Netzwerksicherheits­richtlinie

Vorlage

# Autorität und Überprüfung

## Dokumentenkontrolle und -prüfung

|  |  |
| --- | --- |
| **Dokumentenprüfung**  |  |
| Autor  |  |
| Eigentümer |  |
| Datum der Erstellung |  |
| Zuletzt überarbeitet von  |  |
| Datum der letzten Überarbeitung |  |

## Versionsverwaltung

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Datum der Genehmigung** | **Genehmigt durch**  | **Beschreibung der Änderung** |
| 1.0 |  |  |  |

# Intro

Die Netzsicherheit innerhalb des Unternehmens ist wichtig, denn sie ist Ihre erste Verteidigung gegen Angriffe von außen. Durch die Umsetzung wirksamer technischer und organisatorischer Netzwerksicherheitsmaßnahmen können Sie verhindern, dass Cyberkriminelle Ihre Infrastruktur angreifen, Ihre Kommunikation stören, unrechtmäßig Daten sammeln oder auf wichtige Anwendungen und Geräte zugreifen.

Dieses Strategiedokument ist Teil einer Reihe von Strategiedokumenten, die **[Organisation]** bei der Entwicklung einer soliden Cybersicherheitsstrategie unterstützen.

# Netzwerksicherheit

## Physische Sicherheit

Netzwerkkomponenten wie Firewalls und Switches sollten in speziellen Schränken untergebracht werden. Der Zugang zu diesen Schränken sollte auf speziell benanntes Personal beschränkt sein. Daten- und Stromkabel sollten vor Beschädigungen geschützt werden.

## Abtrennung von Netzwerken

Um zu verhindern, dass sich Schadsoftware und andere Malware im Netz ausbreitet, sollte das Netz als getrennte Topologie konzipiert sein. Die Systeme sollten sich in bestimmten virtuellen LANs (VLANs) befinden, die durch Firewall-Zugriffsregeln getrennt sind.

Die folgenden VLAN-Trennungsregeln müssen beachtet werden:

* Systeme, die Online-Dienste anbieten (d.h. eingehenden Datenverkehr aus dem Internet entgegennehmen), sollten von anderen Systemen getrennt werden.
* Die Netzwerkverwaltung erfolgt über ein separates VLAN.
* Systeme, die verbundene Dienste anbieten (d.h. eingehenden Datenverkehr aus nicht vertrauenswürdigen Netzen außer dem Internet annehmen), sollten von anderen Systemen getrennt werden.
* Endbenutzergeräte sollten von Servern getrennt werden.
* Nicht verwaltete Geräte sollten von verwalteten Geräten getrennt werden.
* Systeme mit unterschiedlichen Zwecken sollten getrennt werden.
* Die physischen Standorte sollten getrennt sein.
* Entwicklungs-, Test- und Produktionssysteme sollten getrennt werden.

## Firewalling

VLANs sollten durch Firewalls getrennt werden. Der Netzwerkverkehr zwischen VLANs und der Verkehr zu oder von nicht vertrauenswürdigen Netzwerken sollte blockiert werden, sofern nicht ausdrücklich verlangt wird, dass er offen ist. Der ausgehende Internetzugang für VLANs von Büroanwendern ist erlaubt, sofern er nicht die Sicherheit oder Leistung des Unternehmens beeinträchtigt. Der Verkehr kann priorisiert werden, um beispielsweise zu verhindern, dass Video- oder Musikstreams den arbeitsbezogenen Büroverkehr beeinträchtigen.

## VPN

Für Telearbeit oder Maschine-zu-Maschine-Kommunikation über nicht vertrauenswürdige Netze kann VPN zur Verschlüsselung von Netzwerkverkehr verwendet werden, der nicht standardmäßig verschlüsselt ist.

Der Zugang zum VPN und damit zu allen zugrundeliegenden Systemen der **[Organisation]** sollte nach Möglichkeit so konfiguriert werden, dass eine Form der Multi-Faktor-Authentifizierung verwendet wird, sodass eine unbefugte Person, die im Besitz kompromittierter Zugangsdaten der **[Organisation]** kommt, dasVPN der **[Organisation]** nicht nutzen kann.

## Sicherung von kabelgebundenen Netzwerken

Netzwerkanschlüsse sollten vor nicht vertrauenswürdigen Geräten geschützt werden. Wenn die physische Sicherheit gering ist, sollten Netzsicherheitstechniken wie MAC-Filterung oder Netzwerkzugangssicherheit eingesetzt werden, um nicht vertrauenswürdige Geräte zu blockieren oder zu isolieren.

## Sicherheit drahtloser Netzwerke

Wi-Fi verwendet verschiedene Standards für die Verschlüsselung und Authentifizierung. Im Folgenden sind die Methoden in der Reihenfolge ihrer besten Sicherheit aufgeführt (die erste ist die einzige sichere Methode):

1. WPA2 + AES
2. WPA + AES (nicht bevorzugt)
3. WPA + TKIP (nicht bevorzugt)
4. WEP (niemals verwenden)
5. Offenes Netz (nie benutzen)

Der Benutzerzugang sollte überprüft werden. Für die Authentifizierung von Wi-Fi-Netzen wird eine zentrale Benutzerdatenbank mit Namen bevorzugt. Die meisten Wi-Fi-Zugangspunkte in Unternehmen bieten LDAP- oder RADIUS-Unterstützung.

Nicht verwaltete Geräte sollten nur auf **[dedizierte Gast-WIFI-Netze]** zugreifen. DerNetzwerkverkehr zwischen Gastnetzen und den von **[Organisation]** verwalteten Netzen sollte verhindert werden.

# Verwaltung des Netzwerkes

* Ein High-Level-Netzwerkschema wird entwickelt und sicher gespeichert (gedruckt). Dieses Schema enthält die Hardware- und Funktionsbeschreibung sowie die notwendige (IP-)Adressierung. Dieses Schema wird in regelmäßigen Abständen aktualisiert.
* Verwaltungsanschlüsse sollten nur von befugtem Personal benutzt werden können und nicht mit dem Internet verbunden sein, es sei denn über VPN.
* Der Benutzerzugang zu den Verwaltungsanschlüssen sollte regelmäßig überwacht werden. Eine zentrale namentliche Benutzerdatenbank ist für die Authentifizierung des Verwaltungszugangs vorzuziehen.
* Die Installation oder Änderung von Netzwerkgeräten muss von oder in Absprache mit **[Organisation IT]** vorgenommen werden.
* Netzwerkinfrastrukturgeräte verfügen über eine Protokollierung, die sich auf die Überwachung und Kontrolle des Datenverkehrs durch Netzwerkzonen und verschiedene Vertrauensstufen konzentriert. Beispiele sind wichtige Administratorereignisse wie Anmeldung, Systemänderungen, Zurücksetzen von Passwörtern...
* Um die Verfügbarkeit und Leistung kritischer und vertraulicher Systeme zu gewährleisten, sollte das Vorhandensein von Service Level Agreements (SLAs) für diese Netzwerkkomponenten in Betracht gezogen werden.