bitrev.dev
info@bitrev.dev

15 kontrolle sigurie për biznesin tuaj

Një listë praktike për ta kaluar me stafin tuaj ose me personin që ju mbulon IT-në. Secila pyetje ka një përgjigje të qartë: po ose jo. Nëse një pikë nuk e dini, trajtojeni si "jo" — mosnjohja është vetë rreziku.

KOPJET REZERVË

- [ ] **1. A ruhen me backup të gjitha sistemet kritike, përfshirë emailin në cloud?**
  Microsoft 365 dhe Google Workspace nuk janë backup. Ata ruajnë të dhënat e fshira vetëm për një periudhë të kufizuar.
- [ ] **2. A është provuar rikthimi i të dhënave gjatë tre muajve të fundit?**
  Një backup që nuk është provuar është një supozim, jo mbrojtje.
- [ ] **3. A ekziston një kopje jashtë zyrës ose e pandryshueshme?**
  Ransomware-i i kërkon qëllimisht kopjet rezervë para se të kriptojë sistemet.

LLOGARITË DHE AKSESI

- [ ] **4. A është aktiv autentikimi me shumë faktorë në email dhe te llogaritë administrative?**
  Ky është ndryshimi i vetëm që ul më shumë rrezik me më pak punë.
- [ ] **5. A janë llogaritë administrative të ndara nga ato të përdorimit të përditshëm?**
  Puna e zakonshme me të drejta administratori e shndërron çdo klikim të gabuar në incident të plotë.
- [ ] **6. A çaktivizohen menjëherë llogaritë e punonjësve që largohen?**
  Llogaritë e harruara janë rrugë hyrjeje që askush nuk i monitoron.
- [ ] **7. A përdorni menaxher fjalëkalimesh në vend të skedarëve ose fletëve?**
  Fjalëkalimet e ripërdorura janë shkaku më i shpeshtë i kompromentimit të llogarive.

PAJISJET

- [ ] **8. A instalohen automatikisht përditësimet e sistemit dhe të programeve?**
  Shumica e sulmeve shfrytëzojnë dobësi të njohura, për të cilat arna ekziston prej muajsh.
- [ ] **9. A është i fshehtëzuar disku i laptopëve?**
  Një laptop i humbur pa fshehtëzim është një rrjedhje e plotë të dhënash.
- [ ] **10. A ka mbrojtje endpoint aktive, dhe a i shikon dikush njoftimet e saj?**
  Mbrojtja që askush nuk e monitoron zbulon incidentin shumë vonë.

RRJETI

☐ **11. A është Wi-Fi i mysafirëve i ndarë nga rrjeti i brendshëm?**
Një pajisje e infektuar e një vizitori nuk duhet të arrijë dot te serverët tuaj.

☐ **12. A janë ndryshuar fjalëkalimet e parazgjedhura të ruterave, switch-eve dhe kamerave?**
Kredencialet e fabrikës janë publike dhe skanohen vazhdimisht nga robotë.

NJERËZIT DHE PROCEDURAT

☐ **13. A verifikohet me telefon çdo ndryshim i llogarisë bankare të një furnitori?**
Ky është mashtrimi më i kushtueshëm për bizneset e vogla, dhe parandalohet me një telefonatë.

☐ **14. A e di stafi ku t'i raportojë emailet e dyshimta, pa frikë se do të qortohet?**
Frika nga turpërimi e vonon raportimin, dhe vonesa është ajo që kushton.

☐ **15. A ekziston dokumentim i sistemeve dhe një plan i shkruar për incidentet?**
Pa dokumentim, çdo ndërhyrje nis me zbulim nga e para — në ditën më të keqe.

Si ta lexoni rezultatin

13–15	Gjendje e mirë. Mbajeni me rishikim periodik dhe me testim të rikthimit.
9–12	Baza ekziston, por ka boshllëqe. Nisni nga pikat 1–4, që mbulojnë rrezikun më të madh.
Nën 9	Biznesi është i ekspozuar. Një incident i vetëm do të kushtonte shumë më tepër se rregullimi.

Nëse doni ta shihni gjendjen reale

Vlerësimi fillestar është falas dhe pa detyrim: shikojmë çfarë mbulohet sot, ku ruhen kopjet dhe sa kohë do të kërkonte një rikthim. Shkruani në **info@bitrev.dev** ose telefononi në **+355 68 811 4320**.