Checklist: 10 points against attacks from outside

For SMEs, associations and public bodies · www.easm.ch

- [ ] **1 Updates within 48 hours**
  Firewall, VPN, servers and website first. Flaws in such devices are often exploited within days.
- [ ] **2 Second factor everywhere**
  For remote access, e-mail, cloud and admin interfaces. Stolen passwords alone are then no longer enough.
- [ ] **3 Keep administration off the internet**
  Make routers, NAS, firewalls, Plesk and databases reachable only internally or via VPN.
- [ ] **4 Block e-mail forgery**
  Set up SPF, DKIM and DMARC and move DMARC step by step to “reject”.
- [ ] **5 Inventory of domains**
  Know all domains and subdomains. Switch off old test and campaign sites, delete orphaned DNS entries.
- [ ] **6 Automatic certificates**
  Renew automatically (e.g. Let’s Encrypt) and monitor the expiry date. Offer only TLS 1.2 and 1.3.
- [ ] **7 Separate backup**
  Keep one copy offline or immutable and test restoring at least once a year.
- [ ] **8 Double-check payments**
  Always confirm changed bank details by phone. Watch similar domains.
- [ ] **9 Include suppliers**
  Whoever has access to your data is part of your attack surface. Check important suppliers and agree on minimum requirements.
- [ ] **10 Prepare for emergencies**
  Who decides, whom do we call, how do we work without IT? Keep printed contacts ready and practise once a year.