

Risikoanalyse

für die

TOWERN3000 Projekt- & Medienagentur GmbH

Inhaltverzeichnis

1	Einleitung.....	3
2	Ausgangslage	4
3	Projektziel.....	4
4	IT-Security im Unternehmen.....	5
5.1	Erfassung aller eingesetzten Hardware und Softwarekomponenten und Identifikation unzureichend geschützter Systeme.....	5
5.2	Bewertung der Netzwerktopologie und möglicher Schwachstellen.....	6
5.3	Bewertung der Absicherung drahtloser und kabelgebundener Netzwerke	8
5.4	Einsatz und Konfiguration der Firewall.....	9
5.5	Prüfung der Benutzerkontenverwaltung und Rechtevergabe	10
5.6	Einsatz sicherer Authentifizierungsmethoden (z. B. Multi-Faktor-Authentifizierung)	11
5.7	Analyse von Sicherheitslücken in Anwendungen und Betriebssystemen.....	12
5.8	Regelmäßige Erstellung und Überprüfung von Backups	13

1 Einleitung

Im Zuge der fortschreitenden Digitalisierung und der zunehmenden Bedrohungslage im Bereich der IT-Sicherheit ist eine strukturierte Risikoanalyse unerlässlich. Ziel dieser IT-Risikoanalyse ist es, die bestehenden technischen und organisatorischen Maßnahmen der Towner3000 Projekt- & Medienagentur GmbH systematisch zu bewerten und potenzielle Schwachstellen in der IT-Infrastruktur zu identifizieren.

Dabei wurden sowohl Hardware- und Softwarekomponenten als auch Netzwerkstruktur, Benutzerverwaltung, Sicherheitsmechanismen und Backup-Verfahren untersucht. Die Analyse dient als Grundlage für konkrete Handlungsempfehlungen zur Erhöhung der IT-Sicherheit und zur Minimierung betrieblicher Risiken durch Cyberangriffe, Datenverlust oder Systemausfälle.

2 Ausgangslage

zweiP IT & WEB Solutions hat als IT-Dienstleister eine umfassende Risikoanalyse der aktuellen IT-Security Situation im Unternehmen durchgeführt.

Aus dieser Analyse ergab sich, dass die vorhandenen Sicherheitsmaßnahmen zwar eine gewisse Grundabsicherung bieten, jedoch auch deutliche Schwachstellen vorhanden sind.

3 Projektziel

Ziel dieser Risikoanalyse ist es, die IT-Sicherheitsstruktur des Unternehmens zu analysieren und geeignete Maßnahmen zur Verbesserung der Sicherheit zu definieren.

4 IT-Security im Unternehmen

Die Sicherheit der IT-Systeme der **Towner3000 Projekt- & Medienagentur GmbH** wurde basierend auf folgenden Punkten analysiert:

- Erfassung aller eingesetzten Hardware- und Softwarekomponenten und Identifikation veralteter oder unzureichend geschützter Systeme
- Bewertung der Netzwerktopologie und möglicher Schwachstellen
- Überprüfung der Absicherung drahtloser und kabelgebundener Netzwerke
- Einsatz und Konfiguration der Firewall
- Prüfung der Benutzerkontenverwaltung und Rechtevergabe
- Einsatz sicherer Authentifizierungsmethoden (z. B. Multi-Faktor-Authentifizierung)
- Analyse von Sicherheitslücken in Anwendungen und Betriebssystemen
- Regelmäßige Erstellung und Überprüfung von Backups

5.1 Erfassung aller eingesetzten Hardware und Softwarekomponenten und Identifikation unzureichend geschützter Systeme.

Die Erfassung der IT-Komponenten erfolgte mit Nmap, Lansweeper und manuellen Aufzeichnungen. Dabei wurden mehrere Windows-Clients mit Betriebssystemen unterhalb von Windows 11 festgestellt. Zudem erfüllen einige dieser Geräte nicht die Hardwareanforderungen für ein Upgrade auf Windows 11.

Risiken:

Veraltetes Betriebssystem (Windows 10):

- Keine oder eingeschränkte Sicherheitsupdates von Microsoft da End-of-Life am 14. Oktober 2025
- Bekannte Schwachstellen, die von Angreifern ausgenutzt werden können
- Erhöhtes Risiko für Ransomware, Trojaner oder Netzwerkwürmer

Unzureichende Hardware für Windows 11

- Keine Möglichkeit für zukünftige Sicherheits-Upgrades
- Potenzieller Verstoß gegen Compliance-Vorgaben (NIS2 - Lieferketten)
- Wirtschaftlich ineffiziente Wartung veralteter Hardware

Einsatz veralteter Software

- Veraltete Software ist anfällig für Malware oder Fehlfunktionen.

Auswirkungen:

- Erhöhte Angriffsfläche durch ungepatchte Systeme
- Potenzieller Datenverlust oder unautorisierter Datenzugriff
- Systemausfälle oder Betriebsunterbrechungen durch Malware
- Imageschaden und mögliche rechtliche Folgen bei Datenschutzverletzungen

Wahrscheinlichkeit: **Hoch**

Veraltete Betriebssysteme werden regelmäßig von automatisierten Scans und Exploits ins Visier genommen.

Schadenspotenzial: **Hoch**

Ein kompromittierter Client kann als Einfallstor für das gesamte Netzwerk dienen und zu großflächigen Ausfällen führen.

Empfohlene Maßnahmen:

Priorität	Maßnahme
Hoch	Bewertung der betroffenen Geräte hinsichtlich Upgrade-Fähigkeit
Hoch	Planung und Umsetzung einer Hardware-Refresh-Strategie für nicht upgradefähige Clients
Hoch	Ersatz veralteter Betriebssysteme durch unterstützte Versionen (mind. Windows 10 22H2)
Mittel	Update aller eingesetzten Softwareprodukte

5.2 Bewertung der Netzwerktopologie und möglicher Schwachstellen

Bewertung der Netzwerktopologie und möglicher Schwachstellen. Die eingesetzten Netzwerkkomponenten wurden vor Ort begutachtet und die Versionsstände (wenn möglich) dokumentiert. Teilweise lagen die Versionsstände mehrere Jahre zurück bzw. waren die Netzwerkkomponenten nicht verwaltbar. Im Zuge der Analyse wurde auch eingesetzte Hardware entdeckt, welche nicht mehr dem aktuellen Stand der Dinge entspricht (unmanaged 100Mbit Switches). Diese wirken sich neben der IT-Sicherheit auch negativ auf die Performance im Netzwerk aus.

Risiken:

- Veraltete Firmware enthält möglicherweise bekannte Sicherheitslücken, die nicht gepatcht wurden.
- Keine zentrale Kontrolle über Konfiguration, Protokollierung oder Monitoring von nicht verwaltbaren Geräten
- Unzureichende Segmentierung oder Zugriffskontrolle durch unmanaged Komponenten.
- Leistungsverlust und Engpässe bei datenintensiven Anwendungen oder Backups bei langsamer Geschwindigkeit.

Auswirkungen:

- Erhöhte Angriffsfläche für interne und externe Bedrohungen
- Fehlende Reaktionsmöglichkeiten bei einem Vorfall (keine Logs, kein Remote-Zugriff)
- Performanceprobleme, die zu Produktivitätsverlust führen
- Störungen bei sicherheitsrelevanten Diensten (z. B. Backup über Netzwerk)

Wahrscheinlichkeit: **Hoch**

Veraltete Komponenten und fehlende Verwaltungsfunktionen erhöhen das Risiko von Sicherheits- und Performanceproblemen erheblich.

Schadenspotenzial: **Hoch**

Ein einzelner veralteter oder unsicherer Netzwerkkomponentenpunkt kann als Einfallstor dienen oder kritische Dienste ausbremsen.

Empfohlene Maßnahmen:

Priorität	Maßnahme
Hoch	Austausch aller unmanaged Switches durch moderne, verwaltbare Modelle (mind. 1Gbit)
Hoch	Firmware-/Software-Update aller Netzwerkkomponenten
Mittel	Einführung eines zentralen Netzwerkinventars und Monitoringsystems
Mittel	Überprüfung der Netzwerktopologie auf Segmentierung und Sicherheitszonen
Mittel	Dokumentation aller Netzwerkpfade und Ports für Audits und bessere Transparenz

5.3 Bewertung der Absicherung drahtloser und kabelgebundener Netzwerke

Die Absicherung des lokalen Netzwerks (LAN/WLAN) wurde überprüft. WLAN-Verschlüsselung wird eingesetzt (WPA2), jedoch gibt es keine Vorkehrungen für den Zugriff auf das kabelgebundene Netzwerk (z. B. kein Port Security oder NAC) im Einsatz.

Risiken:

- **Unkontrollierter physischer Zugang zum LAN:** Jeder, der sich physisch mit einem freien Port verbindet, erhält Netzwerkzugang.
- **Keine Geräteauthentifizierung:** Systeme ohne Berechtigung können unbemerkt Netzwerkressourcen nutzen oder abhören.
- **Keine VLAN-Trennung / Zugriffskontrolle auf Switch-Ebene:** Angriffe durch interne Bedrohungen (z. B. manipulierte Clients, BYOD-Geräte).
- **WLAN-Sicherheit nur auf Basis von WPA2:** Ohne zusätzliche Maßnahmen kann ein kompromittiertes WLAN-Passwort den gesamten Netzwerkzugang ermöglichen.

Auswirkungen:

- Unautorisierter Zugriff auf interne Systeme und Daten
- Möglichkeit zur Ausnutzung von Netzwerkdiensten durch Angreifer
- Erhöhtes Risiko für Man-in-the-Middle-Angriffe und Abhörversuche
- Risiko der Infektion durch kompromittierte Geräte (z. B. Ransomware aus Gastnetz)

Wahrscheinlichkeit: **Hoch**

Insbesondere in nicht-segmentierten Netzwerken mit physischem Zugang zu Netzwerkports besteht ein realistisches Einfallstor für Angriffe.

Schadenspotenzial: **Hoch**

Ein nicht authentifiziertes Gerät im internen Netzwerk kann schwerwiegende Sicherheitsprobleme verursachen.

Empfohlene Maßnahmen:

Priorität	Maßnahme
Hoch	Einführung von Port-Security auf allen Switchports (MAC-based, max. Gerätezahl pro Port)

Priorität	Maßnahme
Hoch	Einführung eines NAC-Systems (z. B. 802.1X mit Zertifikaten)
Mittel	Überprüfung der WLAN-Konfiguration auf WPA3-Upgradefähigkeit und Client-Isolation
Mittel	Einführung von VLANs zur Segmentierung verschiedener Geräteklassen (z. B. Clients, Gäste)

5.4 Einsatz und Konfiguration der Firewall

Die Firewall-Konfiguration wurde zunächst auf die Firmware und anschließend auf die aktiven Regeln geprüft. Es wird eine renommierte Firewall eingesetzt, wobei ein Zugriff von extern nur über den vorherigen Aufbau einer VPN-Verbindung möglich ist.

Risiken:

- Veraltete Firmware (falls nicht regelmäßig geprüft)
- Fehlkonfigurationen in Firewall-Regeln
- Unzureichende Protokollierung oder Monitoring

Auswirkungen:

- Zugriff durch unautorisierte Personen bei erfolgreicher Umgehung des VPNs oder Missbrauch von Zugangsdaten
- Mögliche Kompromittierung sensibler Systeme (z. B. Server, interne Anwendungen)

Wahrscheinlichkeit: Mittel

Aufgrund der vorhandenen VPN-Beschränkung ist das Grundrisiko reduziert, jedoch abhängig von Wartung und Konfigurationssorgfalt.

Schadenspotenzial: Hoch

Ein erfolgreicher Angriff über einen Firewall-/VPN-Zugang kann umfassenden Zugriff auf interne Systeme ermöglichen.

Empfohlene Maßnahmen:

Priorität	Maßnahme
Hoch	Regelmäßige Prüfung und Aktualisierung der Firewall-Firmware
Hoch	Review aller aktiven Firewall-Regeln auf Notwendigkeit und Minimierung (Least Privilege-Prinzip)
Mittel	Protokollierung und zentrales Monitoring der Firewall-Aktivitäten aktivieren bzw. prüfen
Mittel	Regelmäßige Überprüfung der VPN-Benutzer und verwendeten Verschlüsselungs-/Authentifizierungsmechanismen

5.5 Prüfung der Benutzerkontenverwaltung und Rechtevergabe

Die Benutzerkontenverwaltung basiert auf Windows, ohne Active Directory. Die Rechtevergabe erfolgt ausschließlich über den Geschäftsführer.

Risiken:

- Fehlende zentrale Kontrolle
- Keine einheitliche Richtlinie zur Rechtevergabe
- Unzureichende Transparenz
- Single Point of Failure:
- Keine zentrale Passwort- oder Sicherheitsrichtlinienumsetzung:

Auswirkungen:

- Erhöhte Wahrscheinlichkeit für unautorisierte Zugriffe
- Verstöße gegen das Prinzip der minimalen Rechtevergabe (Least Privilege)
- Schwierige Nachvollziehbarkeit bei Sicherheitsvorfällen
- Verzögerungen bei Kontoverwaltung (z. B. bei Onboarding/Offboarding von Mitarbeitenden)

Wahrscheinlichkeit: Mittel

Manuelle, dezentrale Verwaltung ist fehleranfällig und im Alltagsbetrieb oft nicht nachhaltig umsetzbar.

Schadenspotenzial: Hoch

Ein überprivilegierter oder verwaister Zugang kann als Einfallstor für Malware oder Datenabfluss dienen.

Empfohlene Maßnahmen:

Priorität	Maßnahme
Hoch	Einführung eines zentralen Benutzerverzeichnisses (z. B. Microsoft Active Directory)
Hoch	Erstellung und Umsetzung einer Richtlinie zur Rechtevergabe und Benutzerverwaltung
Mittel	Schulung des Geschäftsführers und verantwortlicher Personen zur sicheren Kontenverwaltung
Mittel	Protokollierung von Kontoänderungen und Rechtevergabe implementieren

5.6 Einsatz sicherer Authentifizierungsmethoden (z. B. Multi-Faktor-Authentifizierung)

Bei der Authentifizierung wurde festgestellt, dass nur bei einer Ausnahme (M365) eine MFA aktiv ist, bei allen anderen Systemen authentifiziert man sich mit Benutzername und Passwort ohne zweiten Faktor.

Risiken:

- **Schwache oder mehrfach verwendete Passwörter** können leicht erraten oder durch Phishing abgefangen werden.
- **Kein zusätzlicher Schutz** bei kompromittierten Zugangsdaten → direkter Zugriff auf Systeme möglich.
- **Admin-Zugänge ohne MFA:** Besonders kritisch, da hier maximaler Schaden bei Missbrauch möglich ist.
- **Rechtliche Risiken:** Mangelnde Zugangssicherung kann im Schadensfall als fahrlässig gewertet werden.

Auswirkungen:

- Unautorisierter Zugriff auf vertrauliche Daten und Systeme
- Potenzieller Datenverlust, Systemmanipulation oder Verschlüsselung durch Ransomware
- Missbrauch von E-Mail-Konten zur Täuschung oder Phishing
- Reputationsschäden, wirtschaftliche Verluste und mögliche Bußgelder bei Datenschutzverletzungen

Wahrscheinlichkeit: **Hoch**

Passwortbasierte Logins sind heute das häufigste Angriffsziel – ohne MFA sind Systeme

besonders anfällig.

Schadenspotenzial: Sehr hoch

Ein kompromittiertes Konto mit weitreichenden Rechten kann ganze Systeme oder Datenbestände gefährden.

Empfohlene Maßnahmen:

Priorität	Maßnahme
Hoch	Einführung von MFA für alle sicherheitsrelevanten Systeme (Admin-Zugänge, Remote-Zugriffe, Mail etc.)
Mittel	Schulung der Mitarbeitenden zu sicheren Anmeldeverfahren und Phishing-Erkennung

5.7 Analyse von Sicherheitslücken in Anwendungen und Betriebssystemen

Es wird kein zentrales Update- und Patchmanagement System eingesetzt, Microsoft Windows Produkte werden nur basierend auf dem Update-Zyklus von Microsoft upgedatet. Allgemeine Software wird nicht aktualisiert, außer wenn eine neue Software angeschafft wird und diese eine veraltete Version ersetzt.

Risiken:

- Bekannte Sicherheitslücken in Softwarekomponenten bleiben unentdeckt und ungepatcht.
- Malware-Infektionen und Ransomware nutzen häufig bekannte Schwachstellen in veralteter Software.
- Manuelle oder unregelmäßige Updates führen zu Inkonsistenzen und erschweren Fehleranalysen.
- Keine Transparenz über Update-Status: Keine Möglichkeit zur Reaktion bei Sicherheitswarnungen (z. B. CVEs).

Auswirkungen:

- Höheres Risiko für externe Angriffe
- Interne Sicherheitsvorfälle durch kompromittierte Softwaremodule
- Betriebsunterbrechungen durch Schadsoftware oder instabile Softwarezustände

Wahrscheinlichkeit: Hoch

Ohne aktives Patchmanagement werden kritische Schwachstellen häufig übersehen oder verspätet behandelt.

Schadenspotenzial: Sehr hoch

Ungepatchte Schwachstellen gehören zu den häufigsten Ursachen für erfolgreiche Cyberangriffe.

Empfohlene Maßnahmen:

Priorität	Maßnahme
Hoch	Einführung eines zentralen Patchmanagement-Systems (z. B. WSUS, PDQ, ...)
Mittel	Durchführung monatlicher Schwachstellenscans zur Erkennung ungepatchter Software

5.8 Regelmäßige Erstellung und Überprüfung von Backups

Backups werden regelmäßig durchgeführt, einerseits durch Speichern in der Cloud (Nextcloud), zusätzlich existieren noch Backupmechanismen in Form von Backup Scripts auf dem Server.

Risiken:

- Keine zentrale Kontrolle oder Überwachung der Backup-Prozesse
- Keine regelmäßige Wiederherstellungsprüfung (Restore-Test)
- Unklare Redundanz und Versionierung: Keine Information, ob frühere Dateistände oder Systemzustände gesichert werden.

Auswirkungen:

- Datenverlust durch menschliches oder technisches Versagen
- Betriebsunterbrechung bei fehlgeschlagener Wiederherstellung
- Unvollständige Wiederherstellung nach Cyberangriff (z. B. Verschlüsselungstrojaner)
- Verstoß gegen Datenschutz- oder Aufbewahrungspflichten bei fehlenden Archivierungsfunktionen

Wahrscheinlichkeit: Mittel

Die Existenz von Backups ist positiv, aber ohne klare Prozesse und Kontrollmechanismen bleibt ein relevantes Risiko.

Schadenspotenzial: Hoch

Ein Datenverlust ohne funktionierendes Backup kann erhebliche finanzielle und betriebliche Auswirkungen haben

Empfohlene Maßnahmen:

Priorität	Maßnahme
Hoch	Einführung eines zentralen Patchmanagement-Systems (z. B. WSUS, PDQ, ...)
Mittel	Durchführung monatlicher Schwachstellenscans zur Erkennung ungepatchter Software