

DORA spragų vertinimo pavyzdys

Santrauka vadovybei ir veiksmų planas

Visi organizacijos duomenys, įrodymai ir radiniai yra išgalvoti. Tai darbo rezultato iliustracija, o ne atlikto kliento projekto ataskaita.

Pirmiausia siūloma patikrinti klientų portalo atkūrimą ir pašalinti nebereikalingą privilegijuotą prieigą. Tiekėjų bei sistemų priklausomybių duomenis reikia sutvarkyti, kad sprendimai būtų grindžiami pilnesniu veiklos vaizdu.

4

pasirinkti radiniai

2

P1 prioritetai

90

dienų plano horizontas

Pavyzdžio kontekstas

Hipotetinė finansų įstaiga turi 80 darbuotojų, klientų portalą ir penkias ICT paslaugų sutartis. Pavyzdyje daroma prielaida, kad jai taikoma bendroji DORA ICT rizikos valdymo sistema, o ne 16 straipsnio supaprastinta tvarka.

Vertinimo ištrauka apima keturis pasirinktus kontrolės klausimus. Ji neapima visų DORA, RTS ar ITS reikalavimų, techninio saugumo testavimo ir bendros atitikties išvados.

Pasirinktų radinių apžvalga

ID ir tema	Būsena	Prioritetas
F01 Portalo atkūrimas	Veiksmingumas nepatvirtintas	P1
F02 Privilegijuota prieiga	Spraga patvirtinta	P1
F03 Informacijos registras	Spraga patvirtinta	P2
F04 Sistemų priklausomybės	Spraga patvirtinta	P2

Siūlomi vadovybės sprendimai

- Patvirtinti darbų savininkus ir atkūrimo bandymui reikalingą laiką bei išteklius.
- Sutarti tarpinius prieigos rizikos mažinimo veiksmus ir patikrinimo terminus.
- Pažangą vertinti pagal uždarymo įrodymus; atidėjimus ir likutinę riziką svarstyti atskirai.

Pirmojo prioriteto radiniai

Visi organizacijos duomenys, įrodymai ir radiniai yra išgalvoti. Tai darbo rezultato iliustracija, o ne atlikto kliento projekto ataskaita.

F01 Portalo atkūrimo galimybė nepatvirtinta

P1 | IT vadovas | Tikslas per 30 dienų

DORA 12 straipsnio 2 dalis ir 6 dalis

Įrodymai ir nustatyta būklė. E01 - patvirtinta atkūrimo politika: portalo RTO 4 val., RPO 1 val. E02 - 30 dienų sėkmingų atsarginių kopijų žurnalas. E03 - pokalbio protokolas: prašyto 12 mėnesių laikotarpio atkūrimo bandymo ataskaita nepateikta. Vien kopijų sėkmės įrašai nepatvirtina paslaugos atkūrimo.

Galimas poveikis. Sutrikus portalui gali nepavykti atkurti paslaugos ir duomenų per verslo nustatytą laiką. Tikrasis atkūrimo laikas šiame pavyzdyje nežinomas.

Siūlomas veiksmas. Suderinti izoliuoto bandymo scenarijų, atkurti portalo duomenis ir paslaugą, užfiksuoti laikus bei patikrinti duomenų vientisumą. Neatitikimus įtraukti į veiksmų planą.

Uždarymo kriterijus. IT ir verslo pasirašytas bandymo protokolas patvirtina pasiektus RTO bei RPO tikslus ir sėkmingą duomenų patikrą. Nepasiekti tikslai lieka atviri iki sėkmingo pakartotinio bandymo. Vadovybės sprendimas dėl likutinės rizikos fiksuojamas atskirai.

F02 Buvusio darbuotojo administratoriaus paskyra aktyvi

P1 | IT vadovas ir personalo funkcija | Tikslas per 30 dienų

DORA 9 straipsnio 4 dalies c punktas

Įrodymai ir nustatyta būklė. E04 - personalo įrašas rodo, kad pasirinkto darbuotojo darbo santykiai baigėsi prieš 14 dienų. E05 - administravimo teisių išrašas rodo, kad jo vardinė paskyra vis dar aktyvi ir turi privilegijuotas teises. Įvertintas vienas išėjimo atvejis.

Galimas poveikis. Nebereikalinga prieiga sudaro sąlygas neteisėtiems pakeitimams ar duomenų atskleidimui. Šis radinys nepatvirtina, kad paskyra buvo neteisėtai panaudota.

Siūlomas veiksmas. Per 2 dienas panaikinti nebereikalingą prieigą, išsaugoti susijusius žurnalus ir peržiūrėti panaudojimą po išėjimo. Per 30 dienų suderinti išėjimo proceso kontrolę ir patikrinti likusias privilegijuotas paskyras.

Uždarymo kriterijus. Paskyra užblokuota, po išėjimo buvęs aktyvumas įvertintas, o visos privilegijuotos paskyros turi patvirtintą savininką bei poreikį. Dokumentuotas personalo pranešimo ir IT įvykdymo patikrinimas.

Duomenų ir valdymo spragos

Visi organizacijos duomenys, įrodymai ir radiniai yra išgalvoti. Tai darbo rezultato iliustracija, o ne atlikto kliento projekto ataskaita.

F03 Informacijos registre trūksta dviejų sutarčių

P2 | ICT tiekėjų valdymo savininkas | Tikslas per 60 dienų

DORA 28 straipsnio 3 dalis

Įrodymai ir nustatyta būklė. E06 - pavyzdžio penkių ICT paslaugų sutarčių sąrašas. E07 - informacijos registro ištrauka apima tris iš jų. Dvi sutartys nesusietos su registro įrašais; viename įrašė nepažymėta, ar paslauga palaiko ypatingos svarbos arba svarbią funkciją.

Galimas poveikis. Nepilnas registras apsunkina priklausomybių vertinimą ir informacijos pateikimą priežiūros institucijai. Pavyzdyje nenagrinėjama visų registro laukų ar pateikimo formato atitiktis.

Siūlomas veiksmas. Sutikrinti visą sutarčių sąrašą su registru, papildyti trūkstamus įrašus ir pagrįsti funkcijų klasifikaciją. Paskirti registro savininką bei atnaujinimo trigerius.

Uždarymo kriterijus. Visos penkios sutartys sutikrintos su registro įrašais; klasifikacija patvirtinta atsakingo asmens. Išsaugotas sutikrinimo protokolas ir atnaujinimo atsakomybė. Pilna ITS struktūros validacija planuojama atskirai.

F04 Neaprašytos dviejų paslaugų priklausomybės

P2 | IT architektūros ir verslo paslaugų savininkai | Tikslas per 60 dienų

DORA 8 straipsnio 1, 4, 5 ir 6 dalys

Įrodymai ir nustatyta būklė. E08 - paslaugų ir sistemų sąrašė yra penkios verslo paslaugos. Trims nurodytos sistemos ir tiekėjų priklausomybės; dviem šie ryšiai neužpildyti. Nebuvo pateiktas kitas dokumentas, paaiškinantis trūkstamus ryšius.

Galimas poveikis. Per sutrikimą gali būti neaišku, kurias sistemas ir tiekėjus įtraukti į atkūrimą. Poveikio analizė ir pokyčių vertinimas gali remtis nepilna informacija.

Siūlomas veiksmas. Su paslaugų savininkais patikslinti ryšius su sistemomis, informaciniu turtu ir tiekėjais. Užfiksuoti svarbą, atsakomybes ir peržiūros tvarką.

Uždarymo kriterijus. Visoms penkioms paslaugoms patvirtinti pagrindiniai ryšiai ir savininkai. Vienas pasirinktas atkūrimo scenarijus peržiūrėtas naudojant atnaujintą žemėlapi; likusios ribos dokumentuotos.

90 dienų veiksmų planas

Diena 0 - vadovybė patvirtina planą. Terminai yra pavyzdžio rekomendacijos, o ne DORA nustatyti spragų šalinimo terminai.

Laikas	Veiksmas ir savininkas	Patikrinamas rezultatas
0-2 d.	F02: IT panaikina nebereikalingą prieigą.	Paskyros būseną ir aktyvumo peržiūros įrašas.
0-7 d.	Vadovybė ir darbų savininkai patvirtina planą, išteklius bei bandymo scenarijų.	Patvirtintos atsakomybės ir bandymo užduotys.
8-30 d.	F01: IT ir verslas atlieka atkūrimo bandymą. F02: IT ir personalas sutvarko prieigos procesą.	Bandymo protokolai; paskyrų peržiūra ir išėjimo kontrolės įrodymai.
31-60 d.	F03: tiekėjų valdymo savininkas papildo registrą. F04: IT ir verslas patvirtina priklausomybes.	Sutarčių sutikrinimas ir patvirtintas paslaugų žemėlapis.
61-90 d.	Rizikų funkcija peržiūri uždarymo įrodymus. Vadovybė sprendžia dėl likusių veiksmų.	Uždarymo išvada arba atviras veiksmas su nauju terminu ir rizikos sprendimu.

Kaip skaityti šį vertinimą

P1 - galimas tiesioginis poveikis svarbios paslaugos atkūrimui ar privilegijuotai prieigai. P2 - duomenų ar valdymo spraga, kurią reikia suplanuoti pašalinti. Tai pavyzdžio prioritetai, ne oficiali DORA rizikos skalė. „Spraga patvirtinta“ reiškia, kad imtyje matomas neatitikimas. „Veiksmingumas nepatvirtintas“ reiškia, kad įrodymų nepakanka. Iš keturių klausimų neskaičiuojamas bendras atitikties procentas. Rizikos priėmimas savaime nepatvirtina reikalavimo įvykdymo.

RTO - tikslinis paslaugos atkūrimo laikas. RPO - tikslinis atkuriamų duomenų taškas, šiame pavyzdyje išreikštas toleruojamu duomenų praradimo laikotarpiu. E01-E08 - išgalvotų įrodymų identifikatoriai.

Teisinės nuorodos ir pavyzdžio ribos

Reglamentas (ES) 2022/2554: pasirinktos sąsajos su 8, 9, 12 ir 28 straipsniais. Nuorodos padeda parodyti atsekamumą; jos neapima visų kontrolės srities reikalavimų. Pilnam vertinimui papildomai nustatoma taikymo sritis ir aktualūs RTS bei ITS.

EUR-Lex teisės akto įrašas | ES oficialiojo leidinio tekstas CySEC svetainėje

Aptarkime jūsų vertinimo apimtį | info@glesum.lt | glesum.lt