CRYPTOITDATA

Cybersicherheit für KMU: die Checkliste mit 25 Punkten

Haken Sie ab, was heute zutrifft, nicht was geplant ist. Jeder offene Punkt wird zu einer Aufgabe mit verantwortlicher Person und Frist.

Governance und NIS2

- [ ] 1 Wir haben schriftlich geprüft, ob das Unternehmen unter die OUG 155/2024 fällt: Größe, Sektor in den Anhängen, Ausnahmen.
- [ ] 2 Falls wir erfasst sind, haben wir das DNSC benachrichtigt und kennen das Datum der Meldung.
- [ ] 3 Die Leitung hat die Sicherheitsmaßnahmen schriftlich genehmigt und eine interne verantwortliche Person benannt.
- [ ] 4 Wir kennen die Meldefristen: 24 Stunden, 72 Stunden, ein Monat.

Identitäten und Zugriff

- [ ] 5 MFA ist auf allen E-Mail-Konten aktiv.
- [ ] 6 MFA ist auf VPN, Fernzugriff und Administratorkonten aktiv.
- [ ] 7 Administratorkonten sind getrennt und werden nur für die Administration genutzt.
- [ ] 8 Konten ausscheidender Mitarbeiter werden binnen höchstens 24 Stunden geschlossen.
- [ ] 9 Wir prüfen vierteljährlich, wer worauf Zugriff hat.

Daten und Backup

- [ ] 10 Kritische Daten liegen in drei Kopien vor, auf zwei Arten von Datenträgern, eine außerhalb des Netzwerks.
- [ ] 11 Die Offline- oder unveränderliche Kopie lässt sich mit einem Domänenkonto nicht löschen.
- [ ] 12 Wir haben in den letzten drei Monaten eine vollständige Wiederherstellung getestet und die Zeit gemessen.
- [ ] 13 Wir wissen, wie alt wiederhergestellte Daten sein dürfen (RPO) und wie schnell wir zurück sind (RTO).

Systeme

- [ ] 14 Wir haben ein vollständiges Inventar der Geräte, der Software und der aus dem Internet erreichbaren Dienste.
- [ ] 15 Kritische Korrekturen auf aus dem Internet erreichbaren Systemen werden binnen höchstens 14 Tagen installiert.
- [ ] 16 Wir haben keine Systeme ohne Sicherheitssupport des Herstellers, oder sie sind isoliert und dokumentiert.
- [ ] 17 Alle Laptops, Arbeitsplätze und Server haben aktiven, überwachten Endpoint-Schutz.
- [ ] 18 Die Festplatten aller Laptops sind verschlüsselt.

E-Mail und Menschen

- [ ] 19 SPF, DKIM und DMARC sind eingerichtet, DMARC mindestens auf p=quarantine.
- [ ] 20 Automatische Weiterleitung an externe Adressen ist gesperrt oder löst einen Alarm aus.
- [ ] 21 Zahlungen und Änderungen von Bankverbindungen, die per E-Mail verlangt werden, bestätigen wir telefonisch.
- [ ] 22 Jeder neue Mitarbeiter absolviert in der ersten Woche eine Anti-Phishing-Schulung.

Vorfälle und Lieferanten

- [ ] 23 Wir haben einen Notfallplan für Vorfälle von 1–2 Seiten, ausgedruckt und jährlich getestet.
- [ ] 24 Notfallkontakte (IT-Dienstleister, Bank, Versicherer, DNSC) liegen auch offline vor.
- [ ] 25 Wir haben eine Liste der Lieferanten mit Zugriff auf unsere Systeme, mit namentlichen Konten und Klauseln zur Meldung von Vorfällen.

Die Schwellen (zum Beispiel 14 Tage für kritische Korrekturen oder ein Wiederherstellungstest alle drei Monate) sind Empfehlungen von CRYPTOITDATA für ein KMU, keine gesetzlichen Vorgaben. Die NIS2-Fristen (24 Stunden, 72 Stunden, ein Monat; Meldung an das DNSC binnen höchstens 30 Tagen) stammen aus der rumänischen OUG 155/2024, konsolidierte Fassung, Stand 8. November 2026. Vollständiger Leitfaden mit Quellen: cryptoitdata.eu/de/blog/securitate-cibernetica-imm-ghid