Įmonės saugumo minimumas

By Deividas Ambrazevičius - 2026-08-10

15 svarbiausių žingsnių, kuriuos jūsų įmonė gali įdiegti jau šią savaitę - nuo autorizacijos iki apsaugos nuo AI sukčių.

Kaip naudotis

Šis checklist'as ne teorija, o konkretūs veiksmai. Peržiūrėkite jį su savo komanda ir pažymėkite, kas jau padaryta. Pradėkite nuo KRITINIS žymėtų punktų - jie duoda didžiausią apsaugą už mažiausią pastangą. Dauguma jų nemokami ir įgyvendinami per kelias dienas.

Kodėl tai svarbu dabar

> Sukčiai vis dažniau taikosi ne į technologijas, o į žmones ir procesus: suklastotas vadovo balsas, apgaulingas el. laiškas, netikras skubus pavedimas. Kartu ES reguliavimas (NIS2, AI Act) kelia reikalavimus ir vadovų asmeninę atsakomybę. Geros naujienos - pagrindinę apsaugą sudaro paprasti, dažnai nemokami dalykai.

1 dalis. Prieigos ir autorizacija

Pavadinimas	Veiksmas	Tipas
Bent dviejų veiksnių autentifikacija (MFA/2FA) visur, idealiausia: Passkeys / FIDO2	El. paštui, bankui, administravimo sistemoms, debesijai, vidinėm sistemom. Tai sustabdo daugumą prisijungimo atakų, net jei slaptažodis nutekėjo. Pradėkite nuo pašto ir banko, kur leidžia ir kur galima įsidiekite passkeys kaip minaliai, FIDO įrenginys - idealu šiai dienai.	KRITINIS

Slaptažodžių valdyklė komandai	Nustokite naudoti tuos pačius ar silpnus slaptažodžius. Slaptažodžių valdyklė sugeneruoja ir saugo unikalius. Draudžia slaptažodžius lapeliuose.	KRITINIS
"Mažiausių teisių" principas	Kiekvienas darbuotojas ir sistema turi tik tas teises, kurių realiai reikia darbui. Peržiūrėkite, kas turi administratoriaus teises, dažniausiai per daug žmonių.	SVARBUS
Buvusių darbuotojų prieigų panaikinimas	Sudarykite procesą: išeinant darbuotojui - iškart panaikinamos VISOS prieigos (paštas, sistemos, debesija, bendri slaptažodžiai).	SVARBUS
Atskiros paskyros administravimui	Kasdieniam darbui - įprasta paskyra; administravimui - atskira. Taip kompromituota kasdienė paskyra neatveria viso namo.	REKOMENDACIJA

2 dalis. Apsauga nuo sukčiavimo (žmonės ir procesai)

	Veiksmas	Tipas

Mokėjimų verifikacijos taisyklė	Įveskite taisyklę: joks nestandartinis ar skubus pavedimas nevykdomas be patvirtinimo antru kanalu (skambutis atgal ŽINOMU numeriu). Net jei skambina direktorius.	KRITINIS
"Keturių akių" principas dideliems pavedimams	Virš sutartos sumos pavedimą turi patvirtinti du žmonės. Vienas apgautas darbuotojas nebegali vienas išsiųsti pinigų.	KRITINIS
Darbuotojų mokymai su realiais pavyzdžiais	Trumpi, praktiški mokymai: kaip atrodo phishing laiškas, deepfake skambutis, netikras vadovo prašymas. Kartokite bent kartą per pusmetį.	SVARBUS
Įtartino pašto atpažinimas	Mokykite pastebėti: netikslus siuntėjo adresas, skubumas, neįprastas prašymas, nuorodos į "prisijunkite čia". Suabejojus - patikrinti kitu kanalu.	SVARBUS
Aiškus pranešimo kanalas	Kiekvienas darbuotojas turi žinoti, KAM iškart pranešti apie įtartiną laišką ar skambutį - be baimės, kad sugaišins laiką ar "atleis" iš darbo. Greitis mažina žalą.	REKOMENDACIJA

3 dalis. Sistemos, duomenys ir pasiruošimas

	Veiksmas	Tipas
Reguliarios atsarginės kopijos (ir jų testas)	Automatinės kopijos, saugomos atskirai nuo sistemos. Bent kartą per ketvirtį PATIKRINKITE, ar iš jų realiai galima atsikurti.	KRITINIS
Atnaujinimai laiku	Sistemos, programos, svetainės - atnaujinkite reguliariai. Daug atakų naudoja seniai žinomas, bet nepataisytas spragas	SVARBUS
Incidento planas (1 puslapis)	Paruoškite: ką darome per pirmą valandą po incidento - kas skambina bankui, kas izoliuoja paštą, kam pranešame, kokie žmonės įtraukiami. Laikykite pasiekiamą, ne tik serveryje, bet, kad ir kiekvienas žinotų proceso eigą.	SVARBUS
"Shadow AI" taisyklės	Susitarkite, kokius įmonės duomenis GALIMA ir NEGALIMA vesti į viešus AI įrankius (ChatGPT ir kt.). Darbuotojai dažnai to nežino ir netyčia nuteka informaciją.	SVARBUS

Kibernetinio saugumo atsakingas asmuo	Paskirkite žmogų (ar partnerį), kuris atsako už saugumą. Kai atsako "visi" tai reiškias, kad neatsako niekas. Vadovybė lieka galutinai atsakinga.	REKOMENDACIJA

Ką daryti toliau

Jei pažymėjote mažiau nei pusę punktų kaip "padaryta" - jūsų įmonė turi spragų, kuriomis sukčiai naudojasi kasdien. Galiu padėti jas uždaryti greitai ir be chaoso nemokamai per 30 min. patikros metu parodau, kas jūsų atveju svarbiausia.

Susisiekite: labas@ambrazevicius.com / ambrazevicius.com