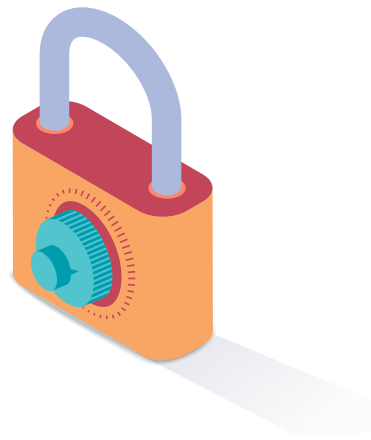
Semerad IT Consulting

CYBER SECURITY AUDIT CHECKLISTE

www.semerad.at

CYBER SECURITY
AUDIT DEFINITION



Ein Cyber Security Audit dient dazu, Schwachstellen in der IT-Sicherheit eines Unternehmens zu identifizieren und Bedrohungen vorzubeugen. Dabei wird eine ausführliche Analyse der Cyber Security und IT-Struktur des Unternehmens durchgeführt, um so alle Probleme aufzudecken und Lösungen für sie zu finden.

Deshalb muss ein Cyber Security Audit auch in regelmäßigen Abständen erstellt werden, um so auf dem neuesten Stand zu bleiben und kontinuierlich die Sicherheit Ihres Unternehmens zu verbessern. Bei großen Unternehmen mit einer hohen Datenmenge sollte ein solches Audit einmal pro Monat durchgeführt werden, bei kleineren Unternehmen kann es ausreichend sein, auch nur zweimal pro Jahr ein Audit zu erstellen.

Neben der Sicherheit Ihrer Daten ist ein Cyber Security Audit auch relevant, um Datenschutzverletzungen zu verhindern und so die Reputation Ihres Unternehmens aufrecht zu erhalten. Das Audit ist daher allgemein notwendig, um die Sicherheit Ihres Unternehmens zu bewahren und ist der grundlegende Baustein für alle Maßnahmen der IT-Sicherheit.

VORTEILE

- Guter Überblick über die aktuelle Lage des IT Systems
- Fehlerquellen und Sicherheitsbedrohungen frühzeitig eliminiert
- Verbesserungspotenziale entdecken
- Potenzielle Kosten durch etwaige Schäden einsparen
- Erhaltung eines positiven Image

1. HARDWARE ÜBERPRÜFEN

Stellen Sie sicher, dass sämtliche Hardwarekomponenten, einschließlich Computer, Mobiltelefone und Datenträger, im Inventar erfasst sind. Dies gewährleistet, dass nur autorisierte Geräte im Netzwerk aktiv sind.

☐ Erstellen Sie ein Inventar

Beginnen Sie mit der Erstellung eines vollständigen Inventars aller Hardwaregeräte im Unternehmen, einschließlich Computer, Laptops, Mobiltelefone und externer Datenträger.

☐ Überprüfen Sie die Autorisierung

Stellen Sie sicher, dass nur autorisierte Geräte mit gültigen Sicherheitszertifikaten im Netzwerk zugelassen sind.

☐ Führen Sie eine physische Inspektion durch

Planen Sie regelmäßige physische Inspektionen, um nicht autorisierte Hardwarekomponenten zu identifizieren und zu entfernen.

☐ Kontrollieren Sie Sicherheitsmaßnahmen

Überprüfen Sie, ob Sicherheitsmaßnahmen wie Festplattenverschlüsselung, Passwortschutz und Remote-Wipe-Funktionen auf Mobilgeräten aktiviert sind.

2. SOFTWARE ÜBERPRÜFEN

Erstellen Sie eine umfassende Liste aller Softwareanwendungen im Unternehmen und überprüfen Sie deren Lizenzen und Aktualität. Klare Richtlinien für die Installation von Software helfen, unautorisierte Anwendungen zu vermeiden.

☐ Erstellen Sie ein Inventar

Eine detaillierte Liste ermöglicht es, sicherheits-relevante Softwareanwendungen zu identifizieren und sicherzustellen, dass Sicherheitsmaßnahmen implementiert sind.

☐ Überprüfen Sie die Lizenzen

Überprüfen Sie die Lizenzinformationen jeder Softwareanwendung, um sicherzustellen, dass alle Anwendungen legal und lizenziert sind.

☐ Implementieren Sie ein Patch-Management

Implementieren Sie ein effektives Patch-Management-System, um sicherzustellen, dass alle Softwareanwendungen auf dem neuesten Stand sind und bekannte Sicherheitslücken geschlossen werden.

☐ Legen Sie Richtlinien fest

Etablieren Sie klare Richtlinien für die Installation von Software durch Mitarbeiter, um unautorisierte Anwendungen zu verhindern.

3. ZUGRIFFSBERECH-TIGUNGEN CHECKEN

Überprüfen Sie regelmäßig die Zugriffsrechte der Mitarbeiter auf sensible Daten und gewährleisten Sie das Prinzip der minimalen Berechtigungen. Zugriffsaktivitäten sollten zudem dokumentiert werden, um verdächtige Aktivitäten frühzeitig zu erkennen.

☐ Überprüfen Sie Zugriffsrechte

Kontrollieren Sie regelmäßig die Zugriffsrechte der Mitarbeiter auf sensible Daten. Das Prinzip der minimalen Berechtigung sorgt dafür, dass einem Benutzer nur diejenigen Berechtigungen gewährt werden, die unbedingt erforderlich sind.

☐ Prozess für Mitarbeiterwechsel

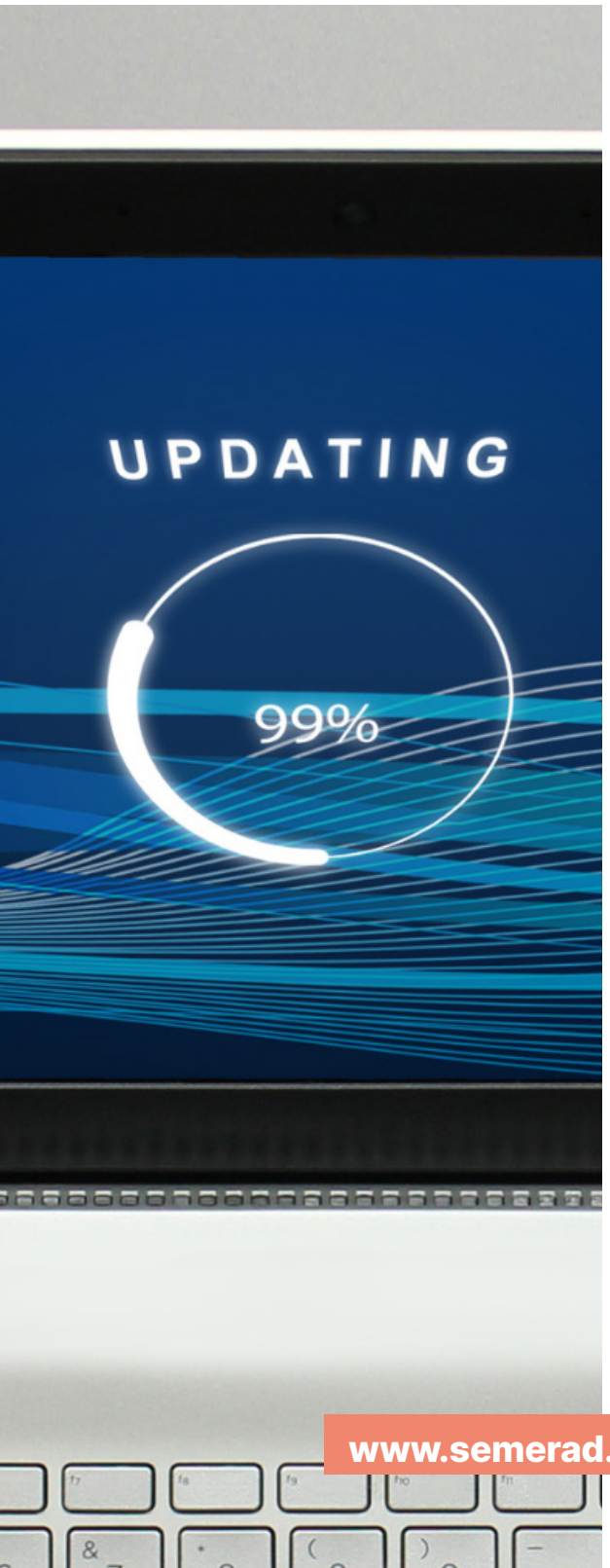
Implementieren Sie einen effizienten Prozess zur sofortigen Deaktivierung von Zugriffsrechten für Mitarbeiter, die das Unternehmen verlassen oder ihre Position ändern.

☐ Überwachung & Protokollierung

Verfolgen und dokumentieren Sie Zugriffsaktivitäten, um verdächtige Aktivitäten frühzeitig zu erkennen und darauf zu reagieren.

4. UPDATES DURCHFÜHREN

Software-Updates enthalten oft Patches, die Sicherheitslücken schließen. Durch regelmäßige Updates werden diese Lücken geschlossen und die Sicherheit des gesamten Systems gestärkt. In vielen Branchen und Unternehmen sind außerdem Compliance-Vorgaben und Sicherheitsstandards zu beachten.



☐ Aktivieren Sie automatische Updates

Aktivieren Sie automatische Updates für Betriebssysteme und alle sicherheitsrelevanten Softwareanwendungen.

☐ Führen Sie manuelle Überprüfungen durch

Planen Sie regelmäßige manuelle Überprüfungen, um sicherzustellen, dass automatische Updates ordnungsgemäß durchgeführt wurden.

☐ Erstellen Sie einen Eskalationsplan

Ein Eskalationsplan dokumentiert den Umgang mit kritischen Sicherheitslücken und dringenden Softwareaktualisierungen. Dieser gewährleistet eine schnelle Reaktionszeit, effektive Kommunikation und klärt Verantwortlichkeiten.

5. BROWSER & E-MAIL SYSTEME CHECKEN

Die Überprüfung von Browsern und E-Mail-Systemen ist in der IT und Cyber Security von entscheidender Bedeutung, da diese beiden Komponenten oft Einfallstore für verschiedene Arten von Bedrohungen, wie Phishing oder Malware, sind.

☐ Sicherheitskonfigurationen

Konfigurieren Sie Webbrowser und E-Mail-Systeme mit Sicherheitsfunktionen wie Phishing-Erkennung und sicherem Browsing.

☐ Führen Sie Mitarbeiterschulungen durch

Regelmäßige Schulungen für Mitarbeiter gewährleisten, dass diese über die neuesten Phishing-Taktiken und Social-Engineering-Angriffe informiert bleiben und sich den Risiken bewusst sind.

☐ Implementieren Sie Filtermechanismen

Filtermechanismen für E-Mails minimieren den Empfang von schädlichen Inhalten. Diese Mechanismen können auf Basis von Signaturen, Verhaltensanalysen und anderen Parametern arbeiten.

☐ Aktivieren Sie E-Mail Verschlüsselungen

Nutzen Sie die Verschlüsselung für E-Mails, insbesondere wenn vertrauliche Informationen übertragen werden, die es gilt zu schützen.

6. MALWARE-PROGRAMM AKTUELL HALTEN

Stellen Sie sicher, dass auf allen Geräten aktuelle Antiviren- und Anti-Malware-Programme installiert sind. Des Weiteren sollten Sie regelmäßige Scans durchführen, um sicherzustellen, dass keine Schadsoftware vorhanden ist.

☐ Antivirus- & Anti-Malware-Software

Gehen Sie sicher, dass alle Geräte mit aktueller Antivirus- und Anti-Malware-Software ausgestattet sind. Diese Programme sollten regelmäßig aktualisiert und auf dem neuesten Stand gehalten werden.

☐ Führen Sie regelmäßige Scans durch

Planen Sie regelmäßige Scans auf allen Geräten, um potenzielle Malware zu erkennen und zu entfernen. Dies umfasst nicht nur Desktop-Computer, sondern auch Server und mobile Geräte.

☐ Implementieren Sie Verhaltensanalysen

Integrieren Sie Technologien zur Verhaltensanalyse in Ihre Sicherheitslösungen. Diese können verdächtige Aktivitäten erkennen, die auf Malware hinweisen, selbst wenn herkömmliche Signaturen nicht vorhanden sind.

☐ Umgang mit verdächtigen Dateien

Legen Sie klare Richtlinien dafür fest, wie mit verdächtigen Dateien umzugehen ist. Dies kann die Quarantäne von Dateien, Benachrichtigungen an Sicherheitspersonal und automatische Reaktionen umfassen.

7. IT-SICHERHEIT KONTROLLIEREN

Die Einhaltung von Sicherheitsstandards, der Schutz vor Sicherheitsbedrohungen und das Risikomanagement gehören zu den wesentlichen Aufgaben in der Cyber Security. Das Sicherheitslevel sollte konstant hoch gehalten werden, um gegen Bedrohungen gewappnet zu sein.

☐ Überprüfen Sie Sicherheitsrichtlinien

Regelmäßige Überprüfung und Aktualisierung von Sicherheitsrichtlinien, um sicherzustellen, dass sie den aktuellen Bedrohungen und Compliance-Anforderungen entsprechen.

☐ Führen Sie interne Audits durch

Planen Sie regelmäßige interne Audits, um die Einhaltung von Sicherheitsrichtlinien zu überprüfen. Dies kann die Überprüfung von Zugriffsprotokollen, Konfigurationseinstellungen und anderen sicherheitsrelevanten Parametern umfassen.

☐ Notfallvorsorge & Wiederherstellungspläne

Überprüfen und aktualisieren Sie regelmäßig Notfallvorsorge- und Wiederherstellungspläne. Stellen Sie sicher, dass alle Teammitglieder mit den Verfahren vertraut sind, um im Ernstfall schnell handeln zu können.

Semerad IT Consulting GmbH

Schönbrunnerstaße 293/4/3
A – 1120 Wien

01 9971333

www.semerad.at