OGSE

IT-SICHERHEIT

Cybersecurity-Guide

Wichtige Maßnahmen für Schutz, Backup und digitale Resilienz im Unternehmen.

OGSE Ressourcen · Lesedauer ca. 9 Minuten

Warum IT-Sicherheit heute Chefsache ist

Cyberangriffe treffen längst nicht mehr nur Großkonzerne — kleine und mittlere Unternehmen sind ein bevorzugtes Ziel, weil Schutzmaßnahmen dort oft weniger ausgereift sind. Gleichzeitig macht die EU-Richtlinie NIS-2 grundlegende Sicherheitsmaßnahmen für immer mehr Unternehmen verbindlich. Der gute Nachricht: Die wirksamsten Maßnahmen sind meist organisatorisch, nicht teuer — sie erfordern vor allem Konsequenz.

Die Basis: fünf Maßnahmen mit dem größten Hebel

- **Multi-Faktor-Authentifizierung (MFA):** für alle wichtigen Zugänge, insbesondere E-Mail, Cloud-Konten und Verwaltungszugriffe — der wirksamste Einzelschutz gegen gestohlene Passwörter.
- **Regelmäßige, geprüfte Backups:** nach der 3-2-1-Regel — drei Kopien, auf zwei unterschiedlichen Medien, davon eine Kopie offline oder unveränderlich gespeichert. Ein Backup im selben Netzwerk hilft im Ernstfall nicht, wenn Ransomware es mitverschlüsselt.
- **Patch-Management:** Betriebssysteme, Anwendungen und Router zeitnah aktualisieren — die meisten erfolgreichen Angriffe nutzen bekannte, längst geschlossene Sicherheitslücken.
- **E-Mail- und Phishing-Schutz:** technische Filter kombiniert mit geschulten Mitarbeitenden, die verdächtige Nachrichten erkennen und melden.
- **Zugriffsrechte konsequent begrenzen:** Mitarbeitende erhalten nur die Rechte, die sie für ihre Aufgabe wirklich brauchen — das begrenzt den Schaden, falls ein Konto doch kompromittiert wird.

Backup-Strategie im Detail

Ein Backup ist nur so gut wie seine Wiederherstellbarkeit. Deshalb gehört zu jeder Backup-Strategie ein regelmäßiger Wiederherstellungstest — nicht nur die Sicherung selbst. Empfehlenswert sind

zusätzlich unveränderliche Speicherorte (Air-Gap oder Write-Once-Speicher), die eine Verschlüsselung durch Ransomware im Nachhinein technisch verhindern.

Vorbereitung auf den Ernstfall

- Einen einfachen Notfallplan dokumentieren: Wer wird informiert, wer trifft Entscheidungen, welche Systeme werden zuerst wiederhergestellt?
- Kontaktdaten für IT-Dienstleister und ggf. Cyberversicherung griffbereit halten — im Ernstfall zählt jede Minute.
- Regelmäßig, mindestens einmal jährlich, den Ernstfall gedanklich oder praktisch durchspielen.

Netzwerk und Monitoring

Eine sinnvolle Netzwerksegmentierung sorgt dafür, dass sich ein Angriff nicht ungehindert im gesamten Unternehmen ausbreitet. Ergänzend hilft laufendes Monitoring dabei, ungewöhnliche Aktivitäten frühzeitig zu erkennen, statt erst beim sichtbaren Schaden zu reagieren.

Mitarbeitende als erste Verteidigungslinie

Die beste technische Absicherung hilft wenig, wenn ein einzelner Klick auf einen gefälschten Link sie umgeht. Regelmäßige, kurze Sensibilisierung — statt einmaliger Pflichtschulung — sorgt dafür, dass Phishing-Versuche im Alltag tatsächlich erkannt und gemeldet werden. Wichtig ist eine Fehlerkultur ohne Bloßstellung: Wer einen Fehler meldet, sollte dafür nicht bestraft, sondern für die schnelle Meldung anerkannt werden.

Verantwortlichkeiten klar regeln

Gerade in kleineren Unternehmen ist oft nicht eindeutig geregelt, wer im Ernstfall welche Entscheidung trifft. Eine kurze, schriftlich festgehaltene Übersicht — wer informiert wen, wer entscheidet über die Abschaltung betroffener Systeme, wer spricht mit Kunden und Behörden — verhindert wertvollen Zeitverlust genau dann, wenn er am teuersten ist. Diese Zuständigkeiten sollten unabhängig von einzelnen Personen dokumentiert sein, damit sie auch bei Abwesenheit oder Personalwechsel funktionieren.

Bereit für den nächsten Schritt?

OGSE unterstützt Sie bei der Umsetzung — von der ersten Einschätzung bis zur laufenden Betreuung. Vereinbaren Sie ein kostenloses Erstgespräch über ogse.info oder schreiben Sie uns direkt an info@ogse.info.