Checkliste: 10 Punkte gegen Angriffe von aussen

Für KMU, Vereine und Verwaltungen · www.easm.ch

1 ☐

Updates innert 48 Stunden

Firewall, VPN, Server und Website zuerst. Lücken in solchen Geräten werden oft innert Tagen ausgenutzt.

2 ☐

Zweiter Faktor überall

Für Fernzugang, E-Mail, Cloud und Verwaltungsoberflächen. Gestohlene Passwörter allein genügen dann nicht mehr.

3 ☐

Verwaltung nicht ins Internet

Router, NAS, Firewall, Plesk und Datenbanken nur intern oder über VPN erreichbar machen.

4 ☐

E-Mail-Fälschung sperren

SPF, DKIM und DMARC einrichten und DMARC schrittweise auf «reject» stellen.

5 ☐

Inventar der Domains

Alle Domains und Subdomains kennen. Alte Test- und Kampagnenseiten abschalten, verwaiste DNS-Einträge löschen.

6 ☐

Zertifikate automatisch

Automatisch erneuern (z. B. Let’s Encrypt) und das Ablaufdatum überwachen. Nur TLS 1.2 und 1.3 anbieten.

7 ☐

Datensicherung getrennt

Eine Kopie offline oder unveränderbar aufbewahren und die Wiederherstellung mindestens jährlich testen.

8 ☐

Zahlungen doppelt prüfen

Geänderte Bankverbindungen immer telefonisch bestätigen. Ähnliche Domains beobachten.

9 ☐

Lieferanten einbeziehen

Wer Zugang zu Ihren Daten hat, gehört zu Ihrer Angriffsfläche. Wichtige Lieferanten prüfen und Mindestanforderungen vereinbaren.

10 ☐

Notfall vorbereiten

Wer entscheidet, wen rufen wir an, wie arbeiten wir ohne IT? Kontakte ausgedruckt bereithalten und einmal im Jahr üben.