TIS2 IR CISO IŠŠŪKIAI: SIZIFO AKMUO AR BRANDOS KELIONĖ?

Jonas Skardinskas,
LTG skaitmeninės ir dirbtinio intelekto saugos vadovas

Sizifo akmuo ar brandos kelionė?

Kibernetinio saugumo kasdienybė dažnai primena Sizifo mito akmenį — nauji reikalavimai, incidentai ir grėsmės nuolat ridena mus atgal.

Ar turime pasmerkti save amžinai kartoti šį procesą?

NIS2 direktyva atveria unikalią galimybę pergalvoti saugumo požiūrį ir kelti brandą, o ne tik formaliai vykdyti reikalavimus.

„Langelių žymėjimas“ neužtikrina saugumo

„Checkbox syndrome“ — MFA įdiegtas, atsarginės kopijos daromos, mokymai įvykdyti.

Tačiau incidentai net aukštos brandos įmonėse parodo: formali atitiktis negarantuoja tikro saugumo.

Tikroji reikalavimų vertė atsiskleidžia ne formaliame įgyvendinime, o realių priemonių ir jų veiksmingumo mūsų sistemose užtikrinime.

Tikrinkime faktus ir nepamirškime išimčių

Atitiktis be išimčių politikos kaip ideali teorija – graži ant popieriaus, tačiau realybėje neįmanoma, nes turim prisitaikyti prie konteksto, rizikų ir išimčių.

- MFA gali būti įdiegtas ne visuose įrenginiuose ar ne visiems vartotojams, o jo įgyvendinimas skirtingose sistemose ir skirtingoms vartotojų grupėms nebus vienodas.
- Atsarginės kopijos daromos, bet ar iš jų buvo atkurta sistema
- Darbuotojų mokymai vyksta kartą per metus, tačiau reikia nuolatinio, tikslinio ir reagavimo tiek po incidentų, tiek ir po reikšmingų pokyčių aplinkoje.

Rizikų vertinimas: kodėl tai kartais neveikia

Kibernetinės grėsmės keičiasi greičiau nei tradiciniai, kartą per metus atliekami rizikų vertinimai.

Su informacinėmis sistemomis susijusių rizikų vertinimas paliekamas kibernetinei saugai ir IT, o ne verslui - rizikose nelieka verslo „skausmo“

Verslo konteksto svarba rizikų vertinime

Kibernetinė sauga ir IT dažnai vertina rizikas neatsižvelgiant į verslo prioritetus ir kontekstą.

Prioritetai: kritinis pažeidžiamumas nekritinėje verslo sistemoje vs vidutinis pažeidžiamumas kritinėje.

Be verslo konteksto rizikų vertinimas tampa techniniu pratimu, o ne priemone verslo apsaugai.

Į verslą orientuotas kibernetinio saugumo rizikų vertinimas

Rizikų vertinimas atsižvelgiant į verslo kontekstą

Sistemų kritiškumas pagal verslo identifikuotą svarbą

Grėsmių modeliavimas remiantis verslo procesais

Kertinis sėkmingo vertinimo klausimas
„Kas nutiks verslui, jei ši rizika materializuosis?“

Brandos lygiai

Reaktyvus: Mes sprendžiame problemas, kai jos atsiranda

Valdomas: Mes žinome, kokios problemos gali kilti

Apibrėžtas: Mes turime procesus problemoms spręsti

Pamatuojamas: Mes matuojame procesus ir taikom prevenciją

Optimizuotas: Mes nuolat tobulėjame ir taikome naujoves

Branda grįstas komunikavimas

Atitinkam/neatitinkam

„Atitinkam“ – šaunuoliai gerai padirbėjot
„Neatitinkam“ – blogai, ieškom naujo CISO

Keliam brandą

„Šiuo metu lygis 3.2 iš 5, kitą ketvirtį planuojame pasiekti 3.5“ – realistiniai lūkesčiai

Taigi - Sizifo akmuo ar brandos kelionė

Formali atitiktis – Sizifo akmuo, amžinas rutinos kartojimas.

Brandos kelionė – dinamiškas, į verslą orientuotas, nuolat tobulėjantis kelias.

„1% geriau kiekvieną dieną“ - kiekvienas žingsnis mažina riziką ir stiprina organizacijos atsparumą.