Liste de contrôle : 10 points contre les attaques venant de l’extérieur

Pour PME, associations et administrations · www.easm.ch

1 **Mises à jour dans les 48 heures** ☐

Pare-feu, VPN, serveurs et site web d’abord. Les failles de ces appareils sont souvent exploitées en quelques jours.

2 **Second facteur partout** ☐

Pour l’accès à distance, la messagerie, le cloud et les interfaces d’administration. Des mots de passe volés ne suffisent alors plus.

3 **Administration hors d’Internet** ☐

Routeur, NAS, pare-feu, Plesk et bases de données accessibles uniquement en interne ou via VPN.

4 **Bloquer la falsification d’e-mails** ☐

Configurer SPF, DKIM et DMARC et passer progressivement DMARC à « reject ».

5 **Inventaire des domaines** ☐

Connaître tous les domaines et sous-domaines. Désactiver les anciennes pages de test et de campagne, supprimer les entrées DNS orphelines.

6 **Certificats automatiques** ☐

Renouveler automatiquement (p. ex. Let’s Encrypt) et surveiller la date d’expiration. N’offrir que TLS 1.2 et 1.3.

7 **Sauvegarde séparée** ☐

Conserver une copie hors ligne ou non modifiable et tester la restauration au moins une fois par an.

8 **Vérifier deux fois les paiements** ☐

Toujours confirmer par téléphone un changement de coordonnées bancaires. Surveiller les domaines similaires.

9 **Impliquer les fournisseurs** ☐

Qui a accès à vos données fait partie de votre surface d’attaque. Contrôler les fournisseurs importants et convenir d’exigences minimales.

10 **Préparer l’urgence** ☐

Qui décide, qui appelons-nous, comment travaillons-nous sans informatique ? Garder les contacts imprimés et s’exercer une fois par an.