15 Sicherheitsgateway	NET.1.1.A4, NET.1.1.A12, NET.1.1.A18
§ 16 Zentrale Serverdienste	NET.1.1.A19
§ 17 Managementnetz	NET.1.1.A21;
§ 18 VLAN	NET.1.1.A24
§ 19 Notfallplanung	NET.1.1.A27