Muster-Prüfprogramm

Netzwerksicherheit und Segmentierung

12 Prüfschritte · ISO 27001, BSI

12 Prüfschritte mit Kriterium, Fundstelle, Prüfhandlung und erwarteten Nachweisen. 8 Unterlagen zur Anforderung und die typischen Feststellungen.

ISO/IEC 27001:2022 Anhang A 8.20 · BSI NET.1.1 · ISO/IEC 27001:2022 Anhang A 8.22 · BSI NET.3.2 · ISO/IEC 27001:2022 Anhang A 8.32 · BSI NET.1.2 · ISO/IEC 27001:2022 Anhang A 8.21 · § 30 Abs. 2 Nr. 10 BSIG · ISO/IEC 27001:2022 Anhang A 8.2 · ISO/IEC 27001:2022 Anhang A 8.16 · NIS2-Richtlinie Art. 21 Abs. 2 lit. f

Prüfungsziel und Geltungsbereich

Die Prüfung beurteilt, ob die Organisation ihre Netze nach Schutzbedarf gestaltet und abgrenzt, den Datenverkehr zwischen den Zonen kontrolliert, Netzdienste und Fernzugänge sicher betreibt und Änderungen sowie Auffälligkeiten im Netz beherrscht. Sie beurteilt außerdem, ob die Dokumentation die tatsächliche Struktur abbildet.

GELTUNGSBEREICH

- Interne Netze, Rechenzentrumsnetze, Standort- und Fernanbindungen, Funknetze und die Übergänge zum Internet
- Firewalls, Router, Switches, VPN-Gateways und Netzdienste wie DNS und DHCP
- Netzmanagement, Änderungen an Regeln und Überwachung des Datenverkehrs
- Nicht Gegenstand: Anwendungssicherheit und Endgerätehärtung, sofern nicht gesondert vereinbart

Prüfschritte 1 bis 3

Schritt 01 ISO/IEC 27001:2022 Anhang A 8.20; BSI NET.1.1

Eine Netzwerksicherheitsrichtlinie besteht, ist freigegeben und regelt Gestaltung, Betrieb und Zugriff auf Netze.

Prüfhandlung Richtlinie lesen, Freigabe und Aktualität feststellen und mit der Netzdokumentation abgleichen.

Nachweise Richtlinie mit Freigabevermerk, Netzdokumentation

Schritt 02 BSI NET.1.1; ISO/IEC 27001:2022 Anhang A 8.20

Netzpläne und Zonenmodell sind aktuell und bilden die tatsächliche Struktur ab, einschließlich der Übergänge zu Dienstleistern und Cloud-Anbindungen.

Prüfhandlung Netzplan mit der Konfiguration von Routern und Firewalls an drei Standorten oder Zonen abgleichen.

Nachweise Netzpläne, Zonenmodell, Konfigurationsauszüge

Schritt 03 ISO/IEC 27001:2022 Anhang A 8.22; BSI NET.1.1

Netze sind nach Schutzbedarf in Zonen getrennt, wesentliche Systeme und Verwaltungsnetze liegen in eigenen Segmenten.

Prüfhandlung Zonenkonzept mit der Umsetzung vergleichen und von einem Benutzernetz aus testen, ob Verwaltungsschnittstellen erreichbar sind.

Nachweise Segmentierungskonzept, Testergebnisse der Erreichbarkeit, Konfigurationsauszüge

Prüfschritte 4 bis 6

Schritt 04 — BSI NET.3.2; ISO/IEC 27001:2022 Anhang A 8.20

Der Datenverkehr zwischen den Zonen wird durch Firewalls kontrolliert, die Standardregel verbietet, was nicht ausdrücklich erlaubt ist.

Prüfhandlung Regelwerke der Firewalls zwischen Internet, Benutzernetz und Rechenzentrum ansehen und die Standardregel prüfen.

Nachweise Regelwerksauszüge, Konfiguration der Standardregel

Schritt 05 — BSI NET.3.2

Regeln sind begründet, mit Verantwortlichen versehen und werden regelmäßig auf Notwendigkeit überprüft; zu weit gefasste und ungenutzte Regeln werden entfernt.

Prüfhandlung Zehn Regeln auswählen, Begründung und Verantwortliche prüfen und mit Trefferzahlen der letzten Monate abgleichen.

Nachweise Regelwerk mit Kommentaren, Bericht der letzten Regelüberprüfung, Trefferstatistik

Schritt 06 — ISO/IEC 27001:2022 Anhang A 8.32; BSI NET.1.2

Änderungen an Netzkomponenten und Regeln laufen über ein genehmigtes Änderungsverfahren und werden dokumentiert.

Prüfhandlung Änderungen an Firewall-Regeln der letzten sechs Monate mit den Änderungsanträgen abgleichen.

Nachweise Änderungsprotokolle der Firewall, Änderungsanträge

Prüfschritte 7 bis 9

Schritt 07 — ISO/IEC 27001:2022 Anhang A 8.21

Netzdienste, auch von Dienstleistern bereitgestellte, sind mit Sicherheitsmerkmalen, Leistungsstufen und Verwaltungsanforderungen festgelegt und werden überwacht.

Prüfhandlung Vereinbarungen zu Netzdiensten lesen und für zwei Dienste die Einhaltung der Sicherheitsmerkmale nachvollziehen.

Nachweise Vereinbarungen zu Netzdiensten, Berichte zur Leistung

Schritt 08 — ISO/IEC 27001:2022 Anhang A 8.20; § 30 Abs. 2 Nr. 10 BSIG

Fernzugänge sind auf das Nötige beschränkt, verschlüsselt und durch Mehrfaktor-Authentifizierung gesichert.

Prüfhandlung Konfiguration der VPN-Gateways und der Fernwartungszugänge prüfen und Ausnahmen durchgehen.

Nachweise Konfigurationsauszüge, Ausnahmeliste mit Genehmigung

Schritt 09 — BSI NET.1.2; ISO/IEC 27001:2022 Anhang A 8.2

Verwaltungszugänge zu Netzkomponenten sind abgesichert: eigene Verwaltungsnetze, individuelle Konten, keine Standardkennwörter, nicht benötigte Dienste deaktiviert.

Prüfhandlung Zehn Netzkomponenten auswählen und Konten, aktivierte Dienste und Zugriffswege prüfen.

Nachweise Konfigurationsauszüge, Kontenliste der Netzkomponenten

Prüfschritte 10 bis 12

Schritt 10

ISO/IEC 27001:2022 Anhang A 8.22

Funknetze sind gegen unbefugten Zugang gesichert und von internen Netzen getrennt, Gastzugänge haben keinen Zugriff auf interne Systeme.

Prüfhandlung Konfiguration von Funknetzen und Gastzugang prüfen und die Trennung durch einen Test belegen.

Nachweise Konfigurationsauszüge, Testergebnis

Schritt 11

ISO/IEC 27001:2022 Anhang A 8.16; BSI NET.1.1

Datenverkehr und Netzereignisse werden überwacht, auffällige Verbindungen erzeugen Alarme, die verfolgt werden.

Prüfhandlung Überwachung der Übergänge zum Internet und zwischen Zonen prüfen und drei Alarme nachverfolgen.

Nachweise Konfiguration der Überwachung, Alarmliste, Tickets

Schritt 12

NIS2-Richtlinie Art. 21 Abs. 2 lit. f

Die Wirksamkeit der Trennung wird regelmäßig durch Sicherheitstests der Netze überprüft, Befunde werden behoben.

Prüfhandlung Berichte der letzten Netzwerktests ansehen und prüfen, ob die Befunde behoben wurden.

Nachweise Testberichte, Maßnahmenliste

Unterlagenanforderung

Diese 8 Unterlagen vor Prüfungsbeginn anfordern

1. Netzwerksicherheitsrichtlinie
2. Netzpläne und Zonenmodell
3. Segmentierungskonzept
4. Regelwerksauszüge der Firewalls mit Begründungen
5. Bericht der letzten Regelüberprüfung
6. Änderungsprotokolle der Firewall und Änderungsanträge
7. Konfigurationsauszüge von VPN-Gateways und Netzkomponenten
8. Berichte der Netzwerktests

TYPISCHE FESTSTELLUNGEN

- Der Netzplan weicht von der Wirklichkeit ab, Übergänge zu Dienstleistern sind nicht dokumentiert.
- Benutzernetze erreichen Verwaltungsschnittstellen von Servern und Netzkomponenten.
- Firewall-Regeln sind seit Jahren nicht überprüft, es bestehen sehr weit gefasste Regeln ohne Begründung.
- Änderungen an Firewall-Regeln erfolgen ohne Änderungsantrag.
- Standardkonten oder Standardkennwörter sind auf Netzkomponenten aktiv.
- Gastzugänge sind nicht wirksam von internen Netzen getrennt.

Bibliothek Muster-Prüfprogramme

29 Muster-Prüfprogramme online

proauditmap.com/pruefprogramme/

Vollständiges Prüfpaket in ProAuditMap

proauditmap.com

ProAuditMap

Muster ohne Gewähr und keine Rechtsberatung. Gesetze, Verordnungen und Standards erscheinen nur als Fundstelle, Normtexte sind nicht abgedruckt. Passen Sie Umfang und Tiefe vor der Verwendung an Ihre Organisation, Ihre Risiken und die aktuelle Fassung der für Sie geltenden Vorschriften an. Stand: 13. Oktober 2026