VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAI LIETUVOJE 2025 M.

Asmens duomenų saugumo pažeidimas (toliau – ADSP) – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (Bendrojo duomenų apsaugos reglamento (toliau – BDAR) 4 straipsnio 12 punktas).

Pranešimai apie ADSP teikiami Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) ir duomenų subjektams, vadovaujantis BDAR 33 ir 34 straipsniais.

VDAI apie ADSP privalo pranešti visi duomenų valdytojai pateikdami pranešimą apie ADSP, išskyrus, kai tikėtina, kad toks ADSP nekels pavojaus asmenų teisėms ir laisvėms. Kai dėl ADSP pobūdžio ir rizikos rimtumo gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas apie ADSP privalo pranešti ir duomenų subjektams.

2025 m. VDAI buvo gauti 223 pranešimai apie ADSP (žr. Diagrama Nr. 1), Lietuvoje paveiktų duomenų subjektų skaičius – 1 249 409 (žr. Diagrama Nr. 2). Palyginti su ankstesnių metų duomenimis, 2025 m. VDAI gavo mažiau pranešimų apie ADSP negu 2024 m. (2024 m. VDAI gautų pranešimų apie ADSP skaičius – 273). Taip pat beveik 200 tūkst. sumažėjo Lietuvoje paveiktų duomenų subjektų skaičius (2024 m. Lietuvoje paveiktų duomenų subjektų skaičius – 1 467 368), tai lėmė mažesnis gautų pranešimų apie ADSP skaičius.

Diagrama Nr. 1

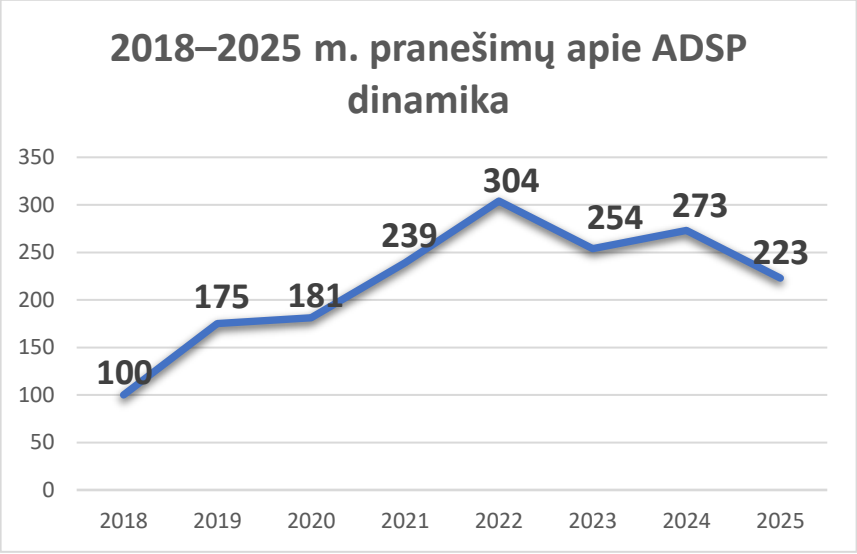
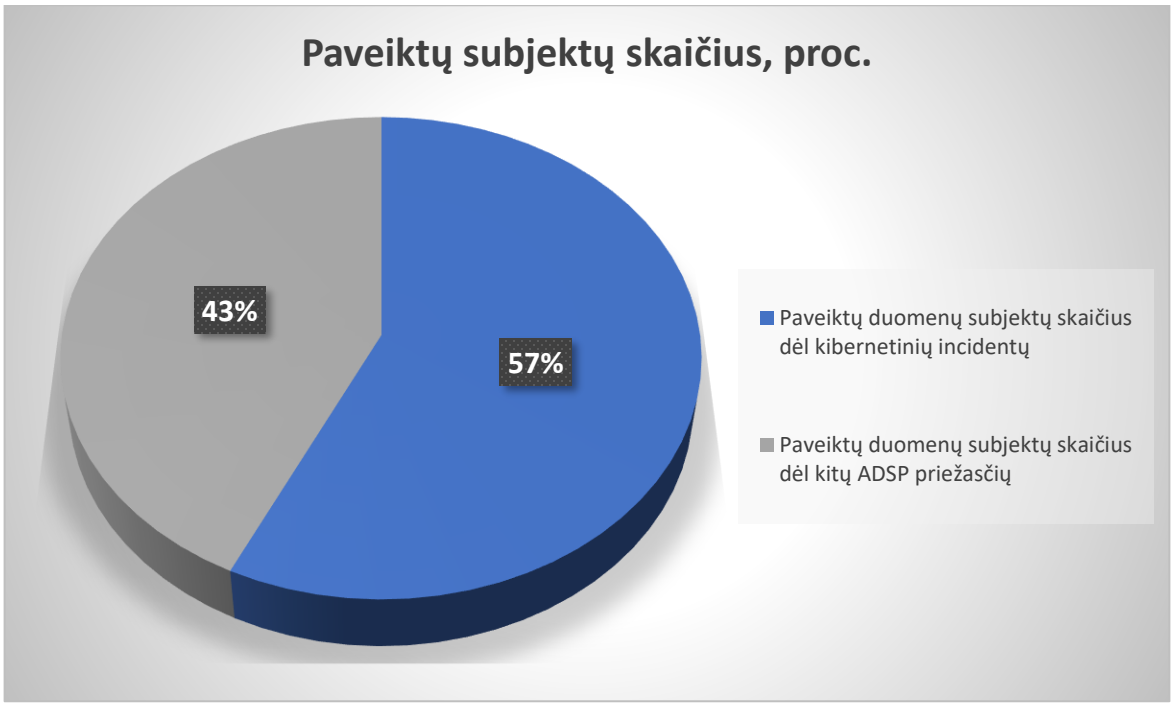


Diagrama Nr. 2

Svarbu paminėti, kad dėl kibernetinių incidentų buvo paveikti 57 proc., t. y. 713 644 (iš visų 2025 m. paveiktų duomenų subjektų) duomenų subjektų duomenys, dėl kitų priežasčių buvo paveikti 43 proc. (535 765) duomenų subjektų duomenys (žr. Diagrama Nr. 3).

Diagrama Nr. 3



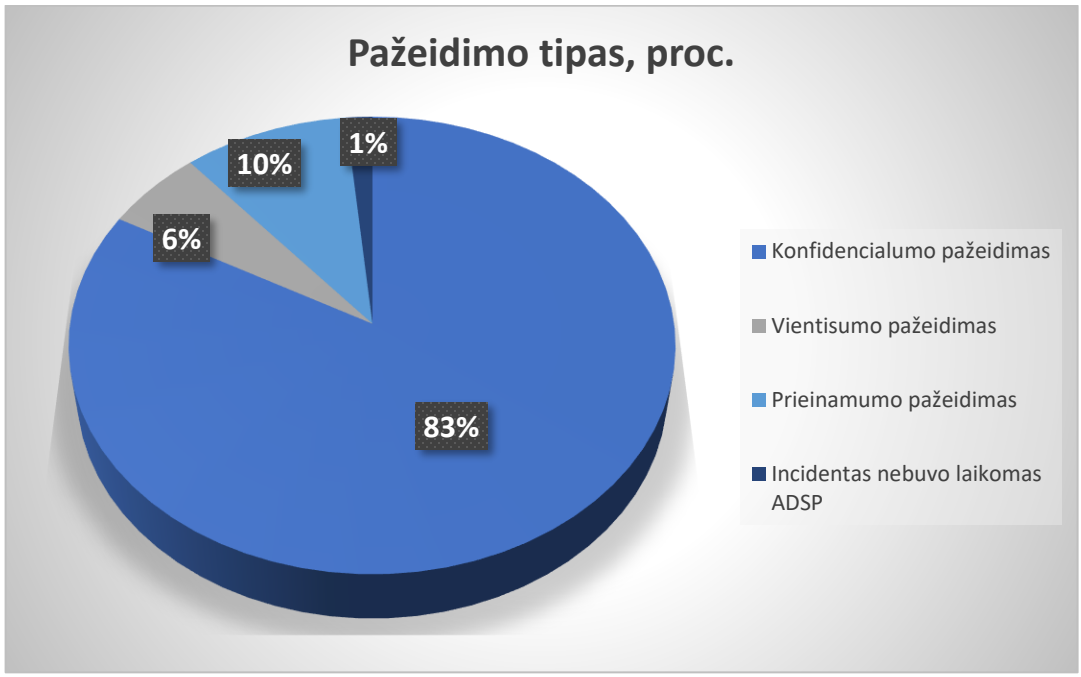
Pagal ADSP pobūdį Lietuvoje statistiškai vyrauja konfidencialumo pažeidimai, kurių skaičius per 2025 m. sudarė net 83 proc. visų atvejų (2024 m. sudarė 87 proc.), 6 proc. atvejų sudarė vientisumo pažeidimai

(2024 m. taip pat sudarė 6 proc.), 10 proc. atvejų – prieinamumo pažeidimai (2024 m. sudarė 6 proc.) ir 1 proc. atvejų incidentas nebuvo laikomas ADSP (neatitiko sąvokos) (2024 m. taip pat sudarė 1 proc.) (žr. Diagrama Nr. 4).

VDAI, įvertinusi gautus pranešimus apie incidentus, kurie nėra laikomi ADSP, nustatė, kad tokie pranešimai buvo susiję su prieigos gavimu prie duomenų, kurie pagal BDAR nėra laikomi asmens duomenimis (pvz., mirusio asmens duomenys), arba pažeidus saugumo priemonę, tačiau faktiškai negavus prieigos prie asmens duomenų. Taip pat VDAI gavo pranešimą apie galimą ADSP iš fizinio asmens, kuris nurodė, kad asmens duomenys buvo tvarkomi vykdant asmeninę, ne profesinę ar komercinę veiklą, todėl remiantis BDAR konstatuojamosios dalies 18 punktu, minėtu atveju BDAR nėra taikomas. Pažymėtina, kad tokiais atvejais teikti ADSP pranešimų VDAI nereikia.

Papildomai atkreiptinas dėmesys, kad VDAI 2025-09-10 paskelbė atnaujintą atvejų, kurie nelaikomi ADSP[1], apibendrinimą. Pastebėtina, kad duomenų valdytojai per 2025 m. nepateikė pranešimų apie atvejus, kurie yra aprašyti apibendrinime.

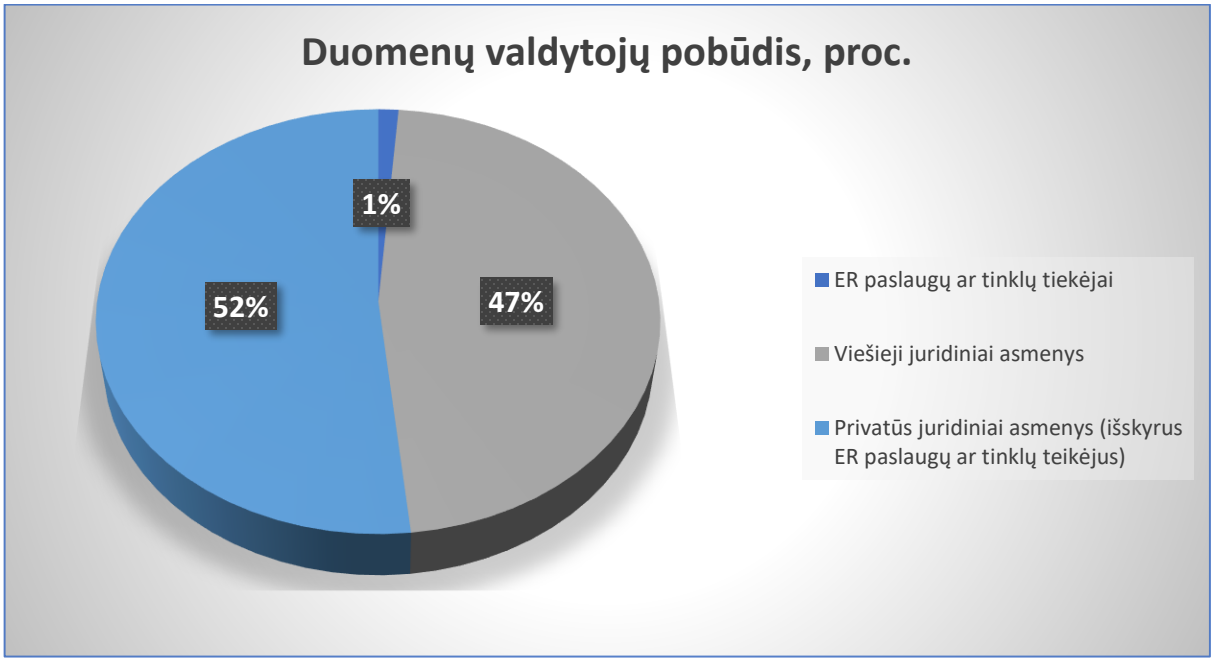
Diagrama Nr. 4



2025 m. daugiausia ADSP pranešimų buvo gauta iš privačių juridinių asmenų – 52 proc., iš viešųjų juridinių asmenų – 47 proc. ir 1 proc. ADSP pranešimų – iš elektroninių ryšių paslaugų ar tinklų tiekėjų (žr. Diagrama Nr. 5). Papildomai pažymėtina, kad 2024 m. ADSP pranešimų, gautų iš privačių juridinių asmenų, taip pat buvo daugiausia (57 proc.).

[1] https://vdai.lrv.lt/lt/naujienos/vdai-pataria-kas-nera-laikoma-asmens-duomenu-saugumo-pazeidimais-7vT/

Diagrama Nr. 5



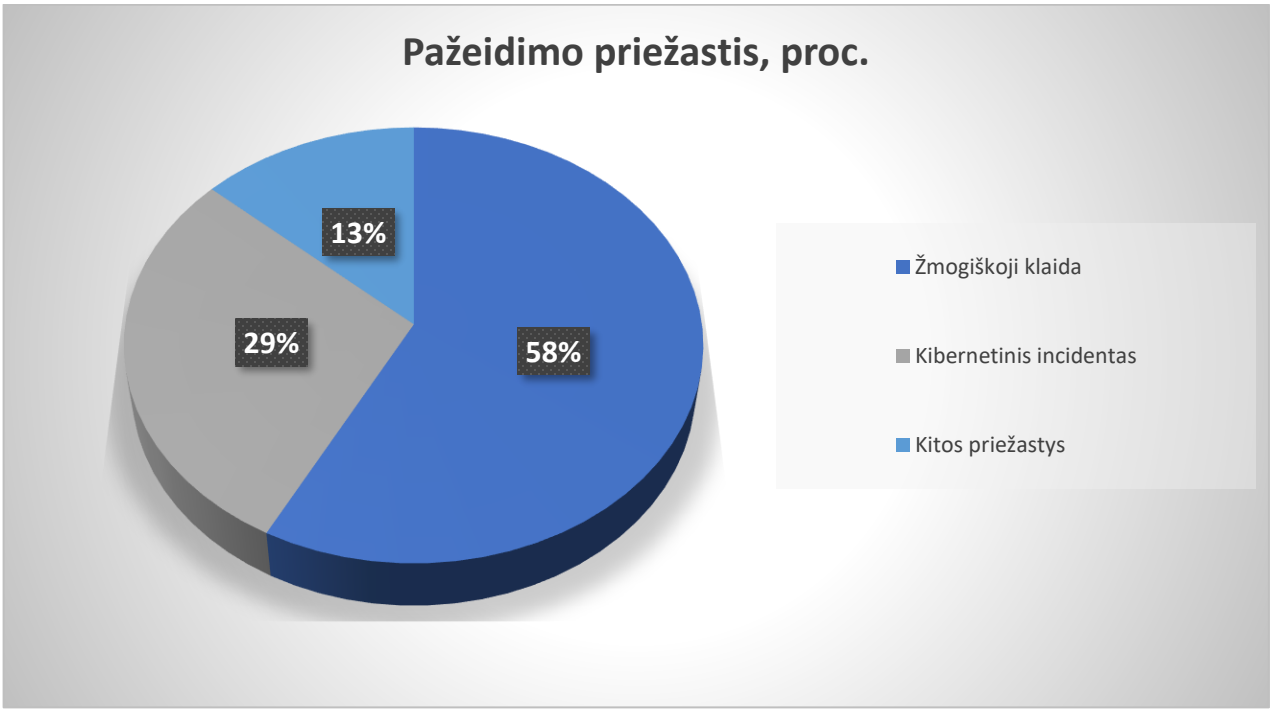
ADSP TENDENCIJOS 2025 M.

VDAI, išanalizavusi 2025 m. gautus pranešimus apie ADSP, nustatė, kad 29 proc. (69) ADSP įvyko dėl kibernetinių incidentų (duomenų užšifravimo, išpirkos reikalavimo, socialinės inžinerijos metodais paremtų ir prisijungimo duomenų užpildymo kibernetinių atakų ir kt.) (žr. Diagrama Nr. 6). Paminėtina, kad 2024 m. buvo gauta 90 tokių pranešimų (33 proc. iš visų 2024 m. gautų pranešimų apie ADSP).

2025 m. 58 proc. ADSP įvyko dėl žmogiškosios klaidos (žr. Diagrama Nr. 6) (2024 m. dėl žmogiškosios klaidos – 52 proc.). Aptariami ADSP įvyksta dėl žmogaus neapdairumo, nežinojimo, kad veiksmai gali sukelti ADSP, taip pat dėl veiksmų, nuo kurių negali apsaugoti įprastai taikomos techninės ir organizacinės priemonės, pavyzdžiui: el. pašto adresų įrašymas į „Kopija“ (angl. *Carbon Copy ar CC),* o ne „Nematoma kopija“ (angl. *Blind Carbon Copy* ar *BCC*), dokumentų su asmens duomenimis siuntimas netinkamiems adresatams, netinkamai nuasmeninto dokumento paviešinimas ir kt.

2025 m. ADSP, įvykę dėl kitų priežasčių, sudaro 13 proc. (žr. Diagrama Nr. 6), t. y. įvairūs IT sistemų trikdžiai, kilę dėl IT sistemų klaidų, dėl kurių atnaujinti duomenys nebuvo laiku perduoti, todėl duomenų valdytojai negalėjo laiku suteikti paslaugų, taip pat nustatyta, kad netinkamai atlikti programavimo darbai arba neatliktas sistemų testavimas prieš jų paleidimą sudarė sąlygas situacijoms, kai asmens duomenys buvo prieinami asmenims, neturintiems teisės su jais susipažinti.

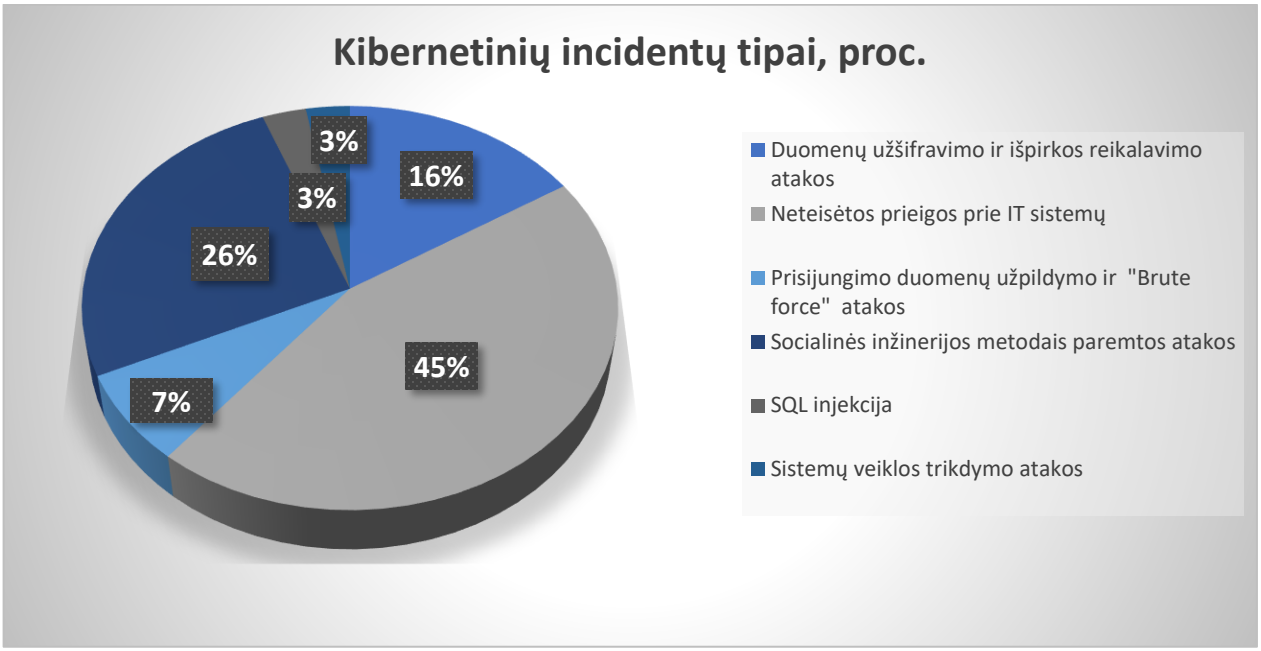
Diagrama Nr. 6



2025 m. gauta 16 proc. (11) pranešimų apie ADSP, kurių metu vyko duomenų užšifravimo ir išpirkos reikalavimo atakos (angl. *Ransomware*), t. y. buvo ne tik užšifruoti serveriai, buhalterinės programos ir kitos sistemos, bet prieš užšifravimą juose esančius duomenis įsilaužėliai nukopijavo ir reikalavo išpirkos už duomenų dešifravimą bei pateikė grasinančius pranešimus nukopijuotus asmens duomenis paskelbti tamsiojo interneto forumuose (angl. *Dark Web Forums*). VDAI buvo gauta 45 proc. (31) pranešimų apie ADSP, kurių metu buvo neteisėtai gautos prieigos prie IT sistemų (žr. Diagrama Nr. 7).

Pastebima, kad 2025 m. 26 proc. (18) ADSP dėl kibernetinių incidentų įvyko dėl socialinės inžinerijos ir duomenų viliojimo (angl. *Phishing*) metodais paremtų atakų, siekiant išvilioti prisijungimų duomenis ar kitus asmens duomenis, pasitelkiant gerai apgalvotus scenarijus. Taip pat 2025 m. buvo vykdomos prisijungimo duomenų užpildymo (angl. *Credential stuffing*) ir brutalios jėgos (angl. *Brute force*) kibernetinės atakos (7 proc. iš visų 2025 m. gautų pranešimų apie įvykusius ADSP dėl kibernetinių incidentų (5), kurių metu piktavaliai, pasinaudoję naudotojų įpročiu naudoti tuos pačius slaptažodžius ir pasinaudoję nutekėjusiais duomenimis (pvz., prisijungimo duomenimis) arba sistemingai bandžius įvairias slaptažodžių kombinacijas buvo atspėti prisijungimo duomenys ir gauta prieiga prie informacinių sistemų. Po 3 proc. ADSP buvo pranešta dėl SQL injekcijų ir sistemų veiklos sutrikdymo atakų (žr. Diagrama Nr. 7).

Diagrama Nr. 7



2025 m. nustatyta, kad ADSP dažnai įvyko dėl prieigos kontrolės valdymo organizacijų kompiuterių tinkluose spragos, kai suteikiant prieigą nėra taikomi apribojimai, nesilaikoma „mažiausių teisių privilegijos“ ir „būtina žinoti“ principų, netaikomas dviejų ir daugiau veiksnių autentifikavimas aukštesnes teises turintiems, nuotoliniu būdu besijungiantiems ar virtualų privatų tinklą naudojantiems vartotojams.

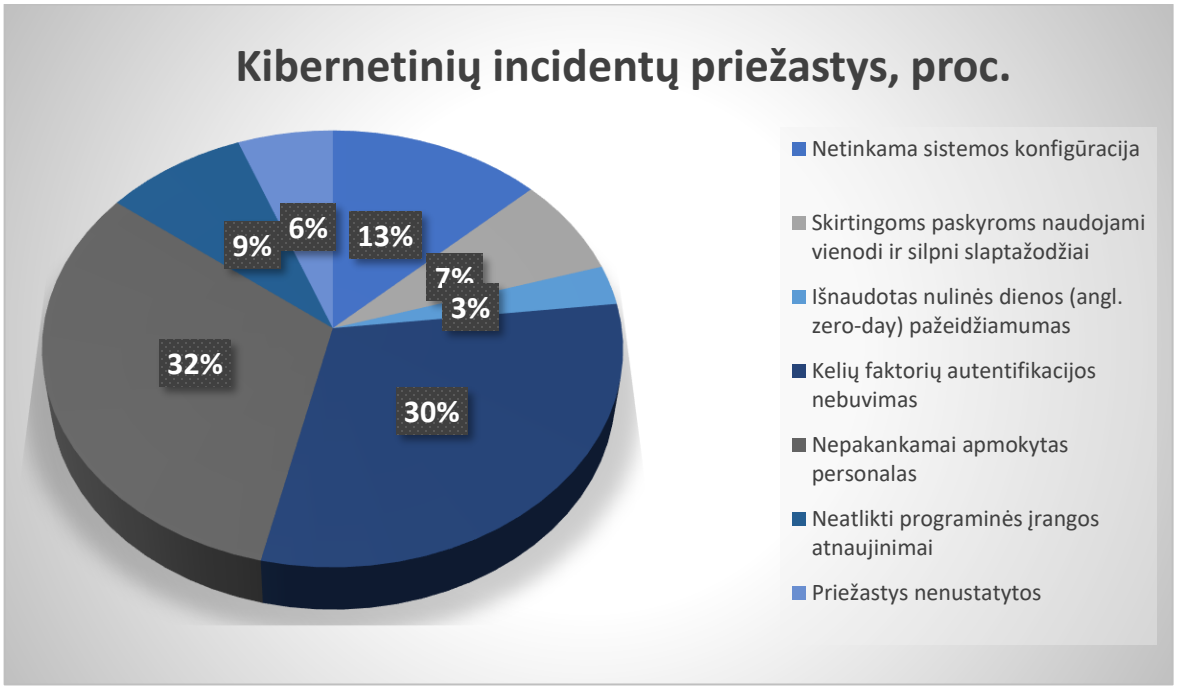
Taip pat pastebima, kad duomenų valdytojai neužtikrina reguliaraus pažeidžiamumų vertinimo, todėl laiku neidentifikuojamos saugumo spragos, kurios gali būti išnaudotos kibernetinių atakų metu.

Dažniausiai pasitaiko, kad ADSP įvyksta dėl kibernetinių incidentų, kurių metu piktavaliai išnaudoja socialinės inžinerijos ir duomenų viliojimo (angl. *Phishing*) metodus. Taip atsitinka, kai darbuotojai nėra tinkamai apmokyti atpažinti kenkėjiškus laiškus ar kitus pranešimus ir paspaudę gautas kenkėjiškas nuorodas suveda ne tik savo prisijungimo duomenis, bet ir papildomą autentifikatorių (pvz., telefone suveda slaptažodį, kuriuo bus atliktas papildomas autentifikavimas). Atsižvelgdami į tai, duomenų valdytojai turi taikyti ne tik tinkamas technines saugumo priemones, kurios padėtų apsaugoti duomenų subjektų asmens duomenis, bet ir organizacines, tokias kaip nuolatinį darbuotojų švietimą ar socialine inžinerija paremtas pratybas, kad darbuotojai, gavę kenkėjiškus laiškus, juos atpažintų ir neatidarytų kenkėjiškų nuorodų ar kitų priedų.

2025 m. dažna problema išlieka duomenų užšifravimo ir išpirkos reikalavimo atakos, kurių metu piktavaliai pašalina duomenų atsargines kopijas ir įvykių žurnalinius įrašus, kurie buvo saugomi toje pačioje vietoje, kaip ir užšifruoti duomenys, dėl to duomenų valdytojai nebegali lengvai atkurti duomenų prieinamumo bei tinkamai atlikti kibernetinio incidento ir ADSP tyrimų.

KIBERNETINIŲ INCIDENTŲ, DĖL KURIŲ ĮVYKO ADSP, PRIEŽASTYS

Diagrama Nr. 8



Pagrindinės kibernetinių incidentų priežastys dėl kurių įvyko ADSP (žr. Diagrama Nr. 8):

- nepakankamai apmokytas personalas (32 proc.);
- kelių faktorių autentifikavimo nebuvimas (30 proc.);
- netinkamai sukonfigūruoti sistemų saugos parametrai (13 proc.);
- reguliariai ir nedelsiant neatliekami programinės įrangos atnaujinimai (9 proc.);
- skirtingoms paskyroms naudojami vienodi slaptažodžiai (7 proc.);
- išnaudotas nulinės dienos (angl. *zero-day*) pažeidžiamumas (3 proc.).

Papildomi faktoriai dėl kurių įvyko ADSP:

- nevykdoma kompiuterių tinklų duomenų srautų stebėsena, nevykdomas įsilaužimų aptikimas ir prevencija;
- nevykdoma prieigos kontrolė;
- perteklinis privilegijuotų teisių naudojimas;
- nėra taikomas IP filtravimas;

- naršyklėse saugomi prisijungimo duomenys;
- naudojami slaptažodžiai nėra stiprūs ir kompleksiški;
- naudojami slaptažodžiai nėra reguliariai keičiami.

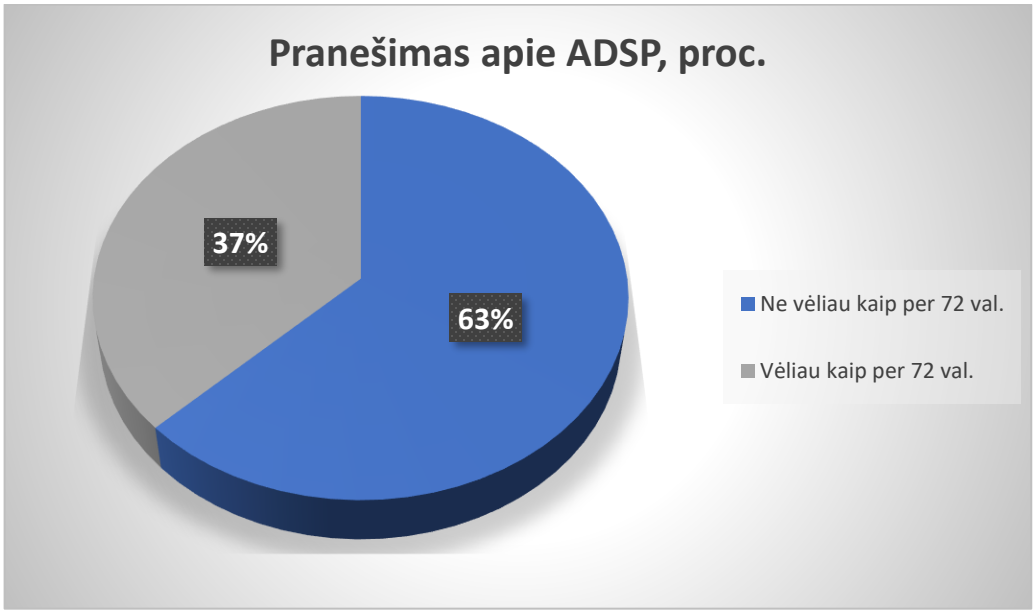
Papildomai atkreiptinas dėmesys, kad 6 proc. iš visų 2025 m. gautų pranešimų apie ADSP (įvykusių dėl kibernetinių incidentų) nebuvo nustatytos incidento priežastys (žr. Diagrama Nr. 8). Šis rodiklis rodo, kad vis dar pasitaiko atvejų, kai įvykus kibernetiniam incidentui duomenų valdytojai ar duomenų tvarkytojai negalėjo tinkamai atlikti kibernetinio incidento tyrimo ir nustatyti priežastis, kurių išaiškinimas galėtų ateityje padėti išvengti tokio pobūdžio atakų. Taip atsitinka dėl to, kad žurnaliniai įrašai yra saugomi per trumpą laiką, taip pat saugomi tame pačiame serveryje arba nėra taikomos priemonės, apribojančios galimybę žurnalinius įrašus ištrinti, sugadinti ar pakeisti.

PRANEŠIMŲ APIE ADSP TEIKIMAS PRIEŽIŪROS INSTITUCIJAI

VDAI atkreipia dėmesį, kad nustatęs, jog ADSP įvyko ir kad yra pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas nedelsdamas, bet ne vėliau kaip per 72 val. nuo sužinojimo apie ADSP, privalo pranešti apie tai VDAI, kaip tai numato BDAR.

2025 m. 63 proc. duomenų valdytojų apie įvykusį ADSP pranešė ne vėliau kaip per 72 val., 37 proc. – vėliau kaip per 72 val. (žr. Diagrama Nr. 9). Palyginti su ankstesnių metų duomenimis, duomenų valdytojai dažniau teikia pranešimus pavėluotai (2024 m. 79 proc. duomenų valdytojų apie įvykusį ADSP pranešė ne vėliau kaip per 72 val., 21 proc. – vėliau kaip per 72 val.).

Diagrama Nr. 9



Išanalizavus ADSP pranešimus, kurie pateikti vėliau nei per 72 val. nuo sužinojimo apie ADSP momento, nustatyta, kad duomenų valdytojai kartais nenurodo vėlavimo priežasčių (BDAR 33 straipsnio 1 dalis). Taip pat paminėtina, kad dažniausia pranešimo VDAI vėlavimo priežastis – duomenų valdytojas ilgai aiškinasi ADSP aplinkybes ir duomenų subjektams keliamą pavojų. VDAI atkreipia dėmesį, kad duomenų valdytojai, nustatę, kad ADSP yra sudėtingas ir jo tyrimas užtruks (jei duomenų valdytojas nustato, kad per 72 val. visos informacijos pateikti negalės), **pranešimus gali teikti dalimis**, t. y. pirminis pranešimas turi būti teikiamas iškart sužinojus apie įvykusį ADSP, jame nurodant, kad tai yra pirminis pranešimas ir papildoma informacija bus pateikta vėliau.

Taip pat dažnai pasitaiko, kad duomenų valdytojai, teikdami pranešimus VDAI, nenurodo visos būtinos pateikti informacijos, kaip tai numato BDAR 33 straipsnio 3 dalis.

Pranešimuose apie įvykusį ADSP turi būti nurodoma:

- asmens duomenų saugumo pažeidimo pobūdis, įskaitant, jeigu įmanoma, atitinkamų duomenų subjektų kategorijos ir apytikslis jų skaičius, taip pat atitinkamų asmens duomenų įrašų kategorijos ir apytikslis jų skaičius;
- duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, vardas bei pavardė (pavadinimas) ir kontaktiniai duomenys;
- tikėtinos asmens duomenų saugumo pažeidimo pasekmės;
- priemonės, kurių ėmėsi arba pasiūlė imtis duomenų valdytojas, kad būtų pašalintas asmens duomenų saugumo pažeidimas, įskaitant, kai tinkama, priemones galimoms neigiamoms jo pasekmėms sumažinti.

Atsižvelgdama į tai, VDAI rekomenduoja naudoti VDAI patvirtintą pranešimo apie ADSP formą ir pildant pranešimą pateikti išsamią informaciją apie įvykusį ADSP[2].

Taip pat pasitaiko atvejų, kad duomenų valdytojai, negalėdami nurodyti privalomos informacijos, nurodo, kad buvo pradėtas tyrimas dėl ADSP ar kibernetinio incidento ir iki pranešimo teikimo dienos jis nėra baigtas. Tokiu atveju, teikiant pirminius pranešimus VDAI, prašome nurodyti datą, kada planuojama pradėtą tyrimą baigti.

2025 M. DUOMENŲ VALDYTOJAMS TAIKYTOS POVEIKIO PRIEMONĖS

2025 m. sausio mėn. VDAI, atlikusi ADSP tikrinimą, priėmė sprendimą viešajai įstaigai skirti 9 tūkst. eurų baudą už nustatytus BDAR nuostatų pažeidimus. VDAI nustatė, kad ADSP įvyko dėl įdiegtų duomenų praradimo prevencijos priemonių netinkamo testavimo atlikimo ir daromos nepagrįstos prielaidos, kad scenarijui neatitikus nustatytos taisyklės, priemonė suveiks. Tačiau duomenų praradimo prevencijos

[2] https://vdai.lrv.lt/lt/adsp-ir-dap/pranesimas-apie-asmens-duomenu-saugumo-pazeidima/

priemonė nesuveikė, dėl to 292 asmenims buvo išsiųstas el. laiškas su pridėtu Excel dokumentu, kuriame buvo 29 636 duomenų subjektų asmens duomenys, įskaitant specialių kategorijų asmens duomenis.

2025 m. vasario mėn. VDAI, atlikusi ADSP tikrinimą, priėmė sprendimą viešajai įstaigai skirti 3 529 eurų baudą už nustatytus BDAR nuostatų pažeidimus. VDAI nustatė, kad įvyko kibernetinė ataka, kurios metu piktavalis įsilaužė į vidinį tinklą ir užšifravo 120 duomenų subjektų duomenis, įskaitant ir specialių kategorijų duomenis. Šiuo atveju duomenų valdytojas nebuvo dokumentavęs ir apibrėžęs vaidmenų ir atsakomybių, neturėjo prieigos valdymo politikos ir tinkamai nevaldė prieigos teisių. Taip pat nebuvo užtikrinta prieigų kontrolė ir autentifikavimas, neįgyvendinta kompiuterinių darbo vietų techninių įrašų registravimo ir stebėsenos sistema, o naudotojams kompiuterinėse darbo vietose buvo suteiktos administratoriaus teisės.

2025 m. liepos mėn., atlikusi ADSP tikrinimą, priėmė sprendimą viešajai įstaigai skirti 4 500 eurų baudą už nustatytus BDAR nuostatų pažeidimus. VDAI nustatė, kad viešojoje įstaigoje įvyko įsilaužimas ir buvo užšifruoti duomenys. ADSP metu buvo pažeistas 22 000 duomenų subjektų asmens duomenų saugumas, įskaitant ir specialių kategorijų duomenis. Šiuo atveju duomenų valdytojas nebuvo dokumentavęs ir apibrėžęs vaidmenų ir atsakomybių, neturėjo prieigos valdymo politikos ir tinkamai nevaldė prieigos teisių. Taip pat nebuvo užtikrinta prieigų kontrolė ir autentifikavimas, neįgyvendinta kompiuterinių darbo vietų techninių įrašų registravimo ir stebėsenos sistema, o naudotojams kompiuterinėse darbo vietose buvo suteiktos administratoriaus teisės.

2025 m. spalio mėn. VDAI atlikusi stebėseną, priėmė sprendimą privačiam juridiniam asmeniui skirti 4 500 eurų baudą už atsisakymą teikti informaciją (bendradarbiauti su VDAI) t. y. už informacijos neteikimą, nurodant, kad tokią informaciją teikia tik teisėsaugos institucijoms, todėl pažeidė BDAR 58 straipsnio 1 dalies a punktą.

Taip pat 2025 m. spalio mėn. VDAI atlikusi ADSP tikrinimą, priėmė sprendimą privačiam juridiniam asmeniui skirti 6 tūkst. eurų baudą už nustatytus BDAR 5 straipsnio 1 dalies f punkto, 32 straipsnio 1 dalies b ir d punktų pažeidimus. VDAI nustatė, kad piktavaliui pasinaudojus privilegijuotas prieigos teisių turinčių naudotojų prisijungimo duomenimis buvo įsilaužta į duomenų bazę ir nutekinti 39 794 duomenų subjektų asmens duomenys. Šiuo atveju duomenų valdytojas nebuvo dokumentavęs slaptažodžių politikos ir neužtikrino reguliaraus privilegijuotų naudotojų slaptažodžių keitimo, nebuvo užblokavęs prieigos prie bendrovės tinklo iš išorės, neužtikrino ir neorganizavo darbuotojų mokymų apie asmens duomenų apsaugą ir saugumo procedūras.

2025 m. VDAI, įvertinusi gautus pranešimus apie ADSP ir nustačiusi, kad yra netinkamai užtikrinamas duomenų subjektų asmens duomenų saugumas, vadovaudamasi teisės aktų nuostatomis teikė 9 nurodymus duomenų valdytojams arba duomenų tvarkytojams suderinti duomenų tvarkymo operacijas su BDAR nuostatomis. Taip pat teikė 22 rekomendacijas duomenų valdytojams, kurios padėtų užtikrinti, kad asmens duomenų tvarkymas atitiktų BDAR reikalavimus.

REKOMENDACIJOS

Organizacinės ir techninės saugumo priemonės, padedančios išvengti ADSP:

- užtikrinti įsilaužimų stebėjimą, aptikimą ir užkardymą;
- žurnalinius įrašus saugoti ne trumpiau nei 3 mėnesius;
- užtikrinti, kad žurnaliniai įrašai ir duomenų atsarginės kopijos būtų saugomi atskiruose serveriuose ir geografiškai nutolusiose vietose, siekiant sumažinti duomenų praradimo riziką;
- užtikrinti reguliarų sistemų pažeidžiamumų skenavimo vykdymą;
- tinkamai sukonfigūruoti išorinėje komunikacijoje dalyvaujančius serverius ir kitą įrangą pagal gerąsias praktikas;
- apriboti išorinio prisijungimo galimybes tokiais protokolais kaip *Windows Remote Desktop Protocol,* daiktų interneto SSH prievadais ir pan.;
- prie IT sistemų leisti jungtis tik iš žinomų IP adresų (angl. *Allow List*) arba prisijungimui naudoti virtualaus privataus tinklo technologijas (angl. *Virtual Private Network*, VPN);
- naudoti ugniasienę ir antivirusinę programinę įrangą su automatiniais atnaujinimais;
- nenaudoti tų pačių slaptažodžių skirtingoms paskyroms, užtikrinti, kad prisijungimų prie IT sistemų slaptažodžiai būtų saugūs ir kompleksiški, naudoti kelių lygių autentifikavimą (el. pašto internetinei prieigai, VPN prieigai, paskyroms, kurios turi prieigą prie kritiškai svarbių sistemų);
- užtikrinti, kad naršyklėse nebūtų saugomi prisijungimo duomenys;
- atlikus sistemų pakeitimus, programavimo darbus ar paleidžiant naujus produktus būtina atlikti sistemos pažeidžiamumo ir atsparumo testavimą;
- apriboti asmeninių įrenginių darbo funkcijoms naudojimą, jei tai padaryti nėra galimybių, turi būti užtikrintas asmeninių ir organizacijos duomenų atskyrimas, naudojant saugias programinės įrangos talpyklas (konteinerius), atskiras paskyras ar kitas organizacijos patvirtintas duomenų segmentavimo priemones;
- įdiegti el. pašto filtravimo mechanizmus, gebančius filtruoti laiškus pagal žinomus grėsmių indikatorius ir specifinius raktažodžius;
- įdiegti prieigos kontrolę pagal organizacijos saugumo politiką, taikant „mažiausių teisių privilegijos“ ir „būtina žinoti“ principus;
- periodiškai mokyti darbuotojus apie IT sistemų saugumo reikalavimus;
- periodiškai organizuoti duomenų viliojimo metodais paremtų atakų simuliacijas;
- taikyti „Keturių akių“ principą, siekiant sumažinti žmogiškosios klaidos riziką, užtikrinant, kad esminiai veiksmai, galintys turėti įtakos asmens duomenų saugumui, būtų patikrinti ir patvirtinti bent dviejų atsakingų asmenų;

- organizacinėmis ir techninėmis priemonėmis užtikrinti, kad siunčiami failai su asmens duomenimis būtų užšifruoti ir apsaugoti slaptažodžiu (slaptažodis turi būti siunčiamas kitu komunikacijos kanalu arba iš anksto sutartas);
- el. pašto programinėje įrangoje naudoti gavėjų grupių klasifikatorius (tai padės užtikrinti siunčiamos informacijos saugumą pagal pritaikytas saugumo politikas, pavyzdžiui, siunčiant dokumentus išorės gavėjams, dokumentai siunčiami šifruoti ir apsaugoti slaptažodžiais bei nustatoma, kiek laiko siunčiami dokumentai gali būti pasiekiami);
- el. pašto programinėje įrangoje naudoti siunčiamų el. laiškų ir jų priedų filtravimą, kuris prieš siunčiant el. laiškus įvertintų, ar siunčiamuose el. laiškuose ir jų prieduose nėra asmens duomenų;
- užtikrinti, kad su duomenų tvarkytojais būtų pasirašytos paslaugų teikimo sutartys, asmens duomenų tvarkymo susitarimai ar kiti dokumentai, kuriuose būtų nustatyta prievolė užtikrinti, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų BDAR reikalavimus;
- jeigu yra galimybė, užtikrinti, kad būtų reguliariai atliekami duomenų tvarkytojų auditai, kurių metu duomenų valdytojas galėtų įsitikinti, jog duomenų tvarkytojas laikosi sutartyse ar kituose dokumentuose nustatytų reikalavimų.