CHECKLISTE FÜR MEHR IT SICHERHEIT

25 PUNKTE »
SOFORTMASSNAHMEN
FÜR DEN SCHUTZ
IHRES UNTERNEHMENS

devial

INHALTSVERZEICHNIS

Schockierende Realität: Alle 11 Sekunden wird ein Unternehmen weltweit Opfer eines Cyberangriffs. Für kleine und mittelständische Unternehmen kann ein solcher Schlag existenzbedrohend sein.

Doch es gibt gute Nachrichten: Die meisten Angriffe nutzen bekannte Schwachstellen aus – Lücken, die mit der richtigen Strategie rechtzeitig erkannt und geschlossen werden können.

Diese Checkliste ist Ihr praktischer Leitfaden, um Ihr Unternehmen proaktiv zu schützen.

SOFORTMASSNAHMEN

☐ 1. STANDARD-PASSWÖRTER ELIMINIEREN

Admin & Passwort

Prüfen: Alle Netzwerkgeräte (Router, Switches, Drucker, WLAN-Access-Points, IoT-Geräte).

Aktion: Standard-Passwörter wie "*admin*", "*password*", "*123456*" sofort ändern und durch starke, individuelle Passwörter ersetzen.

Kritikalität: HOCH – Rund 81% der Datenschutzverletzungen nutzen schwache oder gestohlene Passwörter als ersten Angriffsvektor.

☐ 2. ADMINISTRATOR-KONTEN INVENTARISIEREN

Admin & Passwort

Prüfen: Wer hat Admin-Rechte in Ihrem System? (Windows, Linux, Datenbanken, Cloud-Dienste).

Aktion: Eine vollständige Liste aller Admin-Accounts erstellen.

Sofortaktion: Unbekannte oder nicht mehr benötigte Accounts umgehend deaktivieren oder löschen.

SOFORTMASSNAHMEN

☐ 3. MULTI-FAKTOR-AUTHENTIFIZIERUNG (MFA) AKTIVIEREN

Admin & Passwort

Wo: Alle Admin-Accounts, E-Mail-Systeme, Cloud-Services und Remote-Zugänge (*VPN, RDP*).

Priorität: Microsoft 365, Google Workspace, externe Remote-Zugänge.

Schutzfaktor: MFA verhindert bis zu 99,9% der erfolgreichen Account-Übernahmen durch Phishing oder gestohlene Zugangsdaten.

☐ 4. FIREWALL-STATUS ÜBERPRÜFEN

Netzwerk Sicherheit

Prüfen: Ist Ihre Firewall aktiv, korrekt konfiguriert und aktuell?

Aktion: Datum der letzten Update-Prüfung und aktive Regelwerke kontrollieren.

Warnsignal: Firewall-Hardware älter als 5 Jahre oder Software nie aktualisiert.

SOFORTMASSNAHMEN

☐ 5. OFFENE PORTS MINIMIEREN

Netzwerk Sicherheit

Scan: Führen Sie einen externen Port-Scan Ihrer Unternehmens-IP-Adressen durch (*z.B. mit Online-Tools oder nmap*).

Regel: Nur unbedingt notwendige Ports für Ihre Geschäftsprozesse öffnen.

Sofortaktion: Unbekannte oder nicht benötigte offene Ports **schließen**.

☐ 6. VPN-SICHERHEIT GEWÄHRLEISTEN

Netzwerk Sicherheit

Prüfen: Aktualität der VPN-Clients und Benutzerberechtigungen.

Aktion: Veraltete VPN-Clients aktualisieren und nicht mehr benötigte Benutzerzugänge deaktivieren.

Kritisch: Split-Tunneling für Geschäftsdaten **deaktivieren**, um zu verhindern, dass Unternehmensdaten über unsichere private Verbindungen geleitet werden.

SOFORTMASSNAHMEN

☐ 7. ANTIVIRUS-STATUS ALLER GERÄTE

Endpoint Sicherheit

Prüfen: Alle Firmen-PCs, Laptops, Server, die mit Ihrem Netzwerk verbunden sind.

Aktion: Veraltete oder deaktivierte Antivirensoftware **sofort aktualisieren** oder aktivieren.

Standard: Automatische Updates und regelmäßige Scans für alle Endgeräte aktivieren.

☐ 8. BETRIEBSSYSTEM-UPDATES

Endpoint Sicherheit

Priorität: Kritische Sicherheitsupdates für alle Betriebssysteme (Windows, macOS, Linux, Server-OS) umgehend installieren.

Automatisierung: Automatische Updates für Sicherheitspatches aktivieren, wo immer möglich.

Notfall: Systeme mit fehlenden, kritischen Updates oder ohne Hersteller-Support **sofort vom Netzwerk trennen.**

KURZFRISTIGE MASSNAMEN

☐ 9. BACKUP-STRATEGIE IMPLEMENTIEREN

Backup & Recovery

Regel: Sorgen Sie für **3 Kopien Ihrer Daten**, auf **2 verschiedenen Speichermedien**, davon **1 Offsite- oder Cloud-Backup.**

Test: Führen Sie **halbjährliche Wiederherstellungstests** durch, um die Funktionsfähigkeit Ihrer Backups zu verifizieren.

☐ 10. OFFLINE-BACKUP ETABLIEREN

Backup & Recovery

Zweck: Optimaler Schutz vor Ransomware-Angriffen, die auch Online-Backups verschlüsseln könnten.

Methode: Externe Festplatten oder Bandlaufwerke nutzen, die nach dem Backup physisch vom Netzwerk getrennt werden.

Rotation: Etablieren Sie eine wöchentliche Rotation der Backup-Medien.

KURZFRISTIGE MASSNAMEN

☐ 11. BACKUP-VERSCHLÜSSELUNG AKTIVIEREN

Backup & Recovery

Standard: Alle Backups, insbesondere die Offsite-Kopien, sollten mit mindestens **AES-256 Verschlüsselung** gesichert werden.

Schlüsselverwaltung: Die Verschlüsselungsschlüssel müssen sicher und getrennt von den Backups aufbewahrt werden.

Compliance: Sicherstellen, dass die Datensicherung den **DSGVO-Anforderungen** entspricht.

☐ 12. PHISHING-AWARENESS-TRAINING

Mitarbeiter Awareness

Häufigkeit: Führen Sie mindestens quartalsweise interaktive Schulungen zu Phishing und anderen Cyberbedrohungen durch.

Simulation: Regelmäßige Fake-Phishing-Tests helfen, die Wachsamkeit Ihrer Mitarbeiter zu prüfen und zu schulen.

Ziel: Höheres Sicherheitsbewusstsein bei den Mitarbeitern fördern.

KURZFRISTIGE MASSNAMEN

☐ 13. STARKE PASSWORT-RICHTLINIEN DURCHSETZEN

Backup & Recovery

Komplexität: Definieren Sie Richtlinien für Passwörter (*Minimum 12 Zeichen, Kombination aus Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen*).

Tools: Führen Sie unternehmensweit einen professionellen Passwort-Manager ein.

Tipp: Länge schlägt Komplexität

☐ 14. INCIDENT-REPORTING-PROZESS

Backup & Recovery

Kanal: Etablieren Sie einfache und klare Meldewege für Sicherheitsvorfälle oder verdächtige Aktivitäten.

Response: Definieren Sie interne Verantwortlichkeiten und eine Reaktionszeit (*z.B. 24 Stunden*) für gemeldete Vorfälle.

Kultur: Fördern Sie eine offene Fehlerkultur, in der Mitarbeiter Sicherheitsvorfälle ohne Angst vor Bestrafung melden.

KURZFRISTIGE MASSNAMEN

☐ 15. PRIVILEGIEN-REVIEW (LEAST PRIVILEGE PRINCIPLE)

Zugriffs-kontrolle

Audit: Führen Sie eine Überprüfung durch, wer auf welche Daten und Systeme zugreifen kann.

Bereinigung: Entziehen Sie übermäßige oder nicht mehr benötigte Berechtigungen.

Regel: Vergeben Sie Benutzern immer nur die minimal notwendigen Rechte für ihre Tätigkeit.

☐ 16. GASTZUGANG ISOLIEREN

Zugriffs-kontrolle

Separates WLAN: Stellen Sie ein komplett separates Gäste-WLAN bereit, das keinen Zugang zum Firmennetzwerk hat.

Zeitlimits: Aktivieren Sie automatische Zeitlimits für Gastzugänge (*z.B. Deaktivierung nach 24 Stunden*).

Monitoring: Überwachen Sie die Aktivitäten im Gäste-Netzwerk auf ungewöhnliche Muster.

MITTELFRISTIGE MASSNAMEN

☐ 17. SIEM-SYSTEM IMPLEMENTIEREN

Incident-Response

Zweck: SIEM (*Security Information and Event Management*) steht für Zentrale Protokollierung, Analyse und Überwachung aller sicherheitsrelevanten Daten aus Ihrem Netzwerk.

Budget: Es gibt mittlerweile auch für KMU zugängliche SIEM-Lösungen.

ROI: Ein SIEM kann die durchschnittliche Erkennungszeit eines Angriffs von 287 auf 23 Tage reduzieren (*IBM Security*).

☐ 18. INCIDENT RESPONSE PLAN ENTWICKELN & TESTEN

Incident Response

Komponenten: Definieren Sie klare Rollen, Verantwortlichkeiten, Kommunikationswege und Eskalationspfade für den Ernstfall.

Test: Führen Sie halbjährlich Notfall-Übungen durch (*Tabletop-Übungen oder Simulationen*).

Externe Hilfe: Halten Sie Kontaktdaten von IT-Forensik-Experten und Krisenkommunikationsagenturen bereit.

MITTELFRISTIGE MASSNAMEN

☐ 19. VULNERABILITY MANAGEMENT PROGRAMM ETABLIEREN

Incident-Response

Scanning: Implementieren Sie regelmäßige (*z.B. monatliche*) automatisierte Schwachstellen-Scans Ihrer gesamten IT-Infrastruktur.

Priorisierung: Nutzen Sie standardisierte Scores (*z.B. CVSS*) zur Priorisierung der Behebung von Schwachstellen.

SLA: Setzen Sie sich interne Ziele, z.B. kritische Schwachstellen binnen 72 Stunden zu beheben.

☐ 20. DSGVO-COMPLIANCE SICHERSTELLEN & PRÜFEN

Compliance & Governance

Dokumentation: Aktualisieren Sie Ihr Verzeichnis von Verarbeitungstätigkeiten und überprüfen Sie Ihre Datenschutzrichtlinien.

TOM: Implementieren und dokumentieren Sie Technische und Organisatorische Maßnahmen (*TOM*) zum Schutz personenbezogener Daten.

Meldepflicht: Stellen Sie sicher, dass Ihr 72-Stunden-Meldeverfahren bei Datenpannen gemäß Art. 33 DSGVO funktioniert.

MITTELFRISTIGE MASSNAMEN

☐ 21. NIS-2-RICHTLINIE & IT-SICHERHEITSGESETZ PRÜFEN

Compliance & Governance

Relevanz: Klären Sie, ob Ihr Unternehmen unter den Geltungsbereich der NIS-2-Richtlinie oder des nationalen IT-Sicherheitsgesetzes fällt.

Anforderungen: Informieren Sie sich über die erhöhten Sicherheits- und Meldepflichten für Betreiber kritischer Infrastrukturen und wichtige Einrichtungen.

☐ 22. CYBER-VERSICHERUNG PRÜFEN ODER ABSCHLIESSEN

Compliance & Governance

Deckung: Sichern Sie sich gegen finanzielle Folgen von Cyberangriffen ab (Deckungssumme mindestens 1 Million Euro).

Leistungen: Achten Sie auf Leistungen wie Incident Response, Forensik, Betriebsunterbrechung und Wiederherstellungskosten.

Präventive Maßnahmen: Viele Versicherer bieten Rabatte für implementierte Sicherheitsmaßnahmen – nutzen Sie das!

MITTELFRISTIGE MASSNAMEN

☐ 23. ZERO TRUST ARCHITEKTUR PLANEN

Strategische Sicherheit

Prinzip: Verfolgen Sie den Ansatz "*Never trust, always verify*" – keinem Gerät oder Benutzer wird standardmäßig vertraut.

Implementierung: Planen Sie eine schrittweise Einführung über die nächsten 12-24 Monate, beginnend mit Identitätsmanagement und Netzwerksegmentierung.

☐ 24. CLOUD-SICHERHEITSSTRATEGIE ENTWICKELN

Strategische Sicherheit

Assessment: Bewerten Sie die Sicherheitskonfiguration Ihrer aktuellen und geplanten Cloud-Services.

Governance: Definieren Sie klare Cloud-Security-Richtlinien und Verantwortlichkeiten.

Monitoring: Implementieren Sie Cloud-spezifische Überwachungstools für Ihre Cloud-Umgebungen.

MITTELFRISTIGE MASSNAMEN

☐ 25. BUSINESS CONTINUITY PLANNING (BCP)

Strategische Sicherheit

RTO/RPO: Definieren Sie Recovery Time Objectives (*RTO – Wiederherstellungszeit*) und Recovery Point Objectives (*RPO – maximaler Datenverlust*) für kritische Systeme.

Alternativstandort: PPlanen Sie Ausweichmöglichkeiten und alternative Betriebsumgebungen bei Totalausfall.

Kommunikation: Entwickeln Sie einen Krisenkommunikationsplan für interne und externe Stakeholder.

IHRE NÄCHSTEN SCHRITTE » HANDELN!

Der erste Schritt ist das Bewusstsein, der zweite ist die Aktion. Nutzen Sie diese Checkliste als Sprungbrett für eine robustere IT-Sicherheit in Ihrem Unternehmen.

- ✅ Die Kritische Sofortmaßnahmen umgehend angehen.
- ✅ IT-Team über diese Prioritäten informieren.
- ✅ Professionellen Penetrationstest in Erwägung ziehen.
- ✅ Cyber-Versicherung prüfen oder abschließen.
- ✅ Umfassenden Incident Response Plan entwickeln.
- ✅ Termine für erste Mitarbeiterschulungen vereinbaren.
- ✅ Ein Budget für die Sicherheitsmaßnahmen beantragen.

3 GRÜNDE FÜR SIE

DURCHSCHNITTLICHE KOSTEN EINES CYBERANGRIFFS FÜR KMU: 2,4 MIO. €

SIGNIFIKANTE RISIKOREDUKTION DURCH KONSEQUENTE UMSETZUNG DIESER CHECKLISTE: BIS ZU 90%

DIE KOSTEN FÜR DIE UMSETZUNG DIESER MASSNAHMEN SIND EIN BRUCHTEIL DESSEN, WAS EIN EINZIGER ERFOLGREICHER ANGRIFF SIE KOSTEN WÜRDE.

RECHTLICHE COMPLIANCE-ANFORDERUNGEN

DSGVO

Die Missachtung von Sicherheitsstandards kann nicht nur finanzielle Schäden durch Angriffe verursachen, sondern auch hohe Bußgelder nach sich ziehen.

Art. 32: Sicherheit der Verarbeitung (Pflicht zur Implementierung technischer und organisatorischer Maßnahmen).

Art. 33: Meldung von Datenpannen binnen 72 Stunden an die Aufsichtsbehörde.

Art. 35: Datenschutz-Folgenabschätzung (bei hohem Risiko).

Bußgeld: Bis zu 20 Mio. € oder 4% des weltweiten Jahresumsatzes.

RECHTLICHE COMPLIANCE-ANFORDERUNGEN

NIS-2

Die Missachtung von Sicherheitsstandards kann nicht nur finanzielle Schäden durch Angriffe verursachen, sondern auch hohe Bußgelder nach sich ziehen.

Erweitert den Kreis der kritischen Infrastrukturen.

Strengere Anforderungen an das Risikomanagement und die Meldepflichten bei Sicherheitsvorfällen.

Führt zu deutlichen Bußgeldern bei Nichteinhaltung (bis zu 10 Mio. € oder 2% des Jahresumsatzes).

devial

Dieses Whitepaper dient als allgemeiner Leitfaden und ersetzt keine individuelle Sicherheitsberatung. Für eine vollständige und auf Ihr Unternehmen zugeschnittene Bewertung Ihrer IT-Sicherheit kontaktieren Sie unsere Experten.

Möchten Sie eine professionelle Bewertung Ihrer aktuellen Sicherheitslage?

Vereinbaren Sie ein Beratungsgespräch mit unseren Cybersecurity-Experten. Wir zeigen Ihnen auf, wie Sie die Punkte dieser Checkliste effizient umsetzen und Ihr Unternehmen nachhaltig schützen können.

+49 7237 202 99 60 www.devial.de info@devial.de

*devial GmbH * Erlenbachstr. 2/1 * 75248 Ölbronn-Dürrn * Ust-ID: DE355489087 * Steuer-Nr: 48020/22505*