

Projektdokumentation IT-Sicherheit

für die

TOWERN3000 Projekt- & Medienagentur GmbH

Inhaltverzeichnis

1	Einleitung.....	3
2	Ausgangslage	4
3	Projektziel.....	4
4	Informationen zum Dokument	4
5	IT-Security im Unternehmen.....	5
5.1	Risikoanalyse IT-Sicherheit	5
5.1.1	Analyse der Sicherheit der eingesetzten IT-Systeme	5
5.1.2	Identifikation von Schwachstellen und Risiken	5
5.1.3	Erstellung Security Awareness Reviews	6
5.2	Beratung zur Optimierung	7
5.2.1	Beratung zur Verbesserung der IT-Infrastruktur hinsichtlich IT-Sicherheit	7
5.2.2	Empfehlungen zur Implementierung neuer Sicherheitslösungen und Best Practices	7
5.3	Einführung IT-Sicherheitsmanagementsystems.....	8
5.3.1	Einführung eines speziell angepassten Sicherheitsmanagementsystems	8
5.3.2	Entwicklung IT-Sicherheitsrichtlinie, IT- Benutzerrichtlinie und IT-Sicherheitshandbuch	8
5.4	Security Awareness Schulung	8
5.4.1	Erstellung angepasster Schulungsunterlagen	8
5.4.2	Grundschulung für die Einhaltung der Sicherheitsstandards.....	9
5.4.3	Quartalsmäßige Awareness Schulung mit aktualisieren Bedrohungen und Gegenmaßnahmen	9
5.4.4	Regelmäßige unangekündigte Tests (z. B. Phishing- Simulation, Social Engineering, ...)	9

1 Einleitung

In einer zunehmend digitalisierten Arbeitswelt sind Unternehmen verschiedensten Bedrohungen ausgesetzt, darunter Cyberangriffe, Datenverlust und Systemausfälle. Eine umfassende IT-Sicherheitsstrategie ist daher essenziell, um Risiken zu minimieren und die Integrität, Verfügbarkeit und Vertraulichkeit der IT-Systeme zu gewährleisten.

Diese Projektdokumentation befasst sich mit der Analyse und Optimierung der IT-Sicherheitsmaßnahmen in der **Towern3000 Projekt- & Medienagentur GmbH**. Ziel des Projekts ist es, bestehende Sicherheitslücken zu identifizieren, bewährte Sicherheitspraktiken zu implementieren und eine nachhaltige Sicherheitsarchitektur zu schaffen. Dazu wurden die aktuelle IT-Infrastruktur sowie bestehende Prozesse untersucht, Schwachstellen ermittelt und Maßnahmen zur Verbesserung der Sicherheit entwickelt.

Um im Unternehmen auch ein anhaltendes Bewusstsein für IT-Sicherheit zu schaffen, werden entsprechende Richtlinien entwickelt und regelmäßige Schulungen zum Thema IT-Sicherheit geplant und durchgeführt werden.

2 Ausgangslage

zweiP IT & WEB Solutions hat als IT-Dienstleister eine umfassende Ist-Analyse 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, insbesondere im Bereich des Patch-Managements, der Zugangskontrollen und der Netzwerksicherheit.

3 Projektziel

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

4 Informationen zum Dokument

Die unter Punkt 5 (IT-Security im Unternehmen) folgenden Analysen beziehen sich auf die in einem Gespräch mit der Geschäftsführung der Towner 3000 Projekt- und Medienagentur GmbH definierten IT-Security Prozesse, die im Jahr 2024, als die derzeit wichtigsten identifiziert wurden.

5 IT-Security im Unternehmen

5.1 Risikoanalyse IT-Sicherheit

5.1.1 Analyse der Sicherheit der eingesetzten IT-Systeme

Die Sicherheit der IT-Systeme der **Towern3000 Projekt- & Medienagentur GmbH** wurde basierend auf folgenden Punkten analysiert:

- Erfassung aller eingesetzten Hardware- und Softwarekomponenten
- 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

5.1.2 Identifikation von Schwachstellen und Risiken

Basierend auf der in Punkt 5.1.1 durchgeführten Analyse wurden folgende Schwachstellen und Risiken gefunden und in diesem Punkt kurz zusammengefasst.

- **Erfassung aller eingesetzten Hardware- und Softwarekomponenten**
Bei der Erfassung der Hard- und Softwarekomponenten wurde im Unternehmen mehrere Windows Clients mit Betriebssystem Versionen kleiner Windows 11 gefunden. Zusätzlich ergab die Analyse, dass einige Geräte die Hardwareanforderungen für Windows 11 nicht mehr erfüllen.
- **Identifikation veralteter oder unzureichend geschützter Systeme**
Die im ersten Punkt beschriebenen Systeme wurden identifiziert.
- **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.

- **Überprüfung 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.
- **Einsatz und Konfiguration der Firewall**
Die Firewall Konfiguration wurde einerseits auf Firmware und anschließend auf die aktiven Regeln geprüft.
- **Prüfung der Benutzerkontenverwaltung und Rechtevergabe**
Die Benutzerkontenverwaltung basiert auf Windows, ohne Active Directory. Die Rechtevergabe erfolgt ausschließlich über den Geschäftsführer.
- **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.
- **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.
- **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.

5.1.3 Erstellung Security Awareness Reviews

Basierend auf den Erkenntnissen der Punkte 5.1.1 bzw. 5.1.2 wurde ein Security Awareness Review erstellt, in welchem die möglichen Sicherheitsrisiken nach aktuellem Stand der Technik evaluiert wurden.

5.2 Beratung zur Optimierung

5.2.1 Beratung zur Verbesserung der IT-Infrastruktur hinsichtlich IT-Sicherheit

Das Security Awareness Review wurde in einem vor Ort Termin der Geschäftsführung der **Towner3000 Projekt- & Medienagentur GmbH** im Zuge eines Management Meetings präsentiert und die weitere Vorgehensweise grob festgelegt

5.2.2 Empfehlungen zur Implementierung neuer Sicherheitslösungen und Best Practices

1. **Modernisierung der Hard- und Softwarelandschaft**
 - Priorisierte Migration aller Windows-Clients auf Windows 11, sofern hardwareseitig möglich.
 - Austausch nicht kompatibler Geräte durch neue Hardware
2. **Verbesserung der Netzwerksicherheit**
 - Austausch veralteter, nicht verwaltbarer Netzwerkkomponenten (z. B. 100Mbit-Switches) durch moderne, managebare Geräte mit Sicherheitsfunktionen.
 - Einführung von Port Security oder Network Access Control (NAC), um unautorisierten Zugriff auf das kabelgebundene Netzwerk zu verhindern.
 - Aktualisierung der WLAN-Verschlüsselung auf WPA3
3. **Optimierung der Firewall- und Zugriffskontrollen**
 - Regelmäßige Überprüfung und Aktualisierung der Firewall-Firmware und -Regeln zur Anpassung an aktuelle Bedrohungslagen.
 - Implementierung einer zentralen Benutzerverwaltung, idealerweise über ein Active Directory (AD).
4. **Einführung sicherer Authentifizierungsverfahren**
 - Umsetzung einer verpflichtenden Multi-Faktor-Authentifizierung (MFA) für alle geschäftskritischen Systeme.
 - Einführung von Passwort-Management-Richtlinien, um die Nutzung sicherer Passwörter zu gewährleisten.
5. **Zentrales Patch- und Update-Management**
 - Einführung eines zentralen Patch-Management-Systems zur regelmäßigen Aktualisierung von Betriebssystemen und Software.
 - Definierte Prozesse zur schnellen Bereitstellung sicherheitskritischer Updates.
6. **Sicherung und Überprüfung von Backups**
 - Erweiterung der Backup-Strategie um eine automatisierte, versionierte Sicherung mit regelmäßigen Tests zur Wiederherstellung.

5.3 Einführung IT-Sicherheitsmanagementsystems

5.3.1 Einführung eines speziell angepassten Sicherheitsmanagementsystems

Aufgrund der in den vorangegangenen Punkten analysierten Sicherheitsprobleme wurde gemeinsam mit der Geschäftsführung entschieden, dass vor der Einführung eines IT-Sicherheitsmanagementsystems noch zu viele grundlegende IT-Sicherheitsmaßnahmen umgesetzt werden müssen.

Daher wurde der Schwerpunkt auf die Implementierung von Sicherheitslösungen, die Erstellung von Richtlinien und die regelmäßige Durchführung von Schulungen der Mitarbeiter gelegt.

5.3.2 Entwicklung IT-Sicherheitsrichtlinie, IT-Benutzerrichtlinie und IT-Sicherheitshandbuch

Für die **Towern3000 Projekt- & Medienagentur GmbH** wurden folgende Richtlinien erarbeitet.

- IT-Sicherheitsrichtlinie (Strategische IT-Security Ausrichtung für Geschäftsführung)
- IT-Benutzerrichtlinie (Anweisung für Mitarbeiter zur Unterzeichnung)
- IT-Sicherheitshandbuch (Handbuch für Notfallmanagement)

5.4 Security Awareness Schulung

5.4.1 Erstellung angepasster Schulungsunterlagen

Die IT- und IT-Security-Schulungsunterlagen wurden erstellt, um Mitarbeiter der **Towern3000 Projekt- & Medienagentur GmbH** dabei zu unterstützen, ihre technischen Fähigkeiten zu verbessern und sicher mit IT-Systemen umzugehen. Sie vermitteln praxisnahe Anleitungen zur Nutzung von Software sowie wichtige Sicherheitsmaßnahmen, um Daten und Systeme vor Bedrohungen zu schützen.

Themen wie Passwortsicherheit, Phishing-Erkennung und sicheres Arbeiten im Homeoffice stehen im Fokus. Durch diese Schulung wird nicht nur die Produktivität gesteigert, sondern auch die IT-Sicherheit des Unternehmens nachhaltig verbessert.

5.4.2 Grundschulung für die Einhaltung der Sicherheitsstandards

Die Grundschulung zur Einhaltung der Sicherheitsstandards wurde durchgeführt, um das Bewusstsein der Mitarbeiter für IT-Sicherheit zu schärfen und die Einhaltung wichtiger Schutzmaßnahmen im Unternehmen sicherzustellen. Ziel war es, Risiken wie Phishing, Datenlecks und unsichere Passwörter zu minimieren.

Die Schulung erfolgte in einem praxisnahen Format vor Ort, das sowohl theoretische Grundlagen als auch interaktive Übungen umfasste. Die Mitarbeiter wurden über aktuelle Bedrohungen, sichere Passwortrichtlinien, den Umgang mit sensiblen Daten und die Erkennung von Cyberangriffen informiert. Durch praxisnahe Beispiele und Tests wurde das erlernte Wissen gefestigt, sodass alle Teilnehmer die Sicherheitsstandards im Arbeitsalltag effektiv umsetzen können.

5.4.3 Quartalsmäßige Awareness Schulung mit aktualisieren Bedrohungen und Gegenmaßnahmen

Die quartalsmäßigen Awareness-Schulungen wurden als kompakte Online-Sessions durchgeführt, um Mitarbeiter regelmäßig über aktuelle Bedrohungen und geeignete Gegenmaßnahmen zu informieren. Diese Schulungen fanden in einem kleineren Rahmen online statt.

Jede Schulung behandelte die neuesten Cyber-Bedrohungen wie Phishing-Angriffe, Ransomware oder Social Engineering und erläuterte effektive Schutzmaßnahmen. Die Inhalte wurden an aktuelle Entwicklungen angepasst, sodass Mitarbeiter stets auf dem neuesten Stand der IT-Sicherheit blieben. Durch Live-Demonstrationen, Fallbeispiele und kurze Tests wurde das Wissen praxisnah vermittelt und gefestigt. Zudem gab es eine Fragerunde, in der individuelle Sicherheitsfragen geklärt werden konnten.

Wenn neue Mitarbeiter in das Unternehmen eingetreten sind, wurde für diese eine separate Grundschulung (siehe Punkt 5.4.2) online durchgeführt.

5.4.4 Regelmäßige unangekündigte Tests (z. B. Phishing-Simulation, Social Engineering, ...)

Regelmäßige unangekündigte Tests (Phishing) werden derzeit manuell von Mitarbeiter der zweiP IT & WEB Solutions durchgeführt. Um diese Tests zu automatisieren, wird aktuell Software evaluiert, die diesen Prozess automatisieren könne.