Projektarbeit IHK Cyber Security Advisor

Richtlinie zur Netzwerksicherheit

zur Erlangung der Zertifizierung
IHK Cyber Security Advisor

Vorgelegt von: Ole [redacted]

Eingereicht am: 15.02.2025

Kurs: WB CS_06

Inhaltsverzeichnis

1 ByteBistro GmbH

1.1 Vorstellung des Unternehmens

ByteBistro GmbH ist ein innovatives Unternehmen mit Sitz in Deutschland, das sich auf digitale Lösungen für die Gastronomie spezialisiert hat. Mit einem Team von rund 150 Mitarbeitern bietet es eine cloudbasierte Plattform, die Restaurants, Cafés und Bars dabei unterstützt, Bestellungen, Zahlungen und Lieferungen effizient zu verwalten. Mit der ByteBistro-App können Kunden direkt von ihrem Smartphone aus Menüs durchsuchen, Bestellungen aufgeben und in Echtzeit verfolgen. Die Plattform wird von über 500 Restaurants in Deutschland genutzt und zählt täglich Tausende von Transaktionen.

Das Unternehmen legt großen Wert auf Benutzerfreundlichkeit, Verfügbarkeit und Datensicherheit, da es sowohl mit sensiblen Kundendaten (z. B. Zahlungsinformationen) als auch mit Betriebsdaten der Restaurants arbeitet.

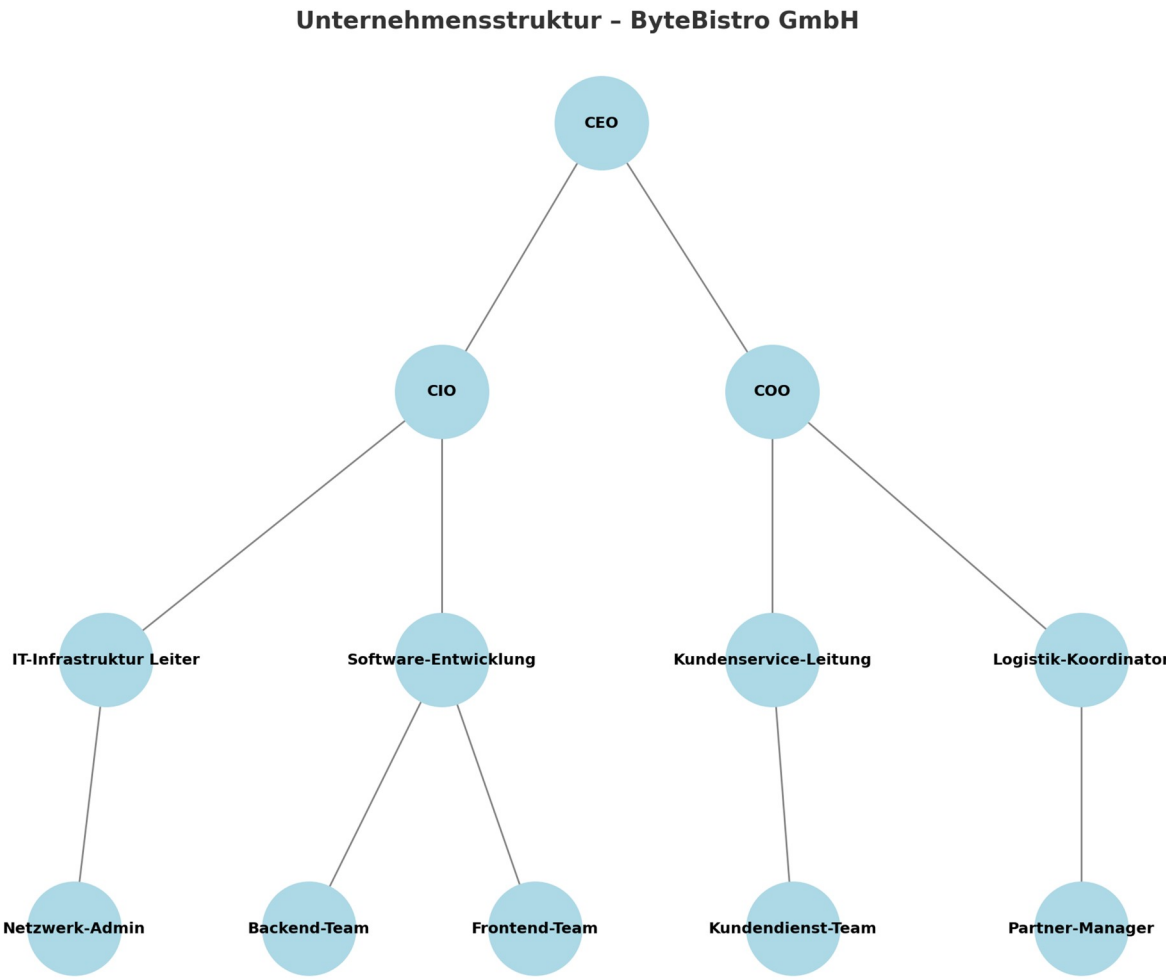
1.1 Leistungsportfolio

Bestell- und Zahlungsverarbeitung: Integration von Zahlungsdienstleistern wie PayPal, Kreditkarte und Sofortüberweisung.

Liefermanagement: Echtzeit-Tracking von Lieferungen.

Restaurant-Dashboard: Ein Dashboard zur Analyse von Verkaufszahlen und Bestellungen.

1.2 Unternehmensstruktur (Organigramm)



1.3 IT-Infrastruktur

ByteBistro betreibt eine hybride IT-Infrastruktur, die sowohl cloudbasierte Dienste als auch lokale Netzwerke für interne Arbeitsabläufe umfasst:

Netzwerk- und Serverstruktur:

Cloud-Umgebung:

ByteBistro nutzt eine Multi-Cloud-Strategie mit AWS (Amazon Web Services) und Microsoft Azure, um die Plattform zu hosten. Die Cloud-Server sind für Skalierbarkeit und hohe Verfügbarkeit konzipiert.

- Datenbankserver: PostgreSQL für Kundendaten.
- Applikationsserver: Containerisierte Anwendungen mit Docker, orchestriert durch Kubernetes.
- Backups: Automatische tägliche Backups, verschlüsselt und geografisch redundant gespeichert.

Lokales Firmennetzwerk:

Das Hauptbüro in Berlin ist mit einer modernen LAN/WLAN-Infrastruktur ausgestattet.

- Netzwerkgeräte: Router und Firewalls von Cisco, verwaltete Switches für die Verbindung von Endgeräten.
- Zugriffskontrolle: Zwei VLANs (Virtual Local Area Networks) trennen die internen Mitarbeitersysteme vom Gast-WLAN.

Endgeräte

- Mitarbeiter verwenden Laptops (Windows und macOS) sowie mobile Geräte für den Zugriff auf interne Systeme.
- Geräte sind durch Endpoint-Security-Software geschützt.

Sicherheitsmaßnahmen

Netzwerkschutz:

- Firewalls mit Intrusion Detection and Prevention Systems (IDPS).
- VPN für Remote-Arbeit.

Datenverschlüsselung:

- End-to-End-Verschlüsselung für Bestellungen und Zahlungsdaten.
- SSL/TLS für alle Netzwerkkommunikationen.

Zugriffsmanagement:

- Zwei-Faktor-Authentifizierung (2FA) für den Zugang zur Cloud-Plattform und kritischen Systemen.

Externe Partner und Schnittstellen

- Die Plattform ist mit APIs von Zahlungsdienstleistern und Lieferdiensten integriert. Diese Verbindungen werden durch verschlüsselte Protokolle und sichere Authentifizierungsmechanismen abgesichert.

2 SOLL-/IST-Abgleich

2.1 Ist-Zustand

Netzwerksicherheit

- Firewalls und IDPS sind implementiert.
- Netzwerke sind in VLANs getrennt (intern vs. Gast-WLAN).
- VPN-Zugänge sind für Remote-Mitarbeiter verfügbar.

Zugriffskontrolle

- Zwei-Faktor-Authentifizierung (2FA) wird genutzt.
- Rollenbasierter Zugriff auf Cloud-Systeme und Datenbanken.

Schwachstellenmanagement

- Regelmäßige Updates und Patches für Betriebssysteme und Software.
- Penetrationstests sind geplant, aber selten durchgeführt.

2.2 Erwarteter Soll-Zustand

Netzwerksicherheit

- Vollständig segmentiertes Netzwerk mit Microsegmentation.
- Automatische Erkennung und Reaktion auf Sicherheitsvorfälle.
- Verschlüsselung von Daten auch im lokalen Netzwerk (z. B. Layer-2-Verschlüsselung).

Zugriffskontrolle

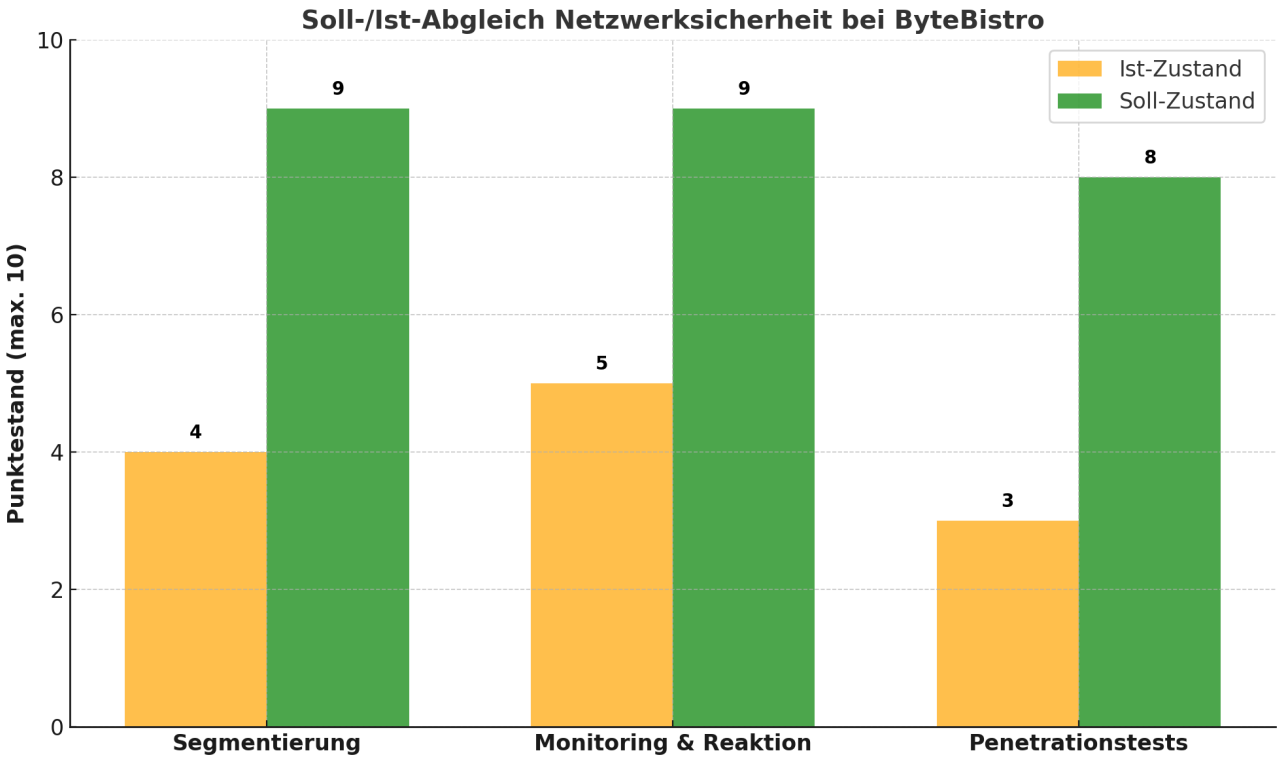
- Einhaltung des Prinzips der minimalen Rechte („Least Privilege“).
- Verbesserte Protokollierung und Überwachung aller Zugriffe.

Schwachstellenmanagement

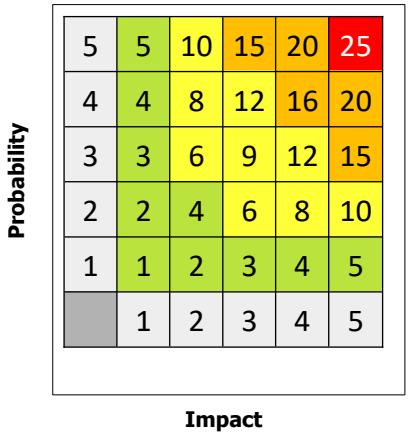
- Häufige Sicherheitsprüfungen und Penetrationstests.
- Automatisierte Tools für Schwachstellenscans.

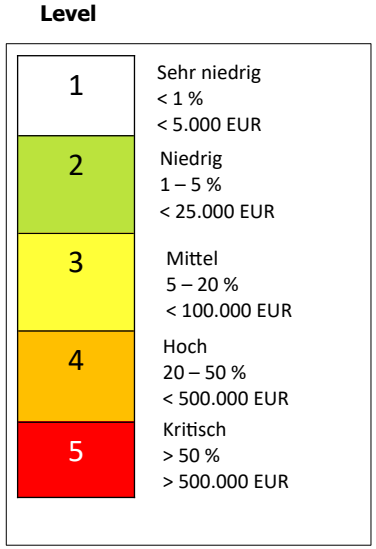
2.3 Soll-/Ist-Abgleich – Identifikation der Probleme

Themenbereich	Ist-Zustand	Soll-Zustand	Problem
1. Segmentierung	VLANs trennen nur internes Netzwerk und Gast-WLAN.	Mikrosegmentierung, um Systeme granularer zu trennen.	Sicherheitsvorfälle können durch lateral movement im Netzwerk eskalieren.
2. Monitoring & Reaktion	IDPS erkennt Bedrohungen, aber Reaktion erfolgt manuell.	Automatische Bedrohungserkennung und Reaktion.	Verzögerte Reaktion auf Angriffe kann zu Datenverlust führen.
3. Penetrationstests	Nur sporadisch und nicht umfassend durchgeführt.	Regelmäßige und tiefgehende Tests.	Schwachstellen bleiben unentdeckt und können von Angreifern ausgenutzt werden.



3 Risikoanalyse





Risiko-ID	Risiko	Auswirkung	Impact Level	Probability Level	Risikobewertung	Maßnahmen	Verantwortlich
R-001	Fehlende Mikrosegmentierung im Netzwerk	Erhöhtes Risiko für lateral Movement von Angreifern	4	4	16	Einführung von Mikrosegmentierung und granularer Kontrolle	IT-Abteilung
R-002	Unzureichendes Monitoring und verzögerte Reaktion	Verzögerte Reaktion auf Angriffe, erhöhte Schadensauswirkungen	5	4	20	Implentierung eines automatisierten SIEM-System zur Reaktion	IT-Abteilung, SOC-Team
R-003	Unregelmäßige Penetraionstests	Nicht erkannte Schwachstellen, potenzielle Sicherheitslücken	5	5	25	Regelmäßige und umfassende Penetrationstests durchführen	IT-Abteilung, externe Sicherheitsdienstleister

Netzwerksicherheitsrichtlinie

Dokumenteneigenschaften

Autor	Markus Bremer
Letzter Bearbeiter	Ole [redacted]
Titel	Netzwerksicherheitsrichtlinie
Art	Richtlinie
Hauptverantwortlicher	ByteBistro GmbH
Ansprechpartner	Markus Bremer (CEO) / Sebastian Krüger (IT-SIB)
E-Mail, Telefon	Markusbremer@bytebistro.de, 0176431955164
Version	1.2
In Kraft seit	01.01.2025
In Kraft gesetzt durch	Markus Bremer (CEO) / Sebastian Krüger (IT-SIB)
Überarbeitungsintervall	12 Monate
Nächste Überarbeitung	01.01.2026

Änderungs-History

Version	Änderung	Datum	Autor
1.0	Erster Entwurf des Dokuments	01.12.2024	Markus Bremer
1.1	Dokument in Kraft gesetzt	01.01.2025	Markus Bremer
1.2	Anpassung von ungenauen Formulierungen	05.01.2025	Ole [redacted]

Inhalt

1. Zielsetzung

Diese Richtlinie dient dem Schutz der Netzwerkinfrastruktur der ByteBistro GmbH vor unbefugtem Zugriff, Datenverlust, Cyberangriffen und anderen Sicherheitsrisiken. Sie stellt sicher, dass die Vertraulichkeit, Integrität und Verfügbarkeit der IT-Systeme gewährleistet werden.

2. Geltungsbereich

Diese Richtlinie gilt für alle Mitarbeiter, Partner, Dienstleister und externen Anbieter, die auf die Netzwerke und Systeme der ByteBistro GmbH zugreifen. Sie umfasst:

- Lokale Netzwerke (LAN)
- Drahtlose Netzwerke (WLAN)
- Cloud-basierte Netzwerke
- Verbindungen zu externen Netzwerken (z. B. Internet)

3. Begriffsdefinitionen

- **Netzwerksegmentierung:** Aufteilung des Netzwerks in separate Zonen, um die Sicherheit zu erhöhen.
- **SIEM:** Security Information and Event Management-System zur Erkennung und Reaktion auf Sicherheitsvorfälle.
- **2FA:** Zwei-Faktor-Authentifizierung zur Erhöhung der Zugriffssicherheit.

4. Verantwortlichkeiten

- **IT-Abteilung:** Verwaltung der Netzwerksicherheitsrichtlinien, Überwachung und Implementierung von Sicherheitsmaßnahmen.
- **SOC-Team (Security Operations Center):** Erkennung und Reaktion auf Bedrohungen.
- **Mitarbeiter:** Einhaltung der Richtlinie und sofortige Meldung von Sicherheitsvorfällen.

5. Richtlinienanforderungen

5.1. Netzwerksegmentierung

1. Das Unternehmensnetzwerk wird in folgende Segmente aufgeteilt:

Produktionsnetzwerk:

Das Produktionsnetzwerk wird für geschäftskritische Systeme verwendet, z. B. für Kassensysteme in den Restaurants und die zentralisierte Kundendatenbank.

➔ **Technische Umsetzung:** Die Server, auf denen die Kundendatenbank und Kassensoftware laufen, befinden sich in einem isolierten VLAN (Virtual Local Area Network). Dieses VLAN hat nur über spezifische Firewall-Regeln Zugriff auf andere Segmente, etwa zur Kommunikation mit dem Managementnetzwerk für Updates.

➔ **Tool-Vorgabe: "**FortiGate-Firewall" sorgt dafür, dass nur autorisierte Geräte wie Kassenterminals Zugriff auf dieses Segment haben.

Gäste-WLAN:

Das Gäste-WLAN wird vollständig vom internen Netzwerk getrennt, um zu verhindern, dass externe Benutzer Zugang zu sensiblen Unternehmensressourcen erhalten.

➔ **Technische Umsetzung:** Gäste verbinden sich über ein separates VLAN, das nur eine Internetverbindung ermöglicht. Es gibt keine Brücke oder Schnittstelle zum Produktions- oder Managementnetzwerk.

➔ **Tool-Vorgabe:** Ein UniFi Access Point von "Ubiquiti" wird konfiguriert, um Gäste über ein isoliertes WLAN-Netzwerk (SSID) zu leiten.

Managementnetzwerk:

Das Managementnetzwerk wird für administrative Aufgaben wie den Zugriff auf kritische Systeme und Server genutzt. Hier werden die Systeme gewartet, aktualisiert und überwacht.

➔ **Technische Umsetzung:** Nur administrativen Benutzern und Geräten mit dedizierten IP-Adressen wird über eine Multi-Faktor-Authentifizierung (z. B. 2FA) Zugriff gewährt. Dieses Segment ist durch strikte Firewall-Regeln geschützt und erlaubt keine ausgehenden Verbindungen ohne explizite Genehmigung.

➔ **Tool-Vorgabe:** Administratoren verwenden VPN-Software von "OpenVPN" oder "Cisco AnyConnect", um von außen sicher auf das Managementnetzwerk zuzugreifen.

2. Firewall-Regeln werden implementiert, um den Datenverkehr zwischen den Segmenten streng zu kontrollieren. Eine zentrale Firewall (FortiGate oder Palo Alto Networks) steuert den Datenverkehr zwischen den Segmenten.

Die Firewall erlaubt dem Produktionsnetzwerk, nur mit spezifischen Diensten im Managementnetzwerk (Backup-Servern oder Update-Servern) zu kommunizieren, blockiert jedoch jeden anderen Datenverkehr zwischen den Segmenten.

5.2. Zugangskontrolle

1. **Zwei-Faktor-Authentifizierung (2FA):**
   Der Zugriff auf alle Netzwerksysteme muss durch eine verpflichtende Zwei-Faktor-Authentifizierung (2FA) abgesichert werden. Hierbei ist "Microsoft Azure AD**"** oder "Duo Security**"** als Authentifizierungsdienst zu verwenden. Alle Benutzer, einschließlich interner Mitarbeiter und externer Anbieter, müssen die 2FA aktivieren, bevor sie Zugriff auf Unternehmensressourcen erhalten.

2. **Prinzip der minimalen Rechtevergabe (Least Privilege):**
   Zugriffsberechtigungen auf Netzwerksysteme und Datenbanken werden ausschließlich nach dem Prinzip der minimalen Rechtevergabe erteilt.
   - Jeder Benutzer erhält nur die Berechtigungen, die für die Erfüllung seiner Aufgaben unbedingt erforderlich sind.
   - Rollen und Berechtigungen sind regelmäßig zu überprüfen und bei Bedarf anzupassen.
   - **Tool-Vorgabe:** Berechtigungen werden durch "Okta Identity Management" oder "Active Directory" zentral verwaltet und überwacht.
3. **Zeitlich begrenzte Berechtigungen für externe Anbieter:**
   Externe Anbieter dürfen nur zeitlich begrenzte Berechtigungen erhalten, die auf die Dauer der erforderlichen Tätigkeit beschränkt sind.
   - Nach Ablauf der zugewiesenen Frist wird der Zugriff automatisch deaktiviert.
   - Externe Anbieter müssen sich vor der Freischaltung verifizieren und die Einhaltung der Sicherheitsrichtlinien bestätigen.
   - **Tool-Vorgabe:** Der Zugriff wird durch ein Privileged Access Management (PAM)-Tool, wie "CyberArk" oder "BeyondTrust", gesteuert.

5.3. Überwachung und Bedrohungserkennung

1. Ein SIEM-System (Splunk oder QRadar) wird zur Überwachung von Netzwerkaktivitäten und zur Erkennung von Sicherheitsvorfällen genutzt.
2. Alle Netzwerksysteme müssen Protokolle über Benutzeraktivitäten und sicherheitsrelevante Ereignisse speichern.
3. Alarme aus dem SIEM-System werden von einem dedizierten SOC-Team überprüft.

5.4. Sicherheitsupdates und Schwachstellenmanagement

1. Sicherheitsupdates und Patches müssen innerhalb von 14 Tagen nach Verfügbarkeit installiert werden.
2. Ein automatisiertes Schwachstellenmanagement-Tool identifiziert regelmäßig Risiken im Netzwerk. Hierfür wird entweder "Tenable Nessus" oder "Qualys Vulnerability Management" verwendet.
3. Kritische Schwachstellen müssen innerhalb von 48 Stunden behoben werden.

5.5. Penetrationstests und Audits

1. Penetrationstests werden halbjährlich durch ein internes und externes Team durchgeführt:
   - Der erste Penetrationstest des Jahres muss bis spätestens "31. Mai" abgeschlossen sein.
   - Der zweite Penetrationstest des Jahres muss bis spätestens "30. November" abgeschlossen sein.

2. Ergebnisse werden dokumentiert, und identifizierte Schwachstellen müssen innerhalb von 30 Tagen behoben werden.
3. Regelmäßige interne und externe Audits überprüfen die Einhaltung dieser Richtlinie.
    - Interne Audits werden jährlich durchgeführt, mit dem ersten Audit bis "31. März" und dem zweiten bis "30. September".
    - Externe Audits erfolgen alle zwei Jahre, beginnend bis "30. Juni" 2025.

5.6. Drahtlose Netzwerke (WLAN)

1. Alle WLAN-Verbindungen müssen mit WPA3 verschlüsselt werden.
    - Es ist sicherzustellen, dass nur WLAN-Geräte, die WPA3 unterstützen, mit dem Unternehmensnetzwerk verbunden werden können.

    ➔ **Vorgabe für Hardware:** Access Points von "Ubiquiti UniFi" oder "Cisco Meraki "sind einzusetzen, da sie WPA3 und fortschrittliche Sicherheitsfunktionen unterstützen.
2. Gästen wird nur Zugriff auf das dedizierte Gäste-WLAN gewährt.
    - **Zugriffskontrolle:** Gäste erhalten über ein Captive Portal Zugriff, das mit einem zeitlich begrenzten Zugangscode oder Voucher (generiert über UniFi oder Cisco Meraki) arbeitet.
3. Administrative Zugriffe auf WLAN-Geräte erfolgen ausschließlich über VPN-Verbindungen.

    ➔ **Vorgabe für VPN:** ByteBistro verwendet "OpenVPN" oder "Cisco AnyConnect", um eine verschlüsselte Verbindung zur Verwaltung der Access Points und Netzwerke herzustellen.

5.7. Notfallwiederherstellung (Disaster Recovery)

1. Ein umfassender Disaster-Recovery-Plan (DRP) muss für alle Netzwerksysteme vorliegen, der klare Prozesse zur Wiederherstellung der Verfügbarkeit und Integrität der Systeme im Falle eines Ausfalls definiert. Der Plan muss alle kritischen Systeme, Daten und die erforderlichen Ressourcen für die Wiederherstellung abdecken.
2. Regelmäßige Übungen zur Wiederherstellung der Netzwerkinfrastruktur werden mindestens jährlich durchgeführt. Diese Übungen müssen bis spätestens "31. März" jedes Jahres abgeschlossen sein.

6. Webfilterung

6.1. Kategoriebasierte Filterung

Es ist sicherzustellen, dass der Zugriff auf Websites, die schädliche oder unerwünschte Inhalte enthalten, unterbunden wird. Die Filterung muss mindestens die Kategorien Pornografie, Glücksspiel, Phishing, Filesharing sowie Social-Media-Seiten, die nicht geschäftsrelevant sind, umfassen. Hierfür ist "Cisco Umbrella" oder "Fortinet FortiGate" als zentrale Webfilterungslösung einzusetzen.

6.2. Blockierung von Uploadfunktionen

Der Zugriff auf Websites mit Uploadfunktionen, wie beispielsweise Filesharing-Dienste (z. B. WeTransfer oder Dropbox), ist zu blockieren, um Datenverlust und unbefugte Übertragungen zu verhindern. Dies ist durch die URL-Filterungsfunktionen der "Sophos XG Firewall" oder "Palo Alto Networks" zu gewährleisten.

6.3. Schutz vor Befehls- und Steuerungsservern

Verbindungen zu Command-and-Control-Servern, die in Verbindung mit Malware oder anderen schädlichen Aktivitäten stehen, sind strikt zu blockieren. Es ist ein SIEM-System ("Splunk" oder "QRadar") einzusetzen, um verdächtige Verbindungen zu erkennen und Bedrohungsdatenbanken von Threat Intelligence Services regelmäßig zu aktualisieren.

6.4. Blockierung illegaler Inhalte

Der Zugriff auf Websites mit illegalen Inhalten, einschließlich Kinderpornografie, Waffenhandel oder anderer krimineller Aktivitäten, ist uneingeschränkt zu unterbinden. Zur Umsetzung ist eine DNS-Filterlösung wie "OpenDNS" oder "Zscaler" verpflichtend einzusetzen, die kontinuierlich aktualisiert wird.

6.5. Regelung für Ausnahmen

Ausnahmen von der Webfilterung sind nur nach schriftlicher Genehmigung und in begründeten Fällen zulässig. Genehmigungsprozesse sind über ein zentrales Ticket-System ("Jira Service Desk") zu steuern. Die gewährten Ausnahmen sind zeitlich zu begrenzen und dokumentiert zu archivieren.

7. Schulung und Sensibilisierung

1. Alle Mitarbeiter müssen bis spätestens "31. Januar" jedes Jahres eine Schulung zu den Netzwerksicherheitsrichtlinien abgeschlossen haben.
2. Neue Mitarbeiter müssen die Schulung vor dem ersten Zugriff auf Unternehmenssysteme abschließen.
3. Zusätzliche Schulungen müssen nach Sicherheitsvorfällen oder Änderungen der Netzwerksicherheitsrichtlinie innerhalb von "30 Tagen" nach dem Vorfall oder der Änderung entsprechende Schulungen angeboten werden. Diese Schulungen werden von der IT-Abteilung organisiert und durchgeführt.

8. Kontrolle und Überprüfung

1. Diese Richtlinie wird mindestens bis zum "31. März" jedes Jahres von der IT-Abteilung überprüft und bei Bedarf aktualisiert. Änderungen werden dokumentiert und den relevanten Abteilungen mitgeteilt.
2. Die Einhaltung der Richtlinie wird mindestens halbjährlich durch interne Audits überprüft, wobei die ersten Audits bis spätestens "30. Juni" und die zweiten Audits bis spätestens "31. Dezember" jedes Jahres abgeschlossen sein müssen. Externe Prüfungen werden alle zwei Jahre durchgeführt, mit dem nächsten externen Audit spätestens bis zum "31. Dezember" 2025.
3. Verstöße gegen die Richtlinie werden innerhalb von 5 Werktagen nach Bekanntwerden durch die IT-Abteilung untersucht. Abhängig von der Schwere des Verstoßes können disziplinarische Maßnahmen ergriffen werden, die in Zusammenarbeit mit der Personalabteilung festgelegt werden.

9. Referenzen

- **ISO/IEC 27001**
- **NIST SP 800-53 (Rev. 5), AC-17, SC-7, SI-4**
- **BSI IT-Grundschutz, SYS.1.2, NET.3.1**
- **EU-DSGVO, Artikel 32**

10. Gültigkeit und Dokumenten-Handhabung

Diese Richtlinie tritt mit Genehmigung der Geschäftsführung (CEO) in Kraft und bleibt bis auf Widerruf gültig. Die Verantwortung für die regelmäßige Überprüfung und Aktualisierung des Dokuments liegt beim IT-Sicherheitsbeauftragter. Die Überprüfung erfolgt mindestens einmal jährlich, spätestens bis zum "31. Januar" jedes Jahres, um sicherzustellen, dass die Richtlinie aktuell, wirksam und angemessen bleibt.

Zur Bewertung der Wirksamkeit der Richtlinie sind folgende Punkte zu berücksichtigen:

- Anzahl der Vorfälle, die durch unbefugte Netzwerkzugriffe verursacht wurden.
- Durchschnittliche Reaktionszeit zur Identifizierung und Eindämmung von Netzwerkverletzungen.
- Jährliche Häufigkeit erfolgreicher Angriffe auf das Netzwerk.

Datum: 05.01.2025
Genehmigt durch: Markus Bremer, CEO

Markus Bremer
CEO

Sebastian Krüger
IT-SIB