IT-Sicherheitscheckliste: Sechs Maßnahmen für messbar mehr Sicherheit

Diese Checkliste zeigt konkrete Schritte auf, um Schwachstellen systematisch zu reduzieren und Ihre IT-Infrastruktur wirksam zu schützen.

Hintergrund: 99,9 Prozent der erfolgreich ausgenutzten Schwachstellen sind seit über einem Jahr bekannt. Wenn Sie die sechs Maßnahmen dieser Checkliste umsetzen, schließen Sie systematisch die häufigsten Einstiegspunkte für Angreifer.

200.000+	100.000+	Täglich
Schwachstellentests	Installationen weltweit	Feed-Updates

☐ Multi-Faktor-Authentifizierung (MFA) aktivieren

Passwörter allein bieten keinen ausreichenden Schutz. Eine zweite Authentifizierungsebene verhindert 99,9 Prozent aller Account-Übernahme-Angriffe, selbst wenn ein Passwort kompromittiert wurde.

- Schutz vor Kontoübernahmen durch Passwortdiebstahl
- Erfüllt Compliance-Anforderungen
- Reduziert unbefugte Zugriffe
- Einfache Umsetzung

Konkrete Umsetzung:
Orientieren Sie sich an Frameworks wie dem NIST CSF 2.0 und erfassen Sie zunächst alle Online-Konten sowie das Risiko von Kontoübernahmen. Setzen Sie Multi-Faktor-Authentifizierung für Konten ein, die auf Finanzsysteme, Kundendaten, administrative Funktionen oder andere sensible Informationen zugreifen, und überprüfen Sie die MFA-Durchsetzung regelmäßig. Beginnen Sie mit administrativen Konten und dem IT-Team und erweitern Sie MFA anschließend auf alle Mitarbeitenden. Authenticator-Apps wie Microsoft Authenticator oder Google Authenticator sind praxisnahe Optionen, für besonders kritische Zugänge eignen sich Hardware-Token. Definieren und kommunizieren Sie zudem einen dokumentierten Backup-Prozess für verlorene oder defekte Geräte, idealerweise bereits im Onboarding.

Zugriffsrechte regelmäßig überprüfen

Zu weitreichende Berechtigungen sind ein erhebliches Risiko: Mitarbeitende haben häufig Zugriff auf Systeme, Daten oder Einstellungen, die sie für ihre Arbeit nicht benötigen. Das Least-Privilege-Prinzip schreibt vor, dass jede Person nur die unbedingt erforderlichen Rechte erhält.

- Minimiert Insider-Risiken
- Verhindert laterale Bewegungen im Netzwerk
- Stellt Compliance sicher (DSGVO, NIS2)
- Verbessert Nachvollziehbarkeit im Audit

Konkrete Umsetzung:
Überprüfen Sie alle Berechtigungen quartalsweise. Nutzen Sie Identity- und Access-Management-Systeme (IAM), die den Prozess automatisieren und dokumentieren können. Bei Rollenwechseln oder beim Ausscheiden von Mitarbeitenden müssen Rechte unverzüglich angepasst werden. Für besonders kritische Aufgaben empfiehlt sich Just-in-Time-Access: Privilegien werden nur temporär und auf Antrag vergeben. Dokumentieren Sie alle Änderungen revisionssicher.

Backup-Strategie testen und validieren

Ein Backup ist wertlos, wenn sich die Daten im Ernstfall nicht wiederherstellen lassen. Regelmäßige Tests zeigen, ob Ihre Backup-Strategie funktioniert. Das ist besonders nach Ransomware-Angriffen entscheidend, wenn Integrität und schnelle Wiederherstellung kritisch sind.

- Erhöht Resilienz gegen Ransomware
- Sichert die Geschäftskontinuität
- Verhindert Datenverlust

Konkrete Umsetzung:
Folgen Sie der 3-2-1-Regel: drei Kopien Ihrer Daten auf zwei unterschiedlichen Medien, davon eine Kopie extern. Testen Sie die Wiederherstellung regelmäßig anhand realistischer Szenarien, nicht nur einzelne Dateien, sondern vollständige Systemzustände. Air-gapped oder unveränderliche Backups bieten zusätzlichen Schutz gegen Ransomware, die versucht, Backups zu verschlüsseln. Dokumentieren Sie Wiederherstellungsprozesse detailliert und schulen Sie Ihr Team regelmäßig.

Patch-Management automatisieren

Fehlende Sicherheitsupdates sind die häufigste Ursache erfolgreicher Angriffe. Viele Schwachstellen, die in Cyberangriffen ausgenutzt werden, sind seit Monaten bekannt und dokumentiert. Automatisiertes Patch-Management schließt diese Lücken konsequent.

- Verhindert Ausnutzung bekannter Schwachstellen
- Reduziert Zeitaufwand
- Erfüllt Compliance-Anforderungen
- Verkürzt Reaktionszeit auf Zero Days

Konkrete Umsetzung:
Setzen Sie auf zentrale Patch-Management-Tools wie WSUS, SCCM oder Ansible. Priorisieren Sie Sicherheitsupdates anhand ihres CVSS-Scores. Schwachstellen mit einem CVSS-Score über 7,0 sollten zeitnah eingespielt werden. Testen Sie kritische Patches vorab in einer Staging-Umgebung, um Kompatibilitätsprobleme frühzeitig zu erkennen. Definieren Sie feste Wartungsfenster für produktive Systeme. In Kombination mit regelmäßigen Schwachstellenscans sehen Sie zuverlässig, wo noch Lücken bestehen.

OPENVAS SCAN implementieren

EMPFEHLUNG

OPENVAS SCAN identifiziert Schwachstellen in Ihrer IT-Infrastruktur, bevor Angreifer sie ausnutzen können. Die Appliance führt automatisierte Scans durch, bewertet Risiken nach Kritikalität und liefert konkrete Empfehlungen zur Behebung.

- Über 200.000 Schwachstellen-tests, täglich aktualisiert
- Authentifizierte und nicht authentifizierte Scans
- Master Sensor Architektur für verteilte Standorte
- Europäischer Anbieter, vollständig DSGVO konform und ISO zertifiziert
- Air gapped Technologie für maximale Sicherheit
- Sofort einsatzbereite Hardware und virtuelle Appliances

Europäischer Anbieter

Hauptsitz in Osnabrück, Deutschland. Alle Daten bleiben innerhalb der EU. Vollständige DSGVO Konformität von Anfang an, nicht erst durch Anpassung.

Zertifizierte Sicherheit

ISO 27001, ISO 9001, TISAX und ISO 14001 zertifiziert. Höchste Qualitäts und Sicherheitsstandards garantiert.

Sofort einsatzbereite Appliances

Weltweit einziger Anbieter sofort einsatzbereiter Hardware Appliances für Vulnerability Management. Direkt betriebsbereit ohne aufwendige Installation.

Skalierbar

Von flexiblen Einstiegslösungen bis hin zu vielseitigen Varianten für unterschiedliche Einsatzszenarien. Unser Portfolio wächst mit Ihren Anforderungen.

Warum OPENVAS SCAN einsetzen?

Umfassende Abdeckung: Der OPENVAS ENTERPRISE FEED enthält über 200.000 Schwachstellentests und wird täglich erweitert. Der Feed deckt eine breite Palette gängiger IT und OT Umgebungen ab, darunter Server, Workstations, Netzwerkgeräte, IoT sowie ausgewählte industrielle Komponenten. Greenbone verfügt über einen schnellen Prozess zur Reaktion auf neue Schwachstellen. Besonders kritische Themen werden in der Regel kurz nach ihrer öffentlichen Bekanntmachung adressiert.

Praxisbeispiele: Unternehmen mit mehr als 500 Endpoints nutzen OPENVAS SCAN für regelmäßige Compliance Scans, etwa für DSGVO, NIS2 oder ISO 27001. Szenarien mit mehreren Standorten werden über Master Sensor Architekturen abgedeckt. Kritische Infrastrukturen profitieren von authentifizierten Scans, die auch Anwendungen ohne Netzwerkdienste prüfen.

Automatisierte Compliance: Automatisierte Scans, detaillierte Reports und vollständige Dokumentation unterstützen Sie bei der Einhaltung regulatorischer Anforderungen. Die Audit Trail Funktion dokumentiert alle Scanner Aktivitäten rechtssicher und nachvollziehbar.

Erste Schritte mit OPENVAS SCAN:

1. **Appliance Modell auswählen:** Hardware Appliance für hohe Performance oder virtuelle Appliance für flexible Bereitstellung
2. **Netzwerksegmente definieren:** Namespace Trennung teilt Management und Scan Traffic
3. **Erste Scans konfigurieren:** Der Task Wizard führt durch die Scan Einrichtung
4. **Authentifizierte Scans einrichten:** Remote Zugriff per SSH oder SMB ermöglicht tiefgehende Systemprüfungen
5. **Automatisierung aktivieren:** Zeitpläne für regelmäßige Scans und automatisierte Reports definieren

Incident Response Plan entwickeln

Tritt ein Sicherheitsvorfall ein, entscheidet die Vorbereitung über Dauer und Ausmaß der Störung sowie über die Höhe des Schadens. Ein dokumentierter Incident Response Plan definiert Verantwortlichkeiten, Kommunikationswege und Handlungsschritte für verschiedene Szenarien.

- Reduziert Reaktionszeit drastisch
- Minimiert Schäden
- Ermöglicht forensische Nachbereitung
- Erfüllt gesetzliche Anforderungen

Konkrete Umsetzung:

- Stellen Sie ein Incident Response Team mit klar definierten Rollen zusammen, etwa Incident Manager, IT Manager, Kommunikation und Rechtsabteilung.
- Erstellen Sie Playbooks für typische Szenarien wie Ransomware, Datenabflüsse oder DDoS Angriffe.
- Richten Sie Kommunikationskanäle ein, die auch dann funktionieren, wenn die IT Infrastruktur kompromittiert ist.
- Führen Sie quartalsweise Tabletop Übungen durch, bei denen das Team realistische Szenarien simuliert.
- Dokumentieren Sie die Lessons Learned nach jedem realen Vorfall.