Lista di controllo: 10 punti contro gli attacchi dall’esterno

Per PMI, associazioni e amministrazioni · www.easm.ch

1 **Aggiornamenti entro 48 ore** ☐

Prima firewall, VPN, server e sito web. Le vulnerabilità di questi dispositivi vengono spesso sfruttate in pochi giorni.

2 **Secondo fattore ovunque** ☐

Per accesso remoto, e-mail, cloud e interfacce di amministrazione. Le password rubate da sole non bastano più.

3 **Amministrazione fuori da Internet** ☐

Router, NAS, firewall, Plesk e banche dati raggiungibili solo internamente o tramite VPN.

4 **Bloccare la falsificazione delle e-mail** ☐

Configurare SPF, DKIM e DMARC e portare gradualmente DMARC a «reject».

5 **Inventario dei domini** ☐

Conoscere tutti i domini e sottodomini. Spegnere vecchie pagine di test e di campagna, cancellare le voci DNS orfane.

6 **Certificati automatici** ☐

Rinnovare automaticamente (ad es. Let’s Encrypt) e sorvegliare la scadenza. Offrire solo TLS 1.2 e 1.3.

7 **Backup separato** ☐

Conservare una copia offline o non modificabile e testare il ripristino almeno una volta all’anno.

8 **Verificare due volte i pagamenti** ☐

Confermare sempre per telefono le coordinate bancarie modificate. Sorvegliare i domini simili.

9 **Coinvolgere i fornitori** ☐

Chi ha accesso ai vostri dati fa parte della vostra superficie d’attacco. Verificare i fornitori importanti e concordare requisiti minimi.

10 **Preparare l’emergenza** ☐

Chi decide, chi chiamiamo, come lavoriamo senza IT? Tenere i contatti stampati e fare un’esercitazione all’anno.