

Informacijos saugos rizikų vertinimas:

dažniausi pažeidžiamumai ir galimas jų poveikis

Jūratė Jurevičiūtė
UAB Atea Informacijos saugos specialistė

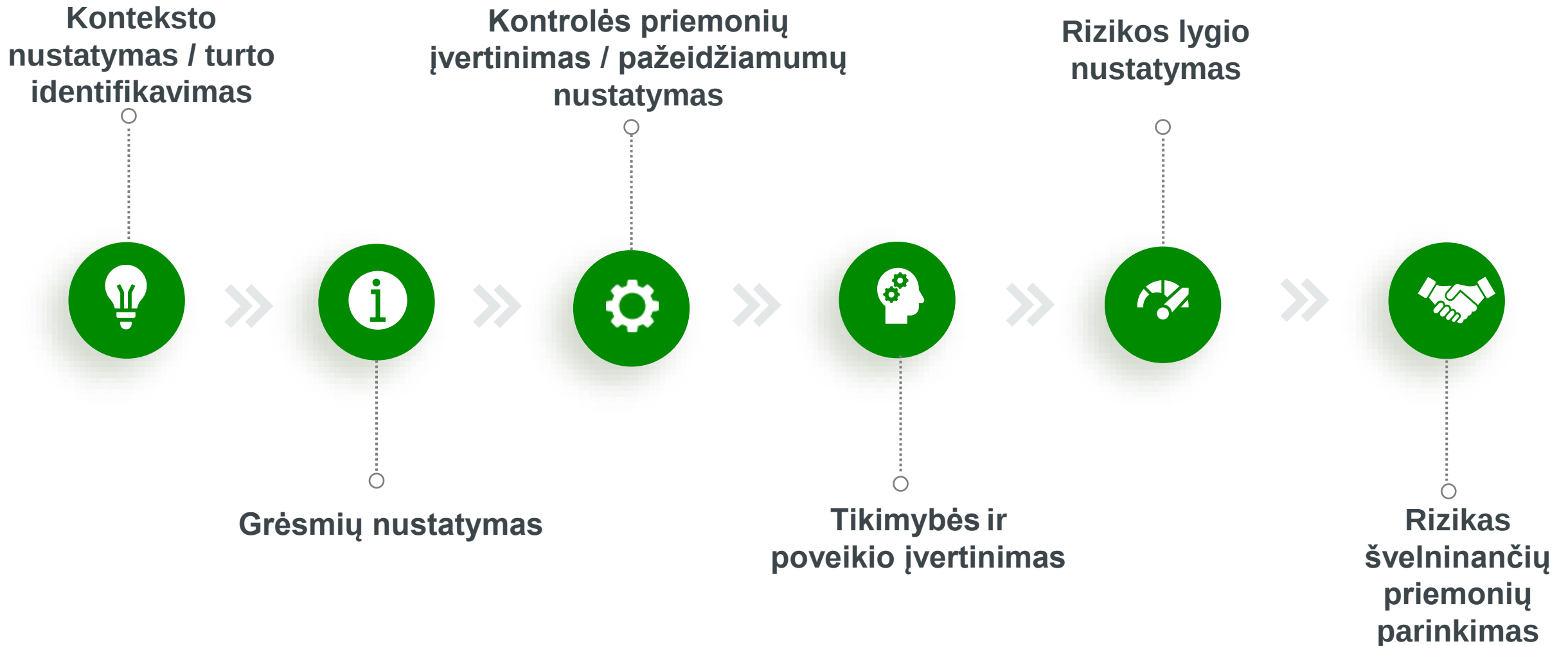
ATEA

Informacijos saugos rizikų vertinimas

tai sistemingas procesas, kurio tikslas – nustatyti organizacijos pažeidžiamumus ir grėsmes, įvertinti saugumo įvykių tikimybę ir nustatyti galimą tokių įvykių poveikį



Vertinimo procesas



Kokie privalumai?



Turto ir procesų kritiškumo identifikavimas

Įvertinamas kontekstas, identifikuojamos sistemos ir kiti informaciniai ištekliai, veiklos procesai ir jų kritiškumas



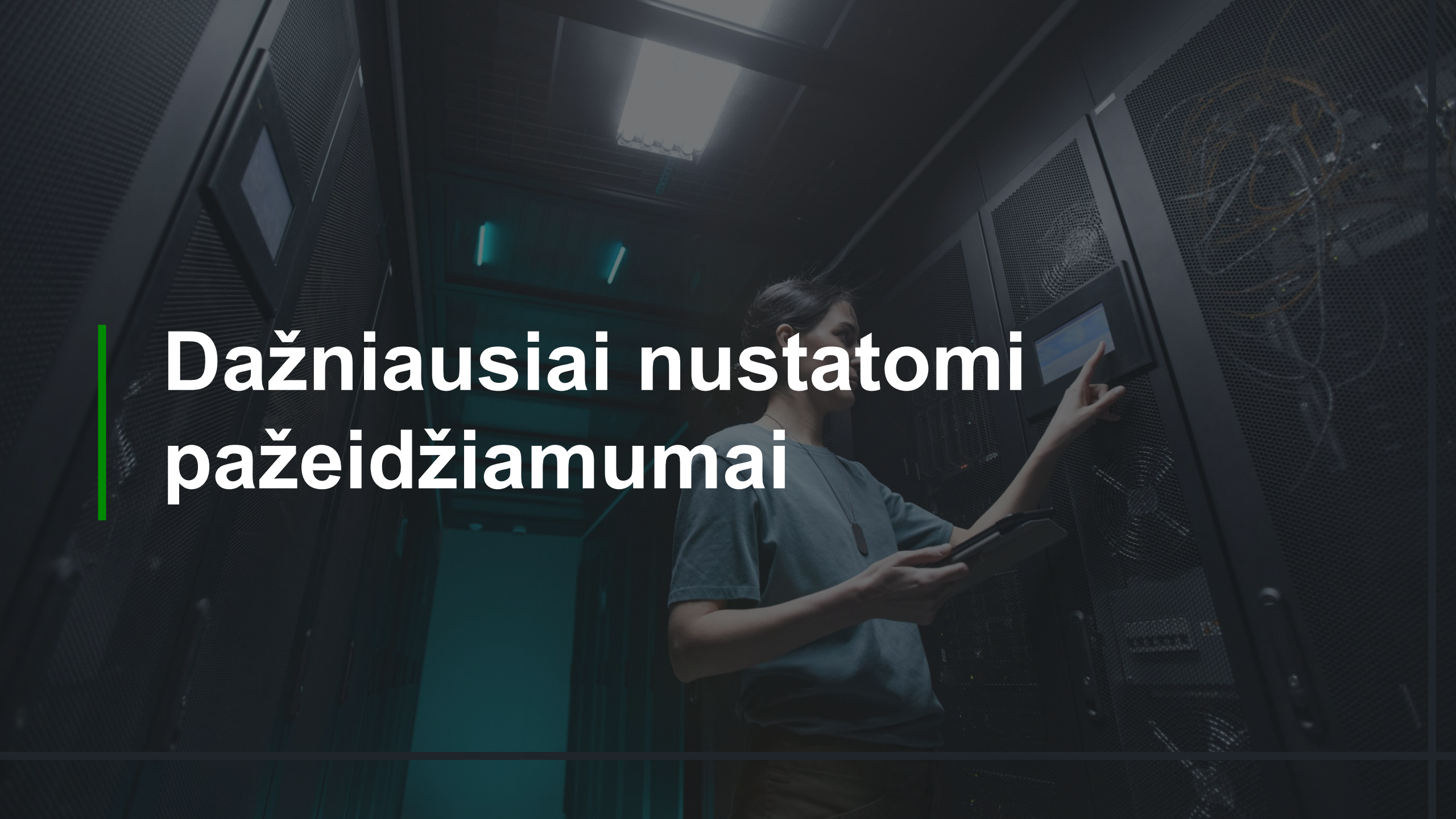
Pažeidžiamumų identifikavimas

Identifikuojami pažeidžiamumai, kurių „nepadengia“ taikomos kontrolės priemonės



Kontrolės priemonių parinkimas, atsižvelgiant į rizikos lygius

Rizikos ir atitinkamai kontrolės priemonės rizikoms valdyti sugrupuojamos pagal kritiškumą, išskiriami prioritetai

A woman in a blue t-shirt is standing in a server room, holding a tablet and pointing at a screen on a server rack. The room is dimly lit with blue ambient lighting. The server racks are black with mesh doors, and some internal components and cables are visible. The ceiling has a skylight and some equipment.

Dažniausiai nustatomi pažeidžiamumai

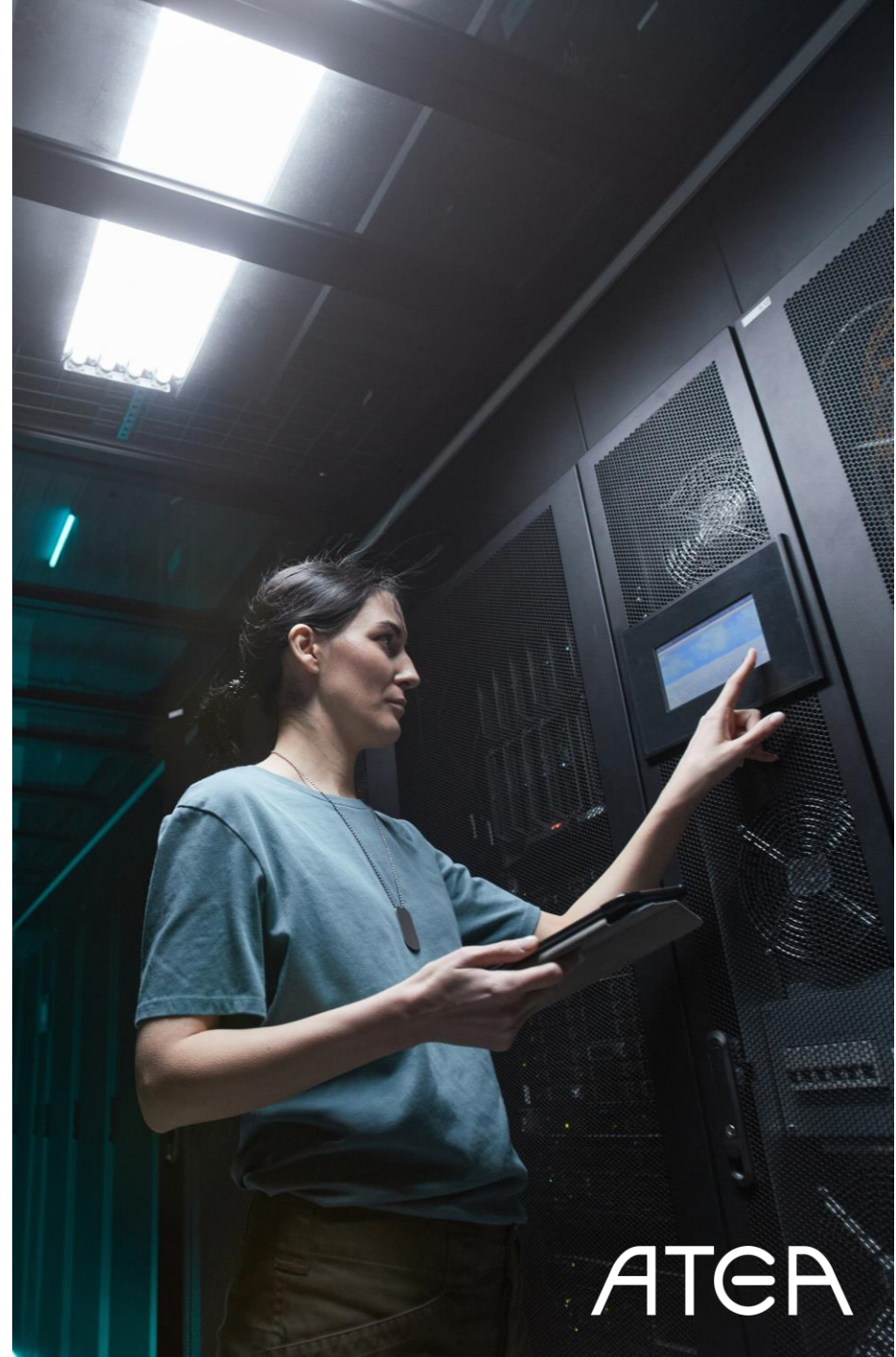
Nėra užtikrinamas tinkamas žurnalinių įrašų fiksavimas, saugojimas ir analizė (I)

Grėsmės:

- Piktnaudžiavimas įgaliojimais
- Nesankcionuota prieiga
- Nesankcionuotas įrangos ir sistemų naudojimas ar administravimas ir kt.

Tinkamas žurnalizavimas turi apimti:

- Programinės įrangos naudojimą (pavyzdžiui, SIEM)
- Tinkamą apimtį nustatymą ir fiksavimą
- Saugojimo laikotarpio nustatymą ir jo laikymąsi
- Nuolatinę analizę ir kt.



ATEA

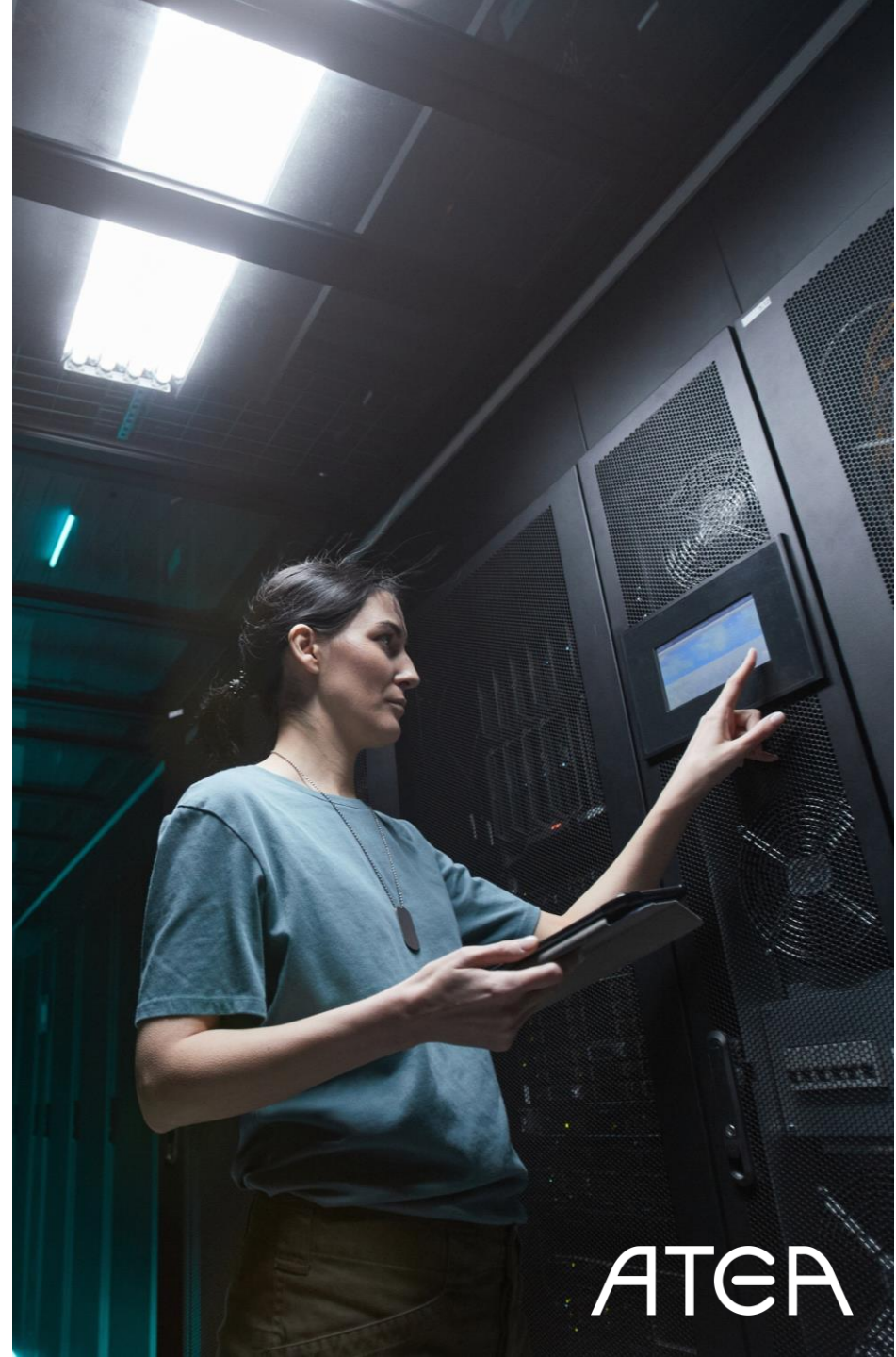
Nėra užtikrinamas tinkamas žurnalinių įrašų fiksavimas, saugojimas ir analizė (II)

Praktinis pavyzdys (poveikis: teisinis, finansinis, reputacinis)

Situacija: įsilaužėliai įgijo neteisėtą prieigą prie vidinių įmonės duomenų bazių, pasisavino duomenis ir paviešino klientų asmeninę informaciją.

Pasekmės:

- Atskleisti klientų asmens duomenys
- Skirta 20000 eurų bauda
- Šio atvejo viešinimas viešojoje erdvėje



ATEA

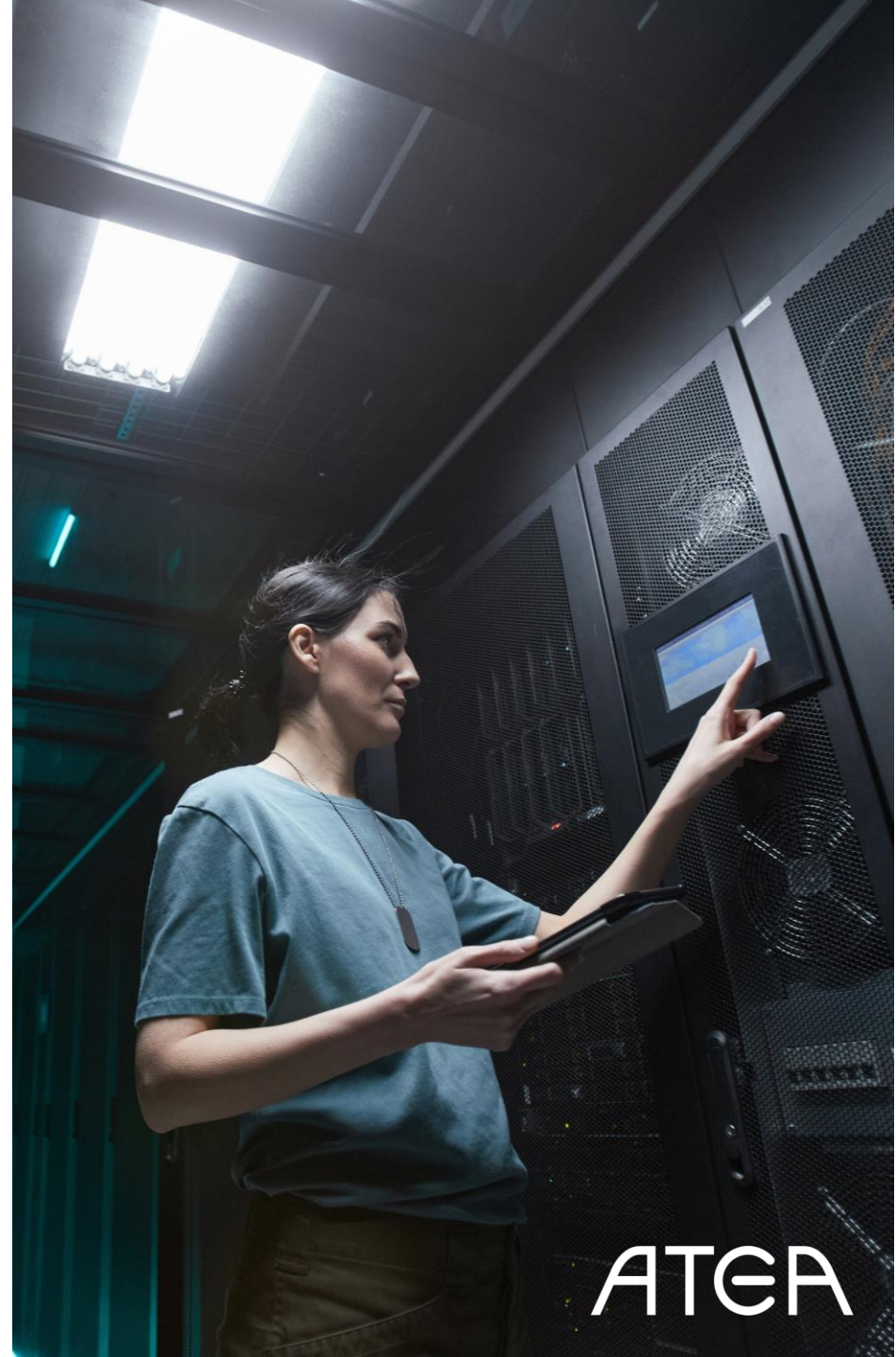
Nėra užtikrinamas tinkamas žurnalinių įrašų fiksavimas, saugojimas ir analizė (III)

Praktinis pavyzdys (poveikis: teisinis, finansinis, reputacinis)

Baudos skyrimo motyvai:

- Nebuvo užtikrinamas tinkamas IT sistemų žurnalinių įrašų kaupimas ir saugojimas, nesilaikoma žurnalinių įrašų saugojimo terminų
- Nebuvo įgyvendintos priemonės, užtikrinančios tinkamą IT sistemų administratorių ir kitų privilegijuotų naudotojų prieigų kontrolę ir autentifikavimą

Šaltinis: Valstybinė duomenų apsaugos inspekcija <https://lrv.lt/lt/>





Atsarginės kopijos saugomos geografiškai nutolusioje vietoje (I)

Grėsmės:

- Kibernetinės atakos (pavyzdžiui, ransomware)
- Fizinės grėsmės (ugnis, vanduo ir pan.) ir kt.

Atsarginių kopijų saugumas turi apimti :

- Jų saugojimą geografiškai nutolusioje vietoje
- Šifravimą
- Atsarginių kopijų testavimą ir kt.



Atsarginės kopijos saugomos geografiškai nenutolusioje vietoje (II)

Praktinis pavyzdys (poveikis: teisinis, finansinis, veiklai, reputacinis)

Situacija: kibernetinės atakos metu buvo užšifruoti vienos valstybinės institucijos duomenys, taip pat ir naujausios atsarginės duomenų kopijos. Dėl šios kibernetinės atakos sutriko valstybinės institucijos paslaugų teikimas, užtruko informacijos atstatymas.

Pasekmės:

- Sutriko paslaugų teikimas (įskaitant socialinių išmokų mokėjimą)
- Atskleisti klientų asmens duomenys
- Skirta 9000 eurų bauda
- Šio atvejo viešinimas viešojoje erdvėje



Atsarginės kopijos saugomos geografiškai nenutolusioje vietoje (II)

Praktinis pavyzdys (poveikis: teisinis, finansinis, veiklai, reputacinis)

Baudos skyrimo motyvai:

- Nebuvo užtikrintas efektyvus duomenų atkūrimas laiku, dėl to buvo sutrikdytas teikiamų paslaugų tęstinumas
- Nebuvo įgyvendintos kitos priemonės (nebuvo naudojamos pakankamos apsaugos nuo kenkimo programų priemonės, netinkamai valdomos prieigos prie serverių teisės, neužtikrinamas slaptažodžių saugumas ir kt.)

Šaltiniai: Valstybinė duomenų apsaugos inspekcija <https://lrv.lt/lt/> ir žiniasklaidos priemonės (straipsniai buvo keliuose portaluose)

ATEA



Nėra vykdomas darbuotojų švietimas (I)

Grėsmės:

- Socialinė inžinerija
- Informacijos perėmimas
- Konfidencialios informacijos atskleidimas ir kt.

Darbuotojų švietimas turi apimti įvairias veiklas:

- Mokymai (bent vieną kartą per metus, naujų darbuotojų apmokymas ir kt.)
- Socialinės inžinerijos imitavimas
- Atmintinės / rekomendacijos / priminimai
- Žinių patikrinimo testai



Nėra vykdomas darbuotojų švietimas (II)

I pavyzdys (poveikis: teisinis, finansinis, reputacinis)

Situacija: dėl darbuotojos žmogiškosios klaidos prie siunčiamo el. laiško buvo prisegtas Excel dokumentas su klientų asmens duomenimis. Laiškas išsiųstas 292 klientams.

Pasekmės:

- atskleisti 29 636 duomenų subjektų asmens duomenys
- skirta 9000 eurų bauda
- šio atvejo viešinimas viešojoje erdvėje



Nėra vykdomas darbuotojų švietimas (III)

I pavyzdys (poveikis teisinis, finansinis, reputacinis)

Baudos skyrimo motyvai:

- Nebuvo atliktas išsamus siunčiamų dokumentų tvarkymo keliamos rizikos vertinimas, testuojant duomenų praradimo prevencijos priemones
- Darbuotoja, išsiuntusi Excel dokumentą, nebuvo tinkamai informuota apie duomenų saugumo procedūras

Šaltinis: Valstybinė duomenų apsaugos inspekcija <https://lrv.lt/lt/>



Nėra vykdomas darbuotojų švietimas (IV)

II pavyzdys: (poveikis finansinis, reputacinis)

Situacija: banko ir teisėsaugos pareigūnais apsimetę sukčiai 2024 m. gruodžio mėn. paskambino vienos įmonės darbuotojai ir iš jos išviliojo įmonės lėšas. Iš darbuotojos banko sąskaitos keliais pavedimais buvo pervesti beveik 9 tūkstančiai eurų ir iš įmonės, kurioje ji dirba, taip pat keliais pavedimais pervesta beveik 200 tūkst. eurų

Pasekmės:

- Finansinės (tik dalį pavedimų pavyko sustabdyti)
- Reputacinės

Šaltinis: žiniasklaidos priemonės (straipsniai buvo keliuose portaluose)

ATERA

Apibendrinimas

Informacijos saugos rizikų vertinimas:

- yra efektyvi priemonė, siekiant nustatyti pažeidžiamumus ir parinkti kontrolės priemones
- padeda nustatyti kontrolės priemonių įgyvendinimo prioritetus / atsako į klausimą „nuo ko pradėti?“



An aerial photograph of a city, likely Vilnius, Lithuania, taken at dusk. The sky is a mix of orange, pink, and blue. The city is densely packed with buildings, many of which have their lights on, creating a warm glow. A river is visible on the left side of the image. The text 'Kuriamė Lietuva su IT' is overlaid in the center in a white, sans-serif font.

Kuriamė Lietuva su IT

ATEA