SAVITIKRA · 20 KLAUSIMŲ

Kibernetinio saugumo kontrolinis sąrašas įmonei

Pažymėkite tai, kas jūsų įmonėje jau įgyvendinta. Jei nežinote atsakymo – palikite nepažymėtą: „nežinau“ dažniausiai reiškia „ne“. Pradėkite tvarkyti nuo grupių, pažymėtų „Pirmiausia“.

ĮMONĖ _____ DATA _____ PILDĖ _____

01 Atsarginės kopijos PIRMIAUSIA

- [ ] 01 **Ar svarbiausi duomenys (buhalterija, projektai, bendri aplankai, el. paštas) kopijuojami automatiškai, bent kartą per parą?**
  Kodėl svarbu: Kai kopijuojama „rankiniu būdu“, kopijos dažniausiai pasensta būtent tada, kai jų prireikia.
- [ ] 02 **Ar bent viena kopija laikoma atskirai – kitoje patalpoje ar debesyje – ir jos negalima ištrinti ar pakeisti iš įprasto darbo kompiuterio?**
  Kodėl svarbu: Išpirkos virusas užšifruoja viską, ką pasiekia per tinklą, kartu ir prijungtus kopijų diskus.
- [ ] 03 **Ar per pastaruosius 6 mėnesius bandėte atkurti duomenis iš kopijos ir žinote, kiek laiko tai užtrunka?**
  Kodėl svarbu: Kopija, kurios niekas nebandė atkurti, yra tik prielaida, kad ji veikia.

02 Prisijungimai ir slaptažodžiai PIRMIAUSIA

- [ ] 04 **Ar el. paštui, debesų paslaugoms ir nuotolinei prieigai įjungtas dviejų žingsnių patvirtinimas (MFA – be slaptažodžio dar reikia kodo telefone ar rakto)?**
  Kodėl svarbu: Pavogto slaptažodžio vieno neužtenka – be antro žingsnio įsilaužėlis neprisijungs.
- [ ] 05 **Ar kiekvienas darbuotojas turi savo paskyrą, o bendrų slaptažodžių („visi jungiamės kaip buhalterija“) nėra?**
  Kodėl svarbu: Su bendra paskyra neįmanoma nustatyti, kas ką padarė, ir sunku atimti prieigą vienam žmogui.
- [ ] 06 **Ar išėjusio darbuotojo ar baigusio darbą rangovo prieigos išjungiamos tą pačią dieną?**
  Kodėl svarbu: Pamirštos aktyvios paskyros – vienas paprasčiausių būdų patekti į įmonės sistemas.
- [ ] 07 **Ar administratoriaus teises turi tik tie, kam jų tikrai reikia, o kasdien dirbama su paprasta paskyra?**
  Kodėl svarbu: Jei virusas paleidžiamas su administratoriaus teisėmis, jis gali pakeisti ar išjungti beveik viską kompiuteryje.

03 Tinklas ir Wi-Fi

- [ ] 08 **Ar svečių Wi-Fi atskirtas nuo darbo tinklo – svečias negali pasiekti jūsų kompiuterių, serverio ar NAS?**
  Kodėl svarbu: Svečio telefonas ar nešiojamas kompiuteris gali būti užkrėstas, ir jūs to nežinote.

- [ ] 09 **Ar vaizdo kameros, spausdintuvai, gamybos įranga ir kiti „protingi“ įrenginiai atskirti nuo kompiuterių tinklo (atskiras tinklo segmentas, VLAN)?**
  Kodėl svarbu: Tokie įrenginiai retai atnaujinami, todėl dažnai tampa lengviausiu keliu į tinklą.

- [ ] 10 **Ar interneto prieigą saugo ugniasienė (įrenginys, filtruojantis, kas įleidžiama iš interneto), pakeisti gamykliniai slaptažodžiai ir nėra be reikalo atvertų prievadų?**
  Kodėl svarbu: Automatiniai skeneriai internete nuolat ieško atvirų įrenginių su gamykliniais slaptažodžiais.

- [ ] 11 **Ar maršrutizatoriaus, ugniasienės, Wi-Fi taškų ir NAS programinė įranga atnaujinama bent kas kelis mėnesius?**
  Kodėl svarbu: Tinklo įrangos spragos viešai skelbiamos, o neatnaujintą įrangą lengva rasti ir išnaudoti.

04 Darbo vietos ir įrenginiai

- [ ] 12 **Ar visų kompiuterių operacinė sistema ir programos atnaujinamos automatiškai, o kompiuterių su nebepalaikoma sistema nebėra?**
  Kodėl svarbu: Dauguma atakų išnaudoja jau žinomas spragas, kurioms pataisymai seniai išleisti.

- [ ] 13 **Ar visuose kompiuteriuose veikia ir atnaujinama apsauga nuo kenkėjiškų programų (antivirusinė)?**
  Kodėl svarbu: Ji sustabdo didelę dalį žinomų virusų dar prieš jiems pradedant veikti.

- [ ] 14 **Ar nešiojamųjų kompiuterių diskai užšifruoti (pvz., BitLocker ar FileVault), kad pamesto kompiuterio duomenų nebūtų galima perskaityti?**
  Kodėl svarbu: Pamestas ar pavogtas nešiojamasis kompiuteris be šifravimo – tai atviri įmonės ir klientų duomenys.

05 Nuotolinis darbas

- [ ] 15 **Ar prie įmonės serverio, NAS ar kompiuterių iš išorės jungiamasi tik per VPN (šifruotą „tunelį“ į įmonės tinklą), o ne per tiesiai į internetą atvertą nuotolinį darbalaukį (RDP)?**
  Kodėl svarbu: Atvertas nuotolinis darbalaukis – vienas dažniausiai atakuojamų įėjimų į įmonių tinklus.

- [ ] 16 **Ar žinote, kas iš viso turi nuotolinę prieigą (darbuotojai, tiekėjai, nuotolinio valdymo programos), ir nenaudojamos prieigos išjungtos?**
  Kodėl svarbu: Seniai pamiršta nuotolinio valdymo programa veikia kaip neužrakintos atsarginės durys.

06 Žmonės ir procedūros

- [ ] 17 **Ar darbuotojai bent kartą per metus mokomi atpažinti sukčiavimo laiškus, netikrus prisijungimo puslapius ir įtartinus skambučius?**
  Kodėl svarbu: Daugybė incidentų prasideda nuo vieno paspaudimo – mokytas žmogus tokį laišką dažniau atpažins.

- [ ] 18 **Ar užrašyta, ką daryti įvykus incidentui: kas sprendžia, kam skambinti (IT partneriui, bankui, NKSC), kaip atjungti užkrėstą kompiuterį?**
  Kodėl svarbu: Kai viskas stoja, laikas gaištamas ieškant telefonų ir sprendžiant, kas atsakingas.

- [ ] 19 **Ar sąskaitų rekvizitų pakeitimai ir skubūs mokėjimo prašymai visada patikrinami kitu būdu – paskambinant žinomu numeriu?**
  Kodėl svarbu: Suklastotas laiškas „pasikeitė mūsų sąskaita“ – paprastas, bet brangiai kainuojantis sukčiavimo būdas.

07 Tiekėjai

☐ 20 **Ar žinote, kurie tiekėjai (IT, programų, įrangos priežiūros) turi prieigą prie jūsų sistemų ir duomenų, ar jų prieigos ribotos ir ar saugumo reikalavimai aptarti sutartyse?**

Kodėl svarbu: Įsilaužimas pas tiekėją gali tapti įsilaužimu pas jus, jei jo prieiga neribota.

Rezultatas

Įvykdyta _____ iš 20

Pakartokite savitikrą bent kas pusmetį ir po didesnių pokyčių (naujas serveris, tiekėjas, darbuotojų kaita).

- **0–9:** didelė rizika – pirmiausia sutvarkykite atsargines kopijas ir prisijungimus (1–7 punktai).
- **10–15:** pagrindai yra, bet liko spragų – tvarkykite nuo viršaus.
- **16–19:** gera būklė – užbaikite likusius punktus.
- **20:** puiku – palaikykite ir tikrinkite reguliariai.

Ką tvarkome pirmiausia

DARBAS	KAS ATSAKINGAS	IKI KADA

Kam skambinti įvykus incidentui

KAS	VARDAS, ĮMONĖ	TELEFONAS
Kas sprendžia įmonėje		
IT partneris		
Bankas (jei pavogti pinigai)		
NKSC (pranešimas apie incidentą)		
Draudikas (jei turite draudimą)		

Kibernetinio saugumo įstatymas (NIS2). Lietuvoje NIS2 direktyva perkelta atnaujintu Kibernetinio saugumo įstatymu (įsigaliojo 2024-10-18). Jis paprastai taikomas vidutinėms ir didelėms įmonėms įstatyme išvardytuose sektoriuose (su išimtimis). Pareigos skaičiuojamos nuo įtraukimo į NKSC Kibernetinio saugumo subjektų registrą. Šis sąrašas naudingas ir toms įmonėms, kurioms įstatymas netaikomas.

Tai ne teisinė konsultacija; ar įstatymas taikomas jūsų įmonei, pasitikrinkite su NKSC ar teisininku. Daugiau: nksc.lt · interaktyvi versija: kpiekranai.lt/kibernetinio-saugumo-sarasas