

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMŲ TENDENCIJOS

Miglė Laima Žukauskaitė

Valstybinės duomenų apsaugos inspekcijos
Informacinių technologijų skyriaus patarėja

// 2026 M. • IKI SPALIO 1 D.

PRANEŠIMŲ APIE ASMENS DUOMENŲ SAUGUMO PAŽEIDIMUS (ADSP) APŽVALGA

248

Pranešimai apie ADSP gauti iki 2026 m. spalio 1 d.

PAGRINDINĖS PRIEŽASTYS

Žmogiškoji klaida	48 %
Kibernetinis incidentas	40 %
Kitos priežastys	12 %

2 717 621

Duomenų subjektą paveikė ADSP

PAŽEIDIMŲ TIPAI

Konfidencialumo pažeidimas	87 %
Vientisumo pažeidimas	5 %
Prieinamumo pažeidimas	6 %
Nelaikyta ADSP	2 %

77 %

pranešimų apie ADSP gauta laiku (per 72 val.)

PRANEŠIMŲ SIUNTĖJAI

Viešieji juridiniai asmenys	43 %
Privatūs juridiniai asmenys	56 %
El. ryšių paslaugų ar tinklų teikėjai	1 %

KIBERNETINIŲ INCIDENTŲ TIPAI



Neteisėtos prieigos prie IT sistemų — 47 · Socialinės inžinerijos atakos — 11 · Duomenų užšifravimo ir išpirkos atakos — 10 · Kenkimo programinės įrangos platinimas — 9 · SQL injekcija — 7 · Aktyvios sesijos perėmimas ir prisijungimo duomenų parinkimo atakos — 9

TAIKYTOS POVEIKIO PRIEMONĖS

9	21	2
Rekomendacijos	Nurodymai	Baudos

Bendra baudų suma 454 500 €

// POVEIKIO MASTAS • 2026 M. IKI SPALIO 1 D.

KIBERNETINIAI INCIDENTAI LEMIA DIDŽIAJĄ POVEIKIO DALĮ

58 %

paveiktų duomenų subjektų nukentėjo
dėl kibernetinių incidentų

1 571 702 asmenys

42 %

paveikė kitos ADSP priežastys – 1 145
919 asmenų

BENDRAS POVEIKIS PAGAL ADSP PRIEŽASTĮ

Kibernetiniai incidentai

1 571 702

Kitos ADSP priežastys

1 145 919

VIDUTINIS POVEIKIS VIENAM ATVEJUI

Kibernetinis incidentas

~16 200

Kitas ADSP

~7 800

Konkretus pavyzdys: 2026 m. birželio mėn. per vieną kibernetinį incidentą, piktavaliui pasinaudojus privilegijuota paskyra ir užšifravus sistemas, paveikti beveik 400 000 duomenų subjektų.

// KIBERNETINIŲ INCIDENTŲ PRIEŽASTYS

KODĖL KIBERNETINIAI INCIDENTAI PAVYKSTA

NUSTATYTOS PRIEŽASTYS • ATVEJŲ SKAIČIUS

Nebuvo kelių faktorių autentifikacijos (MFA)	30
Neatlikti programinės įrangos atnaujinimai	17
Netinkama sistemų konfigūracija	13
Nepakankamai apmokytas personalas	12
Priežastys iš viso nenustatytos	12
Netaikytas neaktyvios sesijos nutraukimas	8

PRIEIGŲ VALDymo SPRAGOS

- MFA netaikomas išoriniams prisijungimams
- Prisijungimai neribojami pagal IP adresus
- Nelykdoma reguliari paskyrų peržiūra
- Nešalinamos nebenaudojamos paskyros

KODĖL PRIEŽASTYS LIEKA NEAIŠKIOS

- Žurnaliniai įrašai saugomi per trumpai
- Įrašai laikomi tame pačiame serveryje
- Nėra apsaugos nuo jų pakeitimo ar ištrynimo

// ATVEJO ANALIZĖ • VDAI 2026 M. KOVO 23 D. SPRENDIMAS

DEBESIJOS PASLAUGŲ TEIKĖJAS ATSAKO KAIP DUOMENŲ TVARKYTOJAS

4 500 €

administracinė bauda duomenų tvarkytojui
– viešosios debesijos paslaugų teikėjui

Incidentas	išpirkos reikalaujanti programa
Taikinys	viešosios debesijos platforma
Prieiga	pasinaudota privilegijuota prieiga
Padariniai	paveikta apie 180 duomenų subjektų

KĄ NUSTATĖ INSPEKCIJA

- Užšifruotos klientų sistemos ir atsarginės kopijos; dalis kopijų prarasta negrįžtamai
- Nebuvo užtikrinta griežta virtualių mašinų izoliacija — nei tinklo, nei prieigos aspektais
- Trūko realių priemonių: MFA išoriniams prisijungimams, VPN jungiantis prie vidinio tinklo, prieigos ribojimo tik įgaliojams asmenims (BDAR 32 str. 1 d. b p.)

KODĖL TAI SVARBU RINKAI

- Sutartis dėl „tik infrastruktūros“ nepanaikina tvarkytojo atsakomybės pagal BDAR 32 str.
- Bazinės saugumo priemonės nėra pakankamos, jei neatitinka realios rizikos

// ATVEJO ANALIZĖ • VDAI 2026 M. BIRŽELIO 19 D. SPRENDIMAS

DU PAŽEIDIMAI TOJE PAČIOJE ĮSTAIGOJE — VIENA BAUDA

ADSP 1 • 2024 M. RUGPJŪTIS–RUGSĖJIS

Neteisėta prieiga prie pacientų sistemos

KAS ĮVYKO

Nutekėjus gydytojos prisijungimo duomenims, trečiasis asmuo kelis kartus prisijungė prie pacientų informacinės sistemos. Paveikti **63 pacientų** asmens duomenys.

KOKIŲ PRIEMONIŲ TRŪKO

- Netaikyta kelių veiksnų autentifikacija (**MFA**) jungiantis per internetą
- Prieiga neapribota pagal **IP adresus** ar teritoriją
- Nebuvo pakankamos prisijungimų stebėsenos — neteisėta prieiga truko kelias savaites



ADSP 2 • 2025 M. SPALIO 29 D.

Išpirkos reikalaujanti (ransomware) ataka

KAS ĮVYKO

Iš kenkėjiško IP adreso per nuotolinio darbalaukio jungtį prisijungta su administratoriaus teises turėjusia paskyra ir užšifruoti sistemose buvę asmens duomenys. Paveikti apie **383 tūkst.** pacientų ir **10 tūkst.** darbuotojų duomenys.

KOKIŲ PRIEMONIŲ TRŪKO

- Netaikyta kelių veiksnų autentifikacija (**MFA**) privilegijuotoms paskyroms jungiantis iš išorės
- Prieiga neapribota pagal IP adresus ar teritoriją — RDP pasiekiamas iš viešojo interneto
- Nenaudojama administratoriaus paskyra nebuvo blokuota (aktyvi nuo 2023 m.)
- Nevykdytos privilegijuotų teisių peržiūros, nestebimi žurnaliniai įrašai



450 000 €

Sveikatos priežiūros įstaigai — už du pažeidimus ir neužtikrintą sveikatos duomenų saugumą

PENKI ŽINGSNIAI, UŽKERTANTYS KELIĄ DAUGUMAI INCIDENTŲ

Tos pačios spragos kartojasi beveik visuose tirtuose pažeidimuose

- 01 Įdiekite kelių veiksmų autentifikaciją (MFA)**
Visiems išoriniams prisijungimams, o ypač privileijuotoms ir administratorių paskyroms.
- 02 Ribokite prieigą pagal IP adresus, vidinį tinklą ar teritoriją**
Nuotolinio darbalaukio (RDP) ir valdymo sąsajos neturi būti pasiekiamos iš viešojo interneto.
- 03 Reguliariai peržiūrėkite paskyras ir prieigos teises**
Nenaudojamas paskyras blokuokite nedelsiant — pamiršta paskyra tampa atakos vektoriumi.
- 04 Kaupkite žurnalinius įrašus atskirai ir ilgiau**
Be tinkamų įrašų incidento priežastis lieka nenustatyta — o tai jau savarankiškas trūkumas.
- 05 Reguliariai mokykite darbuotojus**
Treniruokite gebėjimą atpažinti fišingo laiškus ir saugiai elgtis su prisijungimo duomenimis.



┌
AČIŲ UŽ DĖMESĮ!
└

vdai.lrv.lt