CHECKLIST

Cybersecurity checklist voor kmo's

15 punten om na te gaan, ook zonder IT-afdeling

Safebyte

Vink aan wat bij u in orde is. Elk vakje dat leeg blijft, is een concrete actie. De uitleg bij elk punt staat op **safebyte.be/blog/cybersecurity-checklist-kmo**.

Accounts en wachtwoorden

- [ ] **1. Tweestapsverificatie staat aan op e-mail en op alles wat van buitenaf bereikbaar is**
  Begin bij e-mail: dat is de sleutel tot bijna al de rest.
- [ ] **2. Iedereen gebruikt een wachtwoordmanager, geen enkel wachtwoord is hergebruikt**
  Test twijfelgevallen op safebyte.be/tools/wachtwoord-checker.
- [ ] **3. Accounts van vertrokken medewerkers en leveranciers worden binnen een dag afgesloten**
  Beheerders werken met een apart account voor beheertaken.

Updates en toestellen

- [ ] **4. Updates worden binnen 14 dagen geïnstalleerd, ook op servers, firewall en VPN**
  Vergeet printers, camera's en de router niet.
- [ ] **5. Er is een overzicht van alle toestellen en software**
  Een eenvoudige lijst is al een goed begin.
- [ ] **6. Laptops zijn versleuteld en vergrendelen vanzelf**
  BitLocker bij Windows, FileVault bij een Mac.

Back-ups

- [ ] **7. Minstens één back-up staat buiten het netwerk en kan niet gewist of versleuteld worden**
  Een kopie die altijd verbonden is, wordt mee versleuteld.
- [ ] **8. De voorbije drie maanden werd een back-up echt teruggezet**
  Een back-up die u nooit test, bestaat in de praktijk niet.
- [ ] **9. We weten hoelang het bedrijf stilligt als alles weg is**
  Bereken het op safebyte.be/tools/ransomware-calculator.

Medewerkers

- [ ] **10. Medewerkers krijgen minstens jaarlijks een opleiding om phishing te herkennen**
  Praktisch, met voorbeelden uit de Belgische praktijk.
- [ ] **11. We weten hoeveel medewerkers op een valse link zouden klikken**
  Meet het met een phishing simulatie in plaats van te gokken.
- [ ] **12. Er is een vaste regel voor betalingen en gewijzigde rekeningnummers**
  Altijd terugbellen, op een nummer dat u al kende.

Als het toch misgaat

- [ ] **13. Iedereen weet wie hij moet bellen bij een cyberaanval**
  IT-partner, verzekeraar, bank: nummers op papier, want e-mail werkt dan misschien niet.
- [ ] **14. We weten dat een datalek binnen 72 uur gemeld moet worden**
  Bij de Gegevensbeschermingsautoriteit; een incident ook bij het CCB via Safeonweb.
- [ ] **15. Een externe partij heeft getest hoe ver een aanvaller zou geraken**
  Een onafhankelijke audit of pentest vindt de blinde vlekken.

Hoeveel vakjes leeg?

0 tot 2: de basis is op orde; laat testen of het standhoudt. **3 tot 6:** duidelijke gaten; begin bij accounts en back-ups. **7 of meer:** een makkelijk doelwit; pak deze week nog punt 1 en 8 aan.

Onze eerste actie deze week:

.....