ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAI LIETUVOJE 2024 M. I PUSMETĮ

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).

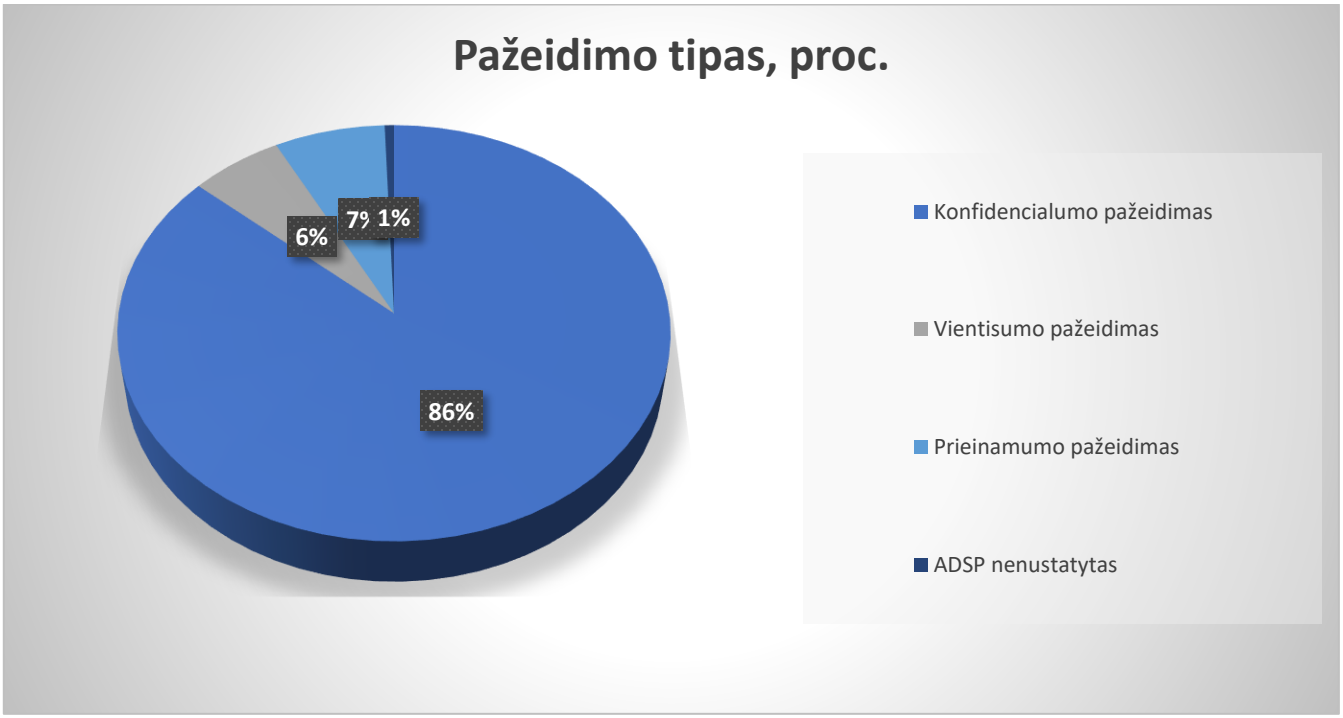
Pranešimai apie ADSP teikiami Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI) ir duomenų subjektams, vadovaujantis BDAR 33 ir 34 straipsniais.

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 kyla didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas apie ADSP privalo pranešti ir duomenų subjektui.

Apžvelgiant į 2024 m. I pusm. pranešimų apie ADSP Lietuvoje statistiką, VDAI buvo gautas 151 panešimas apie ADSP, Lietuvoje paveiktų duomenų subjektų skaičius – 402446.

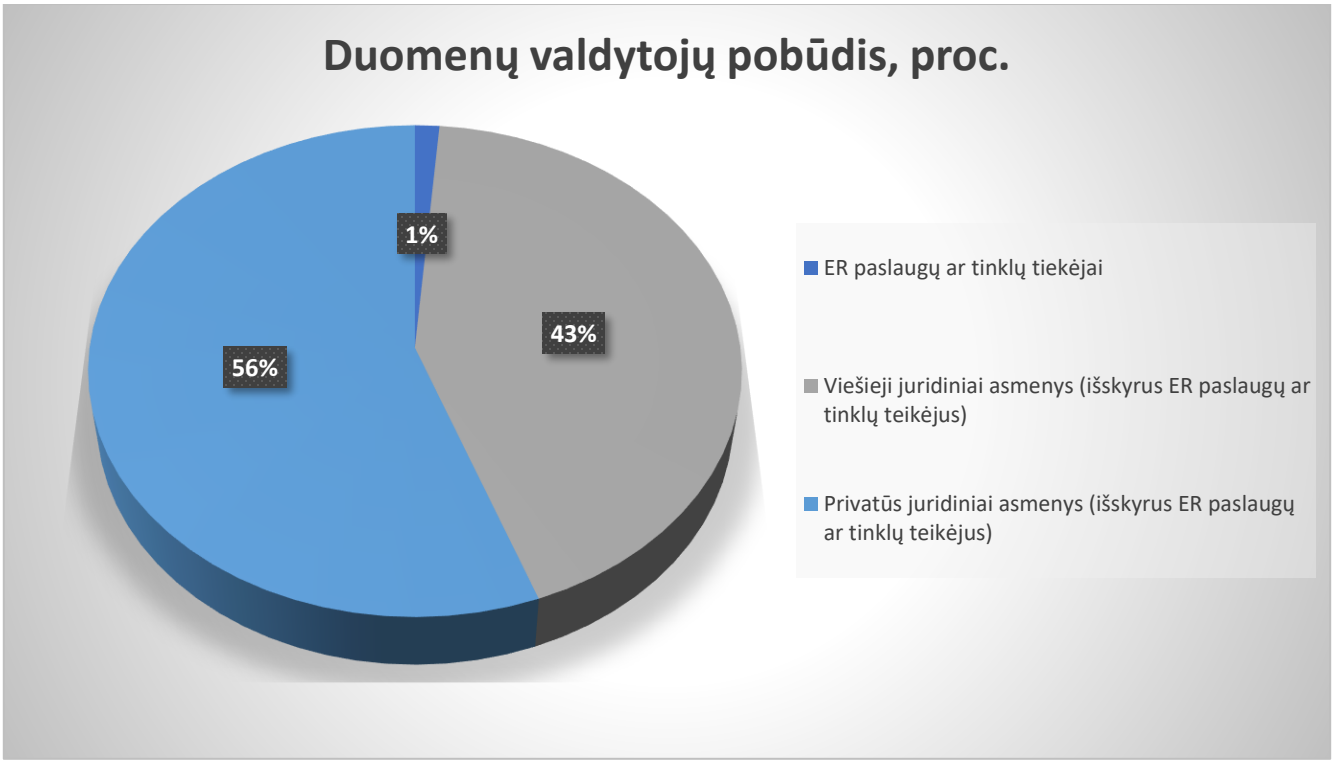
Pagal ADSP pobūdį Lietuvoje statistiškai vyrauja konfidencialumo pažeidimai, kurių skaičius per 2024 m. I pusm. sudarė net 86 proc. visų atvejų, 6 proc. atvejų vientisumo pažeidimai, 7 proc. atvejų prieinamumo pažeidimai.

Papildomai atkreiptinas dėmesys, kad VDAI 2024-01-11 paskelbė atvejų apibendrinimą, kurių VDAI nelaiko ADSP[1]. Pastebėtina, kad duomenų valdytojai per 2024 m. I pusm. nepateikė pranešimų apie atvejus, kurie yra aprašyti apibendrinime.

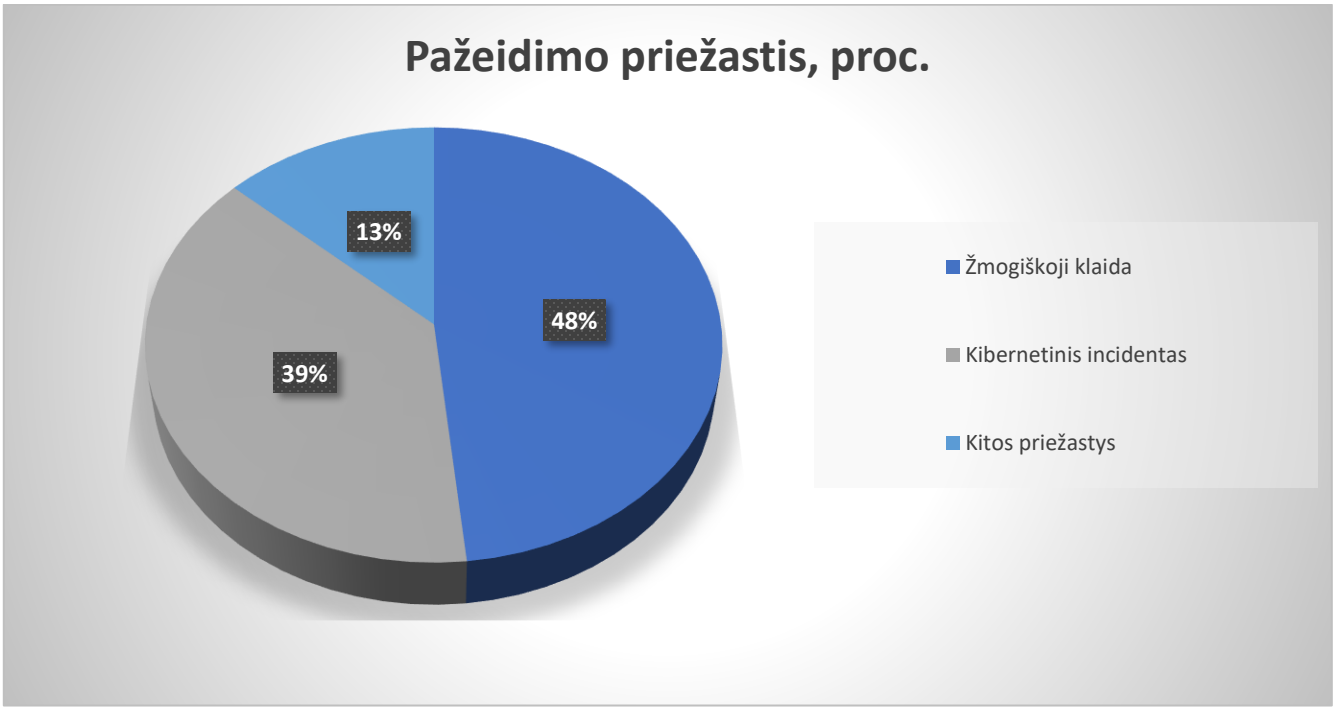


[1] https://vdai.lrv.lt/lt/naujienos/vdai-pataria-del-pasitaikanciu-atveju-kai-pranesama-apie-ivykusius-incidentus-kurie-nera-laikomi-asmens-duomenu-saugumo-pazeidimais/

2024 m. I pusm. daugiausia ADSP pranešimų buvo gaunama iš privačių juridinių asmenų – 56 proc., iš viešųjų juridinių asmenų – 43 proc., visų atvejų ir 1 proc. atvejų pranešimų – iš elektroninių ryšių paslaugų ar tinklų teikėjų.



2024 m. I pusm. ADSP tendencijos



2024 m. I pusm. 48 proc. ADSP įvyko dėl žmogiškosios klaidos. Pastebima, kad VDAI yra mažiau pranešama apie ADSP, kurie įvyko dėl žmogiškosios klaidos. Tai rodo 2024 m. I pusm. statistikos palyginimas su 2023 m. I pusm. (ADSP, įvykę dėl žmogiškosios klaidos, sudarė net 77 proc. visų gautų ADSP).

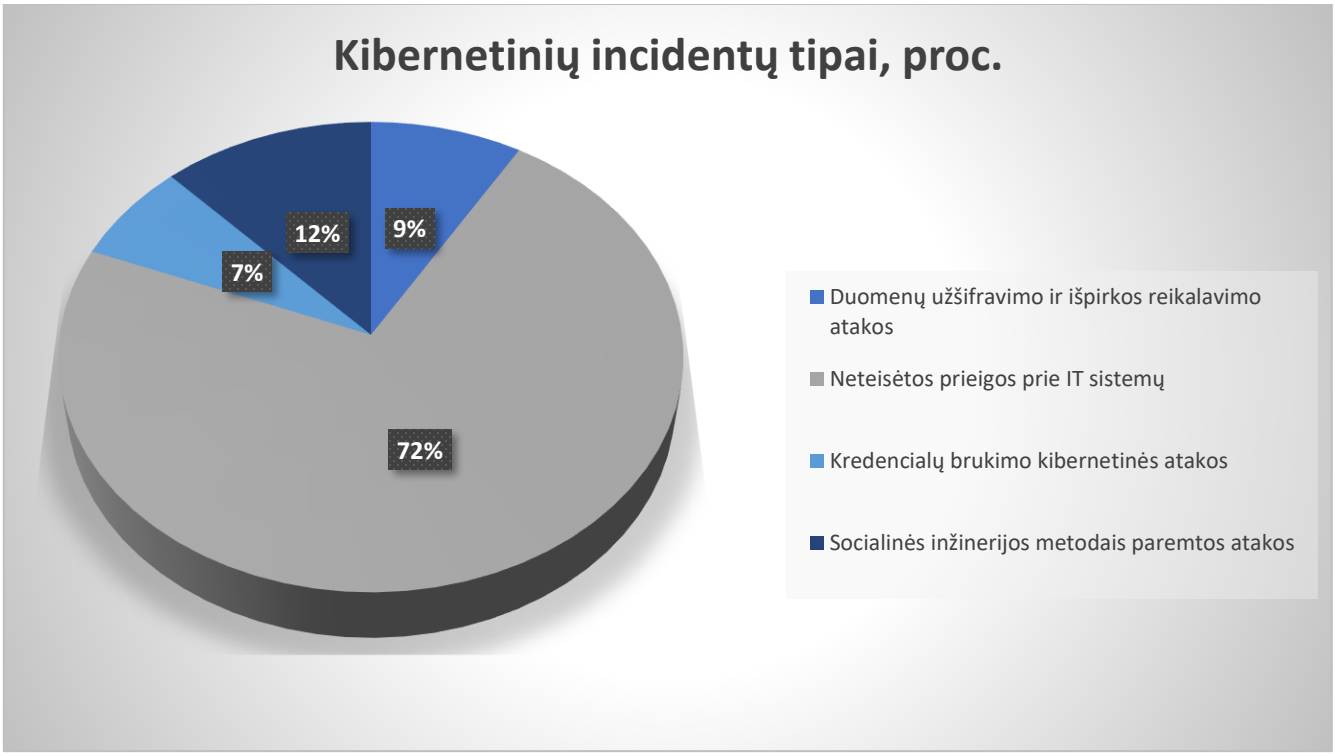
Aptariami ADSP įvyksta dėl žmogaus padaromų veiksmų, kurie pasireiškia neapdairumu, nežinojimu, kad veiksmai gali sukelti ADSP, taip pat dėl veiksmų, nuo kurių apsaugoti negali įprastai taikomos techninės ir organizacinės priemonės, pavyzdžiui, el. pašto adresų įrašymas į „Kopija“ (ar angl. *CC*), o ne „Nematoma kopija“ (ar angl. *BCC*), dokumentų su asmens duomenimis siuntimas netinkamiems adresatams, netinkamai nuasmeninto dokumento paviešinimas ir kt.

VDAI, atsižvelgdama į tai, kad ADSP dažniausiai įvyksta dėl žmogiškosios klaidos, atkreipia dėmesį, kad darbuotojų mokymai yra svarbi priemonė minimizuojant žmogiškąsias klaidas. Mokymai apie duomenų apsaugą yra svarbūs vykdant prevenciją dėl netyčinio duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų (BDAR 32 straipsnio 2 dalis). Taip pat efektyvi priemonė yra „Keturių akių“ principo įgyvendinimas. Siekiant išvengti ADSP dėl žmogiškosios klaidos, kai asmens duomenys per klaidą yra išsiunčiami netinkamiems adresatams, duomenų valdytojai gali, pavyzdžiui, organizacinėmis ir techninėmis priemonėmis užtikrinti, kad siunčiami failai su asmens duomenimis būtų užšifruoti ir apsaugoti slaptažodžiu (slaptažodis turi būti siunčiamas kitu kanalu arba iš anksto sutartas), el. pašto programinėje įrangoje naudoti gavėjų grupių klasifikatorius (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) ir kt.

2024 m. I pusm. ADSP įvykę dėl kitų priežasčių sudaro 13 proc., tai buvo įvairūs IT sistemų trikdžiai ir kt., pavyzdžiui, dėl IT sistemos klaidos atnaujinti duomenys nebuvo laiku perduoti, dėl to

duomenų valdytojas negalėjo laiku suteikti paslaugų, taip pat netinkamai atlikus programavimo darbus, asmens duomenys buvo pasiekiami asmenims, kurie neturėjo teisės su jais susipažinti ar kt.

VDAI išanalizavusi per 2024 m. I pusm. gautus pranešimus apie ADSP nustatė, kad 58 (39 proc.) ADSP įvyko dėl kibernetinių incidentų (duomenų užšifravimo, išpirkos reikalavimo, socialinės inžinerijos metodais paremtų ir kredencialų brukimo kibernetinių atakų ir kt.), o jų metu buvo paveikti 75 proc. (iš visų 2024 m. I pusm. paveiktų subjektų) subjektų duomenys, dėl žmogiškosios klaidos ir kitų priežasčių buvo paveikti tik 25 proc. subjektų duomenys. Svarbu paminėti, kad lyginant 2024 m. I pusm. gautus pranešimus apie ADSP su 2023 m. I pusm. (ADSP įvykę dėl kibernetinio incidento sudarė tik 15 proc. iš visų gautų ADSP), pastebima, kad VDAI vis daugiau pranešama apie ADSP, kurie įvyko dėl kibernetinių incidentų.

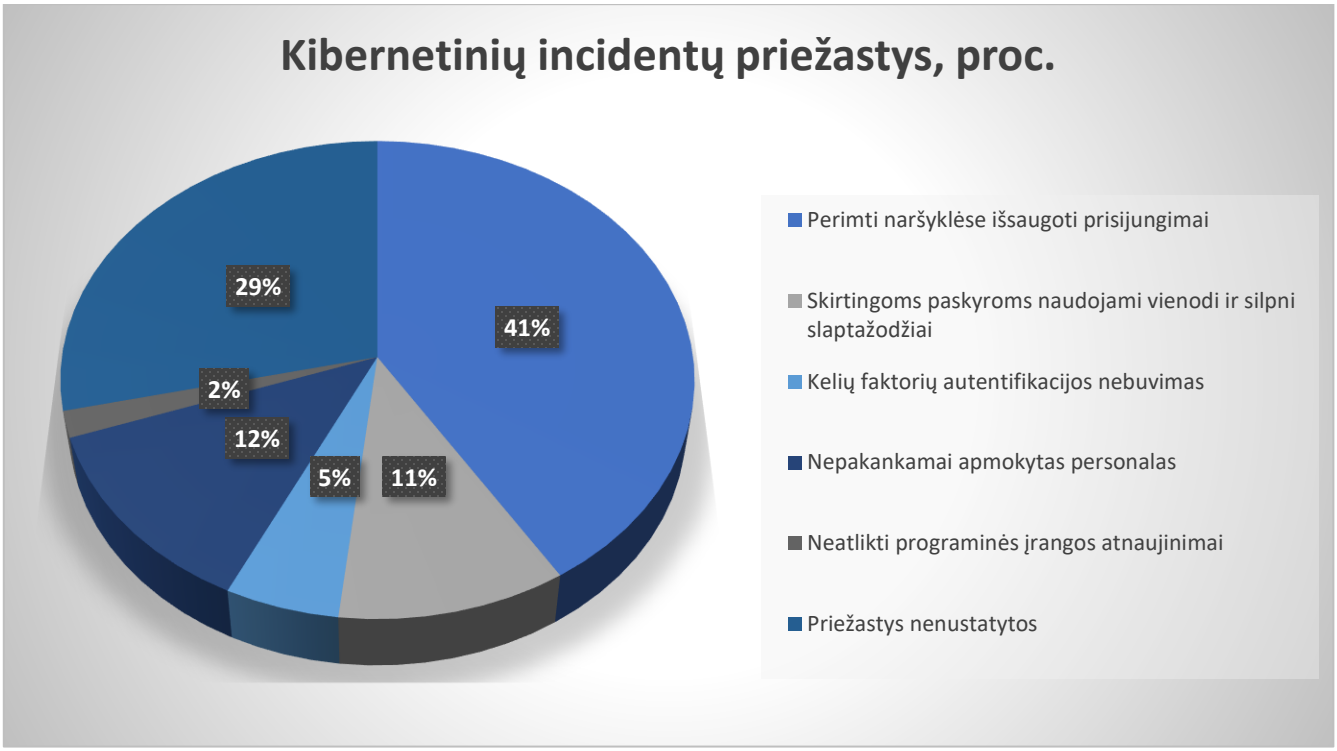


2024 m. I pusm. gauti 5 pranešimai apie ADSP, kurių metu vyko duomenų užšifravimo ir išpirkos reikalavimo atakos (angl. *Ransomware*). 42 pranešimai apie ADSP, kurių metu buvo neteisėtai gautos prieigos prie IT sistemų (pastebėta, kad tokie incidentai dažnai įvykdavo darbuotojams išsaugojus IT sistemų prisijungimo duomenis naršyklėse).

ADSP metu piktavaliai naudojo įvairius socialinės inžinerijos ir duomenų viliojimo (angl. *Phishing*) metodus, siekdami išvilioti įvairiausius prisijungimų duomenis, pasitelkdami gerai apgalvotus scenarijus ir įvairius ryšio užmezgimo kanalus. Lyginant su 2023 m. gautais pranešimais apie ADSP, pastebima, kad 2024 m. I pusm. buvo vykdomos kredencialų brukimo (angl. *Credential stuffing*) kibernetinės atakos, kurių metu piktavaliai, pasinaudojus nutekėjusiais duomenimis (pvz. prisijungimo duomenimis), bandė prisijungti prie svetainėse esančių vartotojų paskyrų.

2024 m. I pusm. ADSP metu išryškėjo prieigos kontrolės valdymo organizacijų kompiuterių tinkluose spragos, kai suteikiant prieigą nėra taikomi apribojimai ir tinklo segmentavimas,

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 įvykus duomenų užšifravimo ir išpirkos reikalavimo atakoms, piktavaliai dažnai pašalina duomenų atsargines kopijas ir įvykių žurnalinius įrašus, kurie buvo saugomi toje pačioje vietoje, kaip ir užšifruoti duomenys, dėl to duomenų valdytojai nebegali lengvai atstatyti duomenų prieinamumo bei tinkamai atlikti kibernetinio incidento ir ADSP tyrimo.



Duomenų saugos valdymo spragos, dėl kurių įvyko kibernetiniai incidentai:

- nevykdoma kompiuterių tinklų duomenų srautų stebėsena, nevykdomas įsilaužimų aptikimas ir prevencija;
- nevaldomas veiklos tęstinumas;
- netinkami serverio nustatymai ir taisyklės;
- nevykdoma prieigos kontrolė;
- naršyklėse saugojami prisijungimo duomenys;
- skirtingoms paskyroms naudojami vienodi slaptažodžiai;
- kelių faktorių autentifikavimo nebuvimas;
- nepakankamai apmokytas personalas;
- pasenusios programinės įrangos naudojimas.

Papildomai atkreiptinas dėmesys, kad net 29 proc. visų 2024 m. I pusm. gautų pranešimų apie ADSP (dėl kibernetinių incidentų atvejų), nebuvo nustatytos incidento priežastys. Šis rodiklis rodo, kad beveik trečdalis duomenų valdytojų negebėjo tinkamai atlikti kibernetinio incidento tyrimo ir nustatyti priežastis, kurių išaiškinimas galėtų ateityje padėti išvengti tokio pobūdžio atakų.

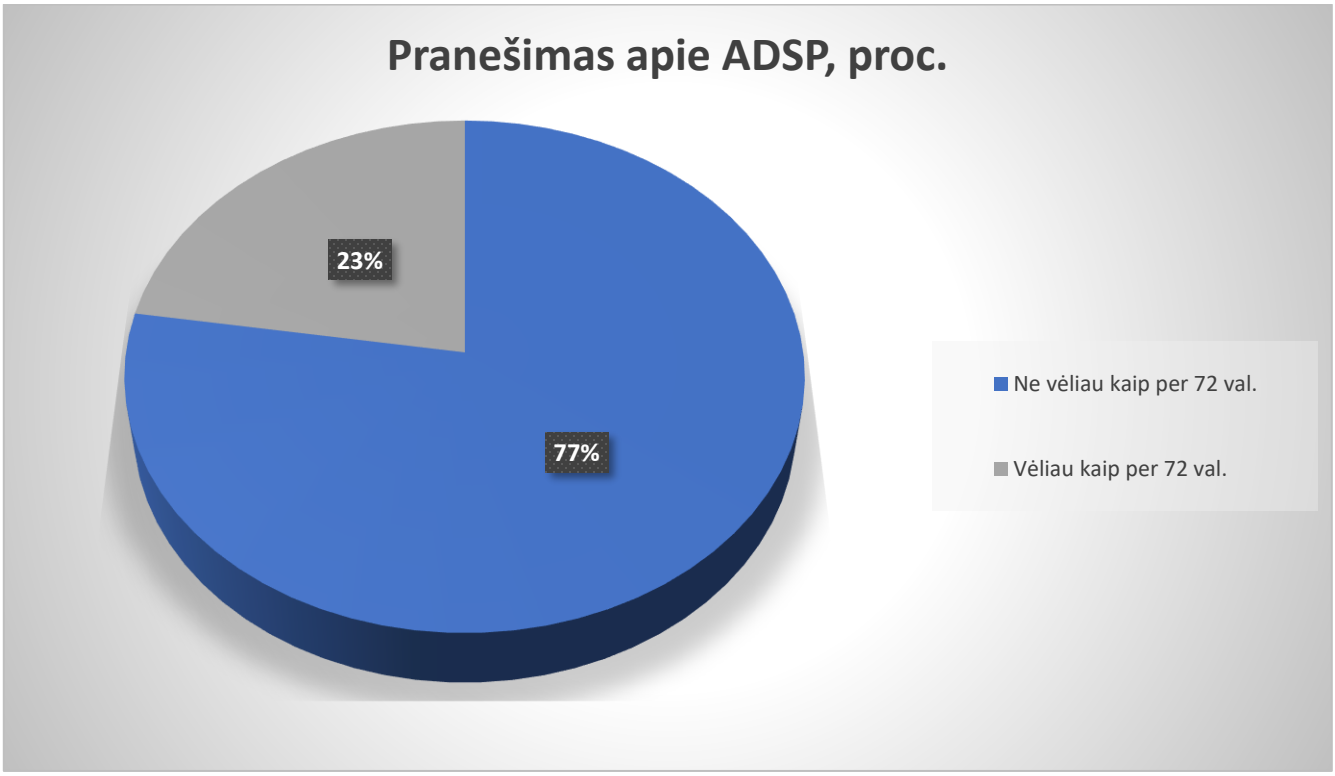
Organizacinės ir techninės saugumo priemonės, padedančios išvengti kibernetinių incidentų:

- Periodiškai daryti pilnas ir dalines atsargines duomenų kopijas (angl. *Backup*) ir saugoti jas geografiškai skirtingose vietose;
- Užtikrinti žurnalinių įrašų rinkimą ir stebėsenos vykdymą, taip pat užtikrinti, kad sistemų žurnaliniai įrašai incidento metu nebūtų ištrinti, pakeisti ar sugadinti;
- Užtikrinti periodinį kritinių operacinių sistemos saugos atnaujinimų diegimą;
- 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*);
- Turimuose įrenginiuose įsidiegti pažangią antivirusinę programinę įrangą;
- 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);
- Apriboti asmeninių įrenginių darbo funkcijoms naudojimą;
- 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.

Pranešimų apie ADSP teikimas priežiūros institucijai

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

2024 m. I pusm. 77 proc. duomenų valdytojų apie įvykusį ADSP pranešė ne vėliau kaip per 72 val., 23 proc. – vėliau kaip per 72 val.



Išanalizavus ADSP pranešimus, kurie pateikti vėliau nei per 72 val. nuo sužinojimo apie ADSP momento, atkreiptinas dėmesys, 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.

Reikšmingesni 2024 m. I pusm. ADSP Lietuvoje

2024 m. I pusm. vertinant pranešimus apie ADSP, pastebima, kad šį pusmetį buvo vykdomos kredencialų brukimo (angl. *Credential stuffing attack*) kibernetinės atakos, kurių metu yra pasinaudojama tamsiajame internete (angl. *Darknet*) ar kitoje vietoje paviešintais prisijungimais prie įvairiose svetainėse esančių vartotojų paskyrų. Piktavaliai, turėdami atskleistus vienos svetainės naudotojų prisijungimo duomenis, bando patikrinti, ar įmanoma turimais prisijungimais prisijungti prie įvairių paskyrų (pvz., el. parduotuvių paskyrų ar kt.). Papildomai pažymėtina, kad duomenų valdytojui pastebėjus, kad yra bandoma neautorizuotai prisijungti prie naudotojų paskyrų, kyla pareiga nustatyti, ar piktavaliui turimais prisijungimais pavyko faktiškai pasinaudoti. Jei nustatoma, kad prisijungimais nebuvo faktiškai pasinaudota, laikytina, kad ADSP neįvyko ir VDAI pranešti

nereikia[2]. Neautorizuotas prisijungimas prie naudotojų paskyrų yra viena iš dažniausių kibernetinio saugumo problemų. Siekiant išvengti šios atakos, naudojamos skirtingos jos aptikimo priemonės: kelių veiksnių autentifikacija (2FA/MFA), įtartinos veiklos stebėjimas, automatinis IP adresų tikrinimas, slaptažodžių politika, biometrinis autentifikavimas, tinklo saugumo įrankiai (IDS/IPS), žurnalinių įrašų analizė (angl. *Log Monitoring*). Atkreiptinas dėmesys, kad paskyroms būtina naudoti skirtingus slaptažodžius. Be kita ko, rekomenduojama juos reguliariai keisti, privalomą slaptažodžių keitimą esant poreikiui turi nustatyti pats duomenų valdytojas.

Taip pat pastebima, kad padaugėjo kibernetinių incidentų, kurie įvyksta dėl naršyklėse išsaugomų prisijungimų duomenų, tarp jų ir naudotojų privilegijuotas teises turinčių prisijungimo duomenų. Piktavaliai, įsilaužę į darbuotojo kompiuterinę darbo vietą ir perėmę naršyklėse išsaugotus prisijungimus, gauna ne tik prisijungimo duomenis, bet ir informaciją kur juos gali panaudoti. Vertinant ADSP pranešimus, pastebima, kad piktavaliui pasinaudojus perimtais prisijungimais, jis prisijungia prie sistemų, kuriose yra saugomi asmens duomenys, jau turėdamas sistemos administratoriaus teises, toliau seka duomenų užšifravimo ir išpirkos reikalavimo atakos, kurių metu užšifruojami serveriai ir kitos sistemos, taip pat reikalaujama išpirkos už duomenų iššifravimą bei grasinama nusikopijuotus asmens duomenis paskelbti tamsiajame internete (angl. *Darknet*).

Pasitaikančios klaidos įvykus ADSP

Įvertinus 2024 m. I pusm. gautus pranešimus apie ADSP, pastebima, kad pasitaiko atvejų, kai duomenų tvarkytojas įvykus ADSP delsia informuoti duomenų valdytoją, nors BDAR 33 straipsnio 2 dalyje yra įtvirtinta pareiga duomenų tvarkytojui, sužinojus apie ADSP, nepagrįstai nedelsiant apie tai informuoti duomenų valdytoją. Ši pareiga užtikrina, kad duomenų valdytojas nedelsiant sužinotų apie įvykusį ADSP ir galėtų imtis taisomųjų veiksmų. Duomenų tvarkytojui delsiant informuoti duomenų valdytoją kyla rizika, kad dėl laiku nesiimamų tinkamų priemonių, duomenų subjektams gali kilti didesnis pavojus.

Taip pat pasitaiko, kad VDAI, susipažinusi su ADSP pranešimų turiniu, nustato, kad pavojus fizinio asmens teisėms ir laisvėms dėl įvykusio ADSP yra vertintas formaliai, t. y. nurodoma, kad pavojus kilo arba nekilo, tačiau nepateikiama argumentacija, dėl kokių priežasčių daromos tokios išvados. Taip pat pastebima, kad duomenų valdytojai, netinkamai atlikę pavojaus fizinių asmenų teisėms ir laisvėms vertinimą, nustato, kad duomenų subjektams didelis pavojus dėl įvykusio ADSP nekyla (atitinkamai duomenų subjektai neinformuojami), nors atsižvelgiant į ADSP pobūdį, specifiką ir rimtumą, toks pavojus fiziniams asmenims visgi yra. Netinkamo pavojaus fizinių asmenų teisėms ir laisvėms vertinimo atlikimas kelia riziką, kad duomenų valdytojas nesiims tinkamų taisomųjų priemonių, o duomenų subjekto neinformavimas užkerta kelią pačiam duomenų subjektui imtis reikiamų priemonių pavojaus dėl įvykusio ADSP rizikoms sumažinti.

[2] https://vdai.lrv.lt/lt/naujienos/vdai-pataria-del-pasitaikanciu-atveju-kai-pranesama-apie-ivykusius-incidentus-kurie-nera-laikomi-asmens-duomenu-saugumo-pazeidimais/

VDAI atkreipia dėmesį, kad įvykus ADSP ir atliekant pavojaus fizinių asmenų teisėms ir laisvėms vertinimą, duomenų valdytojas turėtų vadovautis BDAR preambulės 75 konstatuojamąja dalimi, rekomendacija[3] bei gairėmis[4].

_____

[3] VDAI 2018 m. liepos 2 d. rekomendacija dėl asmens duomenų saugumo pažeidimų nustatymo, tyrimo, pranešimo apie juos ir dokumentavimo tvarkos.

[4] 2017 m. spalio 3 d. 29 straipsnio duomenų apsaugos darbo grupės gairės dėl pranešimo apie asmens duomenų saugumo pažeidimą pagal Reglamentą (ES) 2016/679 (nauja redakcija nuo 2023 m. kovo 28 d.) bei 2021 m. gruodžio 14 d. Europos duomenų apsaugos valdybos gairės 01/2014 dėl pranešimo apie asmens duomenų saugumo pažeidimą pavyzdžių.