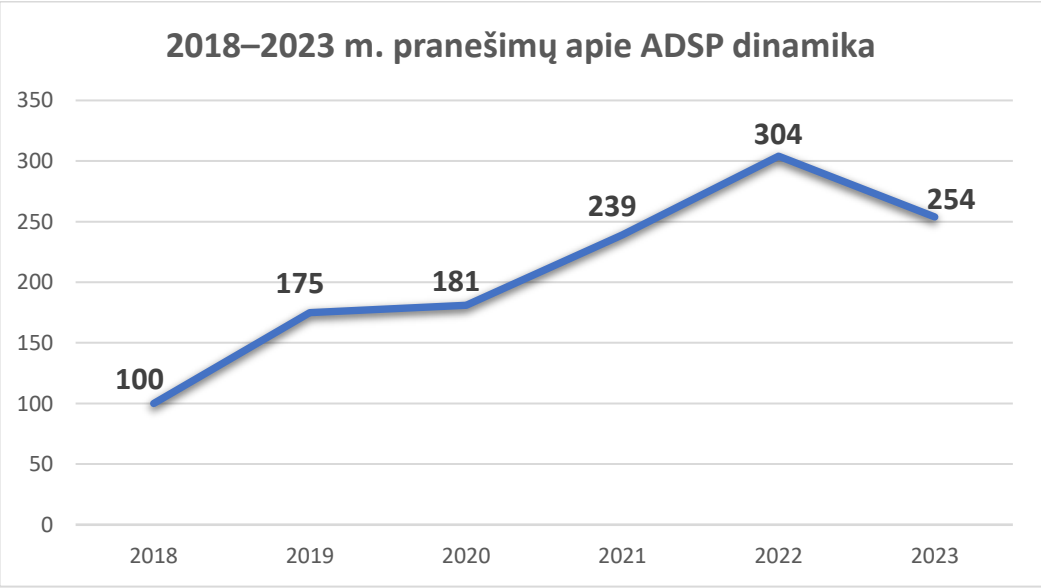
ASMENS DUOMENŲ SAUGUMO PAŽEIDIMAI LIETUVOJE 2023 M.

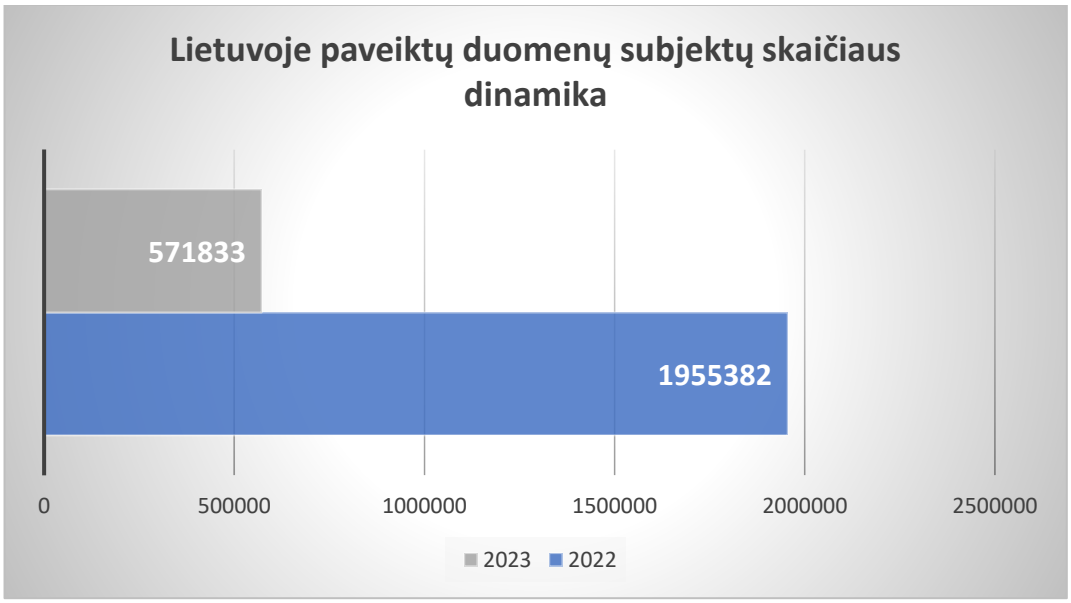
Asmens duomenų saugumo pažeidimas (toliau – ADSP) – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga (Bendrojo duomenų apsaugos reglamento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

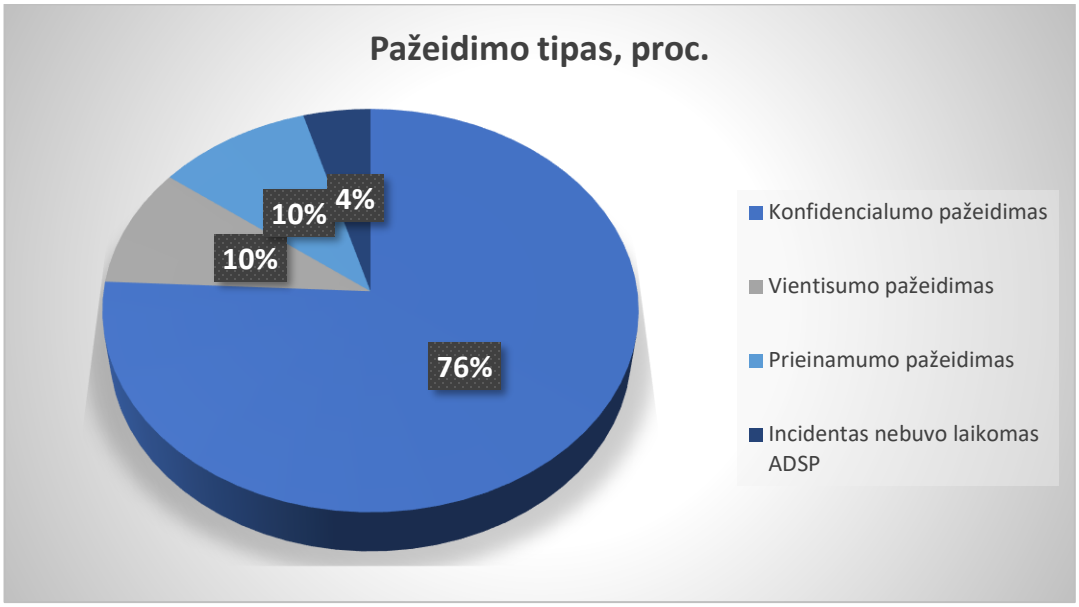
VDAI apie ADSP privalo pranešti visi duomenų valdytojai pateikdami pranešimą apie ADSP, išskyrus, kai tikėtina, kad toks ADSP nekels pavojaus asmenų teisėms ir laisvėms. Kai dėl ADSP pobūdžio ir rizikos rimtumo kyla didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas apie ADSP privalo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

Apžvelgiant 2023 m. pranešimų apie ADSP Lietuvoje statistiką, VDAI buvo gauti 254 pranešimai apie ADSP, Lietuvoje paveiktų duomenų subjektų skaičius – 571 833. Palyginti su ankstesnių metų duomenimis, VDAI gavo mažiau pranešimų apie ADSP negu 2022 m. (2022 m. VDAI gautų pranešimų apie ADSP – 304), taip pat Lietuvoje paveiktų duomenų subjektų skaičius sumažėjo daugiau negu 3 kartus (2022 m. Lietuvoje paveiktų duomenų subjektų skaičius – 1 955 382).

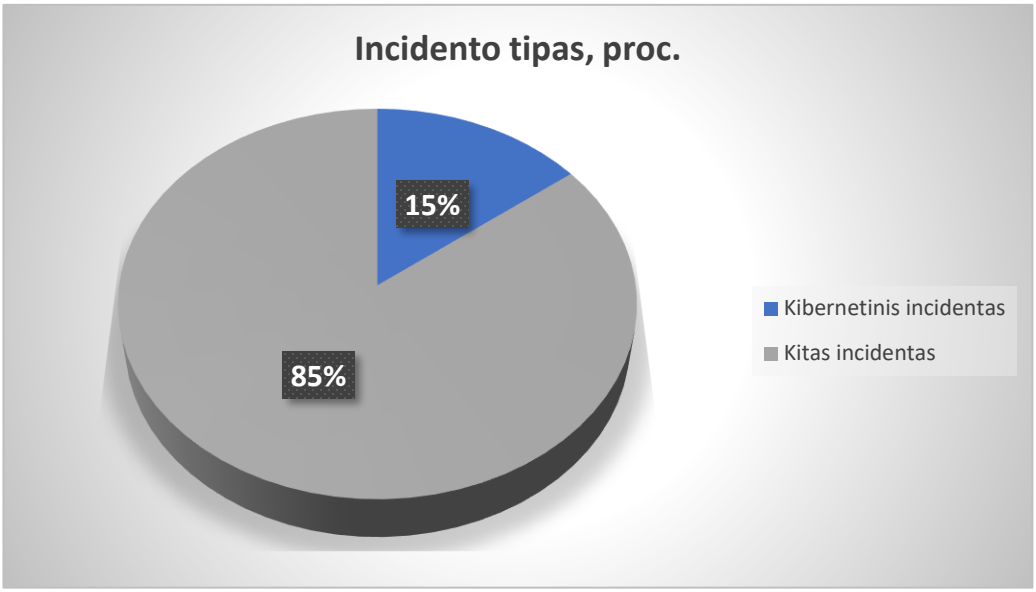




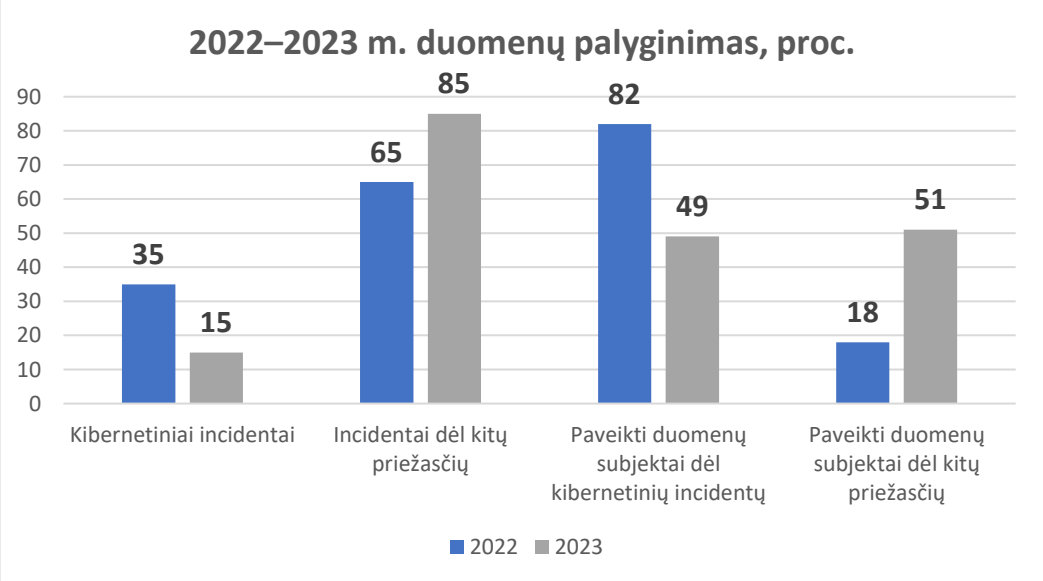
Pagal ADSP pobūdį Lietuvoje statistiškai vyrauja konfidencialumo pažeidimai, kurių skaičius per 2023 m. sudarė net 76 proc. visų atvejų, 10 proc. atvejų vientisumo pažeidimai, 10 proc. atvejų prieinamumo pažeidimai ir 4 proc. atvejų incidentas nebuvo laikomas ADSP (neatitiko sąvokos).



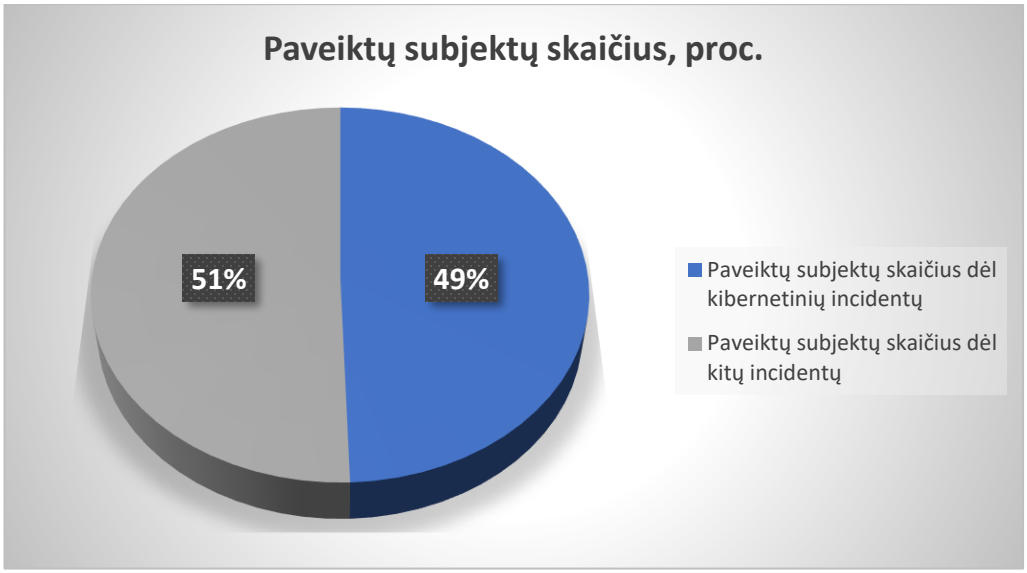
VDAI, išanalizavusi per 2023 m. gautus pranešimus apie ADSP nustatė, kad 85 proc. ADSP įvyko dėl įvairių priežasčių (žmogiškosios klaidos, IT sistemų trikdžių ir kt.), 15 proc. ADSP įvyko dėl kibernetinių incidentų (duomenų užšifravimo, išpirkos reikalavimo, socialinės inžinerijos, duomenų viliojimo atakų ir kt.).



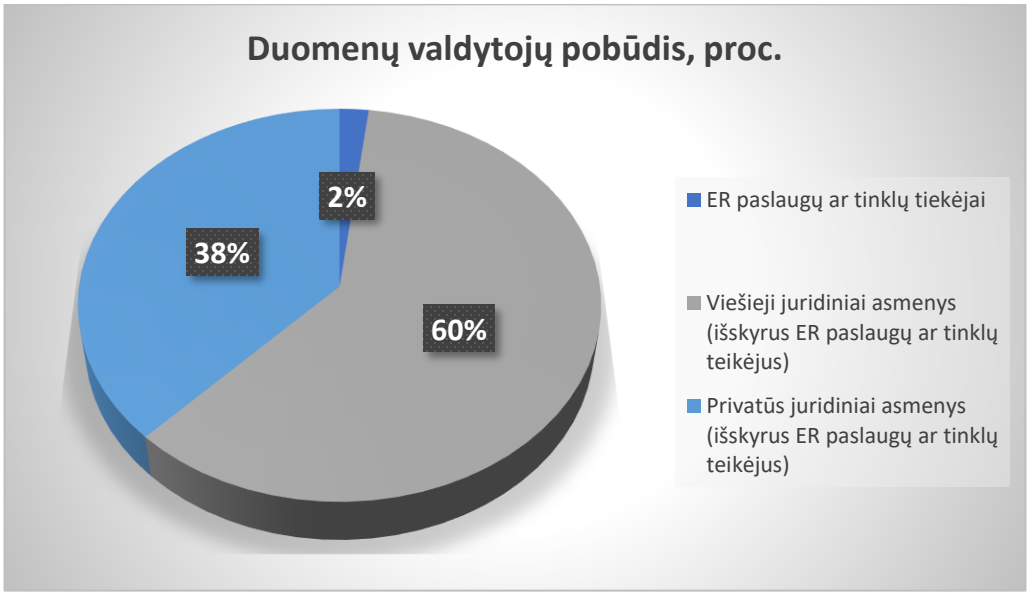
Palyginti su praėjusių metų duomenimis, pastebima, kad įvykusių ADSP dėl kibernetinio incidento yra mažiau negu 2022 m. (2022 m. dėl kibernetinio incidento įvykę ADSP – 35 proc., o įvykusių dėl kitų priežasčių – 65 proc.).

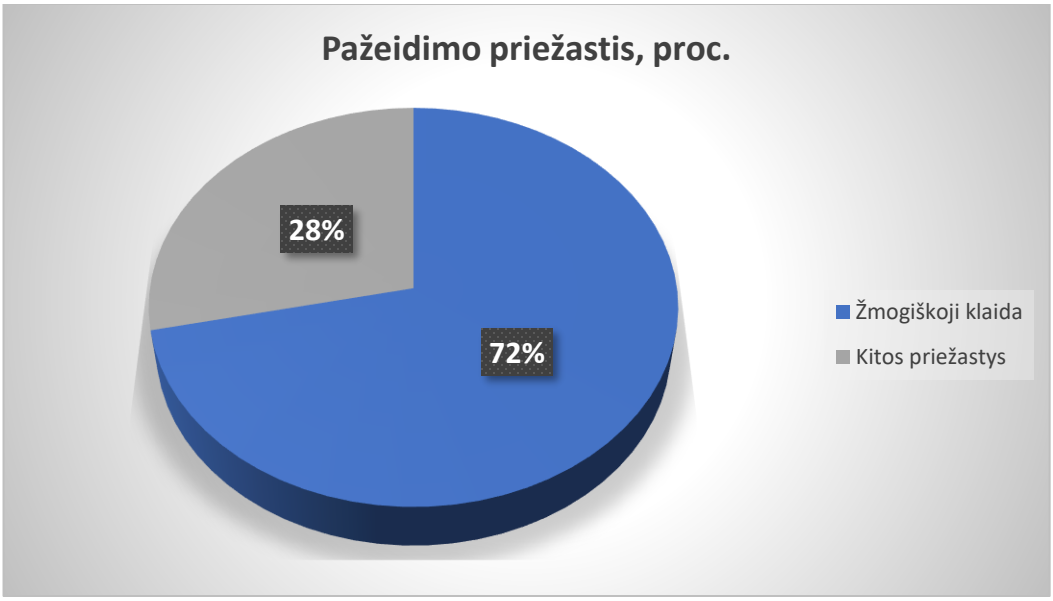


Svarbu paminėti, kad nors kibernetiniai incidentai sudarė tik 15 proc. visų 2023 m. įvykusių ADSP, bet jų metu buvo paveikti 49 proc. (iš visų 2023 m. paveiktų subjektų) subjektų duomenys, dėl kitų priežasčių buvo paveikti 51 proc. subjektų duomenys. Palyginti su praėjusių metų duomenimis, pastebima, kad dėl 2022 m. įvykusių kibernetinių incidentų buvo paveikta 82 proc. duomenų subjektų (iš visų 2022 m. paveiktų duomenų subjektų skaičiaus), o dėl kitų priežasčių buvo paveikta 18 proc. duomenų subjektų.



2023 m., kaip ir kasmet, daugiausia ADSP pranešimų buvo gaunama iš viešųjų juridinių asmenų – 60 proc., iš privačių juridinių asmenų – 38 proc. ir 2 proc. pranešimų – iš elektroninių ryšių paslaugų teikėjų.





Palyginti su praėjusių metų duomenimis, ADSP įvykusių dėl žmogiškosios klaidos daugėja. 2023 m. 72 proc. ADSP įvyko dėl žmogiškosios klaidos (2022 m. tokių ADSP buvo 60 proc.). 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 kitiems gavėjams, netinkamai nuasmeninto dokumento paviešinimas ir kt.. Dėl kitų priežasčių įvykę ADSP sudaro 28 proc. (2022 m. 40 proc.). Tai buvo įvairūs kibernetiniai incidentai, IT sistemų trikdžiai ir kt., pavyzdžiui, piktavaliui pasinaudojus sistemų pažeidžiamumu ir įsilaužus į serverį, jame esantys duomenys yra užšifruojami, dėl IT sistemos klaidos atnaujinti duomenys nebuvo laiku perduodami, dėl to duomenų valdytojas negalėjo laiku suteikti paslaugų ir kt.

VDAI, atsižvelgdama į tai, kad ADSP vis dažniau įvyksta dėl žmogiškosios klaidos, atkreipia dėmesį, kad labai svarbi priemonė minimizuojant žmogiškąsias klaidas ir siekiant išvengti kibernetinių incidentų (duomenų viliojimo atakų ir kt.) yra **darbuotojų mokymai**. Mokymai apie duomenų apsaugą ir saugumo procedūras (pvz., slaptažodžių naudojimą ir prieigą prie konkrečių IT sistemų) ir įvairios duomenų viliojimo metodais paremtų atakų simuliacijos yra svarbūs tinkamam organizacinių ir techninių saugumo priemonių įgyvendinimui ir prevencijai dėl netyčinio duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų (BDAR 32 straipsnio 2 dalis). Žinios apie asmens duomenų tvarkymui keliamus reikalavimus bei atsakomybes yra ypač svarbios tiems asmenims, kurie

atlieka didelės rizikos asmens duomenų tvarkymo operacijas, pavyzdžiui, specialiųjų kategorijų duomenų tvarkymą.

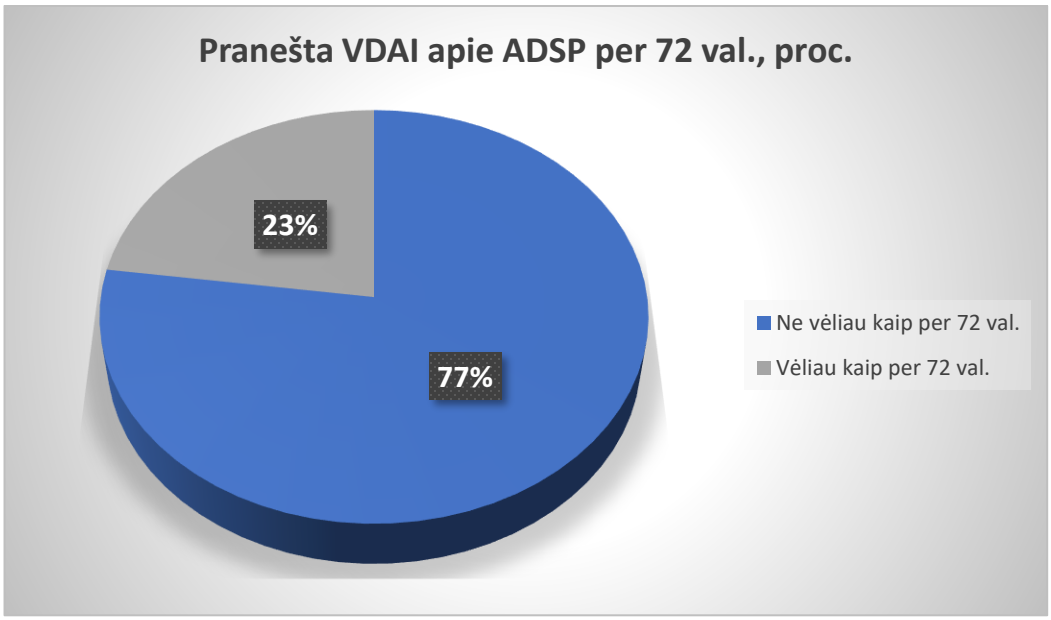
2023 m. buvo gauta 12 pranešimų apie ADSP, kurių metu vyko duomenų užšifravimo ir išpirkos reikalavimo atakos (angl. *Ransomware*).

ADSP metu piktavaliai naudojo įvairius socialinės inžinerijos ir duomenų viliojimo (angl. *Phishing*) metodus, siekdami išvilioti įvairiausius prisijungimų duomenis, pasitelkdami gerai apgalvotus scenarijus. Taip pat buvo vykdomos prisijungimo duomenų užpildymo (angl. *Credential stuffing*) kibernetinės atakos, kurių metu piktavaliai, pasinaudojus nutekėjusiais duomenimis (pvz., prisijungimo duomenimis), bandė prisijungti prie kitiems asmenims priklausančių paskyrų. 2023 m. ADSP metu buvo pastebėtos ir DDoS (angl. *Distributed Denial of Service*) paskirstytos paslaugos atkirtimo atakos. Didėjo naudojamos programinės ir techninės įrangos gamintojų ar debesijos paslaugų tiekėjų patikimumo, reputacijos ir kilmės šalies įvertinimo ir potencialių rizikų duomenų saugumui nustatymo svarba.

2023 m. 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 ir tinkamai atlikti kibernetinio incidento ir ADSP tyrimo.

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, turėtų pranešti apie tai VDAI, kaip tai numato BDAR.

2023 m. 77 proc. duomenų valdytojų apie įvykusį ADSP pranešė ne vėliau kaip per 72 val., 23 proc. – vėliau kaip per 72 val.



VDAI, išanalizavusi ADSP pranešimus, kurie pateikiami vėliau kaip per 72 val. nuo sužinojimo apie ADSP momento, atkreipia dėmesį, kad duomenų valdytojai dažnai 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. Atsižvelgiant į tai, 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 2023 m. ADSP Lietuvoje

Duomenų valdytojai pranešė apie įvykdytas duomenų užšifravimo ir išpirkos reikalavimo atakas, kurių metu buvo ne tik užšifruoti serveriai, buhalterinės programos ir kitos sistemos, bet prieš juos užšifruojant, juose esantys duomenys buvo piktavalių nukopijuoti, dėl ko įsilaužėliai reikalavo išpirkos už duomenų dešifravimą bei pateikė grasinančius pranešimus, nukopijuotus asmens duomenis paskelbti tamsiajame internete (angl. *Darknet*). VDAI dėl šių rezonansinių ADSP pradėjo tyrimus savo iniciatyva.

Baudos

2023 m. kovo mėn. VDAI, atlikusi ADSP tyrimą, priėmė sprendimą paslaugų teikimo bendrovei skirti 20 tūkst. eurų baudą už nustatytus BDAR nuostatų pažeidimus. Per incidentą buvo pažeistas apie 55 tūkst. duomenų subjektų (vartotojų) asmens duomenų konfidencialumas. VDAI nustatė, kad dėl netinkamai vykdomos prieigų kontrolės ir autentifikavimo buvo prisijungta prie bendrovės duomenų bazės ir nutekinti bendrovės klientų duomenys.

2023 m. kovo mėn. VDAI, atlikusi ADSP tyrimą, priėmė sprendimą viešojo sektoriaus įstaigai skirti 6 600 eurų baudą už nustatytus BDAR nuostatų pažeidimus. Per incidentą buvo pažeistas 13 525 duomenų subjektų (vartotojų) asmens duomenų konfidencialumas. VDAI nustatė, kad dėl neatnaujinamos programinės įrangos ir galimybės prie valdymo panelės prisijungti iš išorinio tinklo, nenaudojant kelių lygių autentifikacijos, sukčiai prisijungė prie interneto svetainės, nusikopijavo vartotojų duomenų bazę ir paskelbė ją tamsiajame internete.

Duomenų saugos valdymo spragos, dėl kurių įvyko kibernetiniai incidentai 2023 metais

Kibernetinio saugumo spragos, dėl kurių įvyko kibernetiniai incidentai 2023 metais	Organizacinės ir techninės saugumo priemonės, padedančios išvengti panašių pažeidimų
Kibernetinio saugumo pažeidimai	
Darbuotojai nėra reguliariai mokomi apie kibernetinį saugumą ir asmens duomenų saugumą.	Reguliariai mokyti darbuotojus apie kibernetinį saugumą, IT sistemų saugumo reikalavimus ir asmens duomenų apsaugą; Įdiegti el. pašto filtravimo mechanizmus, gebančius filtruoti laiškus pagal žinomus grėsmių indikatorius ir specifinius raktažodžius; Reguliariai organizuoti duomenų viliojimo metodais paremtų atakų simuliacijas; Parengti ir reguliariai testuoti veiklos tęstinumo planą.
Darbuotojai, komunikacijos priemonėmis gavę kenkėjiškus laiškus, negeba jų kritiškai vertinti.	
Darbuotojai, paspausdami kenkėjiškose žinutėse esančias nuorodas, atsidarę prie laiško pridėtus kenksmingus priedus, neatsargiai elgiasi (suveda turimų paskyrų prisijungimus).	
Ypač pavojinga, kai darbuotojas su administratoriaus prieiga įrašo kenksmingą programą į savo kompiuterinę darbo vietą.	
Prieigų kontrolės ir autentifikavimo pažeidimai	
IT administratoriams išėjus iš darbo, nėra panaikinamos administratoriaus prieigos.	IT administratoriams išėjus iš darbo ar pasikeitus paslaugos teikėjui, nedelsiant panaikinti visas prieigas; Užtikrinti sistemų pirminių slaptažodžių pakeitimą; Įdiegti prieigos kontrolę pagal organizacijos saugumo politiką, taikant „mažiausių teisių privilegijos“ ir „būtina žinoti“ principus; Nenaudoti tų pačių slaptažodžių skirtingoms paskyroms, naudoti kelių faktorių autentifikavimą (el. pašto internetinei prieigai, VPN prieigai, paskyroms, kurios turi prieigą prie kritiškai svarbių sistemų).
IT administratoriaus prieigomis nuolat naudojasi kiti darbuotojai (nėra priskirtos ribotam darbuotojų skaičiui).	
Naudojamos bendros vartotojų paskyros.	
Paskyrų slaptažodžiai nėra kompleksiški.	
Paliekami pirminiai sistemų prisijungimai.	
IT administratorių prieigoms nėra naudojami kelių faktorių autentifikavimo metodai.	
Pažeidimai susiję su netinkamais serverio nustatymais ir taisyklėmis	
Paveiktuose serveriuose buvo saugomi pertekliniai asmens duomenys.	Užtikrinti, kad tvarkomi asmens duomenys atitiktų duomenų tvarkymo tikslus; Šifruoti saugomus specialių kategorijų asmens duomenis. Nenaudoti gamyklinių serverių nustatymų.
Specialių kategorijų asmens duomenys saugomi nešifruoti.	
Naudojami gamykliniai serverių nustatymai.	
Pažeidimai susiję su operacinių sistemų ar antivirusinių programų pažeidžiamumais	
Naudojamos nebepalaikomos operacinės sistemos.	

Operacinių sistemų saugos atnaujinimai yra atliekami nereguliariai.	Turimuose įrenginiuose įsidiegti pažangią antivirusinę programinę įrangą; Užtikrinti kritinių operacinių sistemos saugos atnaujinimų diegimą reguliariai ir nedelsiant; Reguliariai daryti pilnas ir dalines atsargines kopijas (angl. Backup), itin svarbius duomenis, kurių praradimas sukeltų didelius nuostolius, rekomenduojama saugiai laikyti bent dvejose atskirose laikmenose.
Antivirusinės programų versijos yra neatnaujinamos arba pažeidimo metu jos yra išjungiamos.	
Pažeidimai susiję su tinklo ir komunikacijos sauga	
IT sistemoms pasiekti nuotoliniu būdu yra naudojami nešifruoti komunikacijos kanalai.	Apriboti išorinio prisijungimo galimybes protokolais (angl. Windows Remote Desktop Protocol), daiktų interneto SSH prievadais ir pan.; Prie maršrutizatorių leisti jungtis tik iš žinomų IP adresų (angl. Allow List) arba prisijungimui naudoti virtualaus privataus tinklo technologijas (angl. Virtual Private Network, VPN); Tinkamai sukonfigūruoti išorinėje komunikacijoje dalyvaujančius serverius ir kitą įrangą pagal gerąsias praktikas.
IT sistemų pasiekiamumas nėra apribotas tik tam tikriems vartotojams.	
Informacinės sistemos tinklas yra neatskirtas nuo kitų duomenų valdytojų tinklų.	

Dažniausiai pasitaikančios klaidos informuojant apie įvykusį ADSP

VDAI atkreipia dėmesį, kad BDAR nustato pranešimo VDAI ir duomenų subjektui turinį.

Dėl pranešimo VDAI. Pranešant VDAI apie įvykusį ADSP dažniausiai pasitaikančios klaidos yra susijusios su tuo, kad nepakankamai išsamiai aprašomos įvykusio ADSP aplinkybės, taip pat neaprašomos priemonės, kurių ėmėsi arba ketina imtis duomenų valdytojas, kad būtų pašalintas ADSP, sumažintas pavojus duomenų subjektų teisėms ir laisvėms ir, kad ADSP ateityje nepasikartotų. Atsižvelgiant į tai, VDAI rekomenduoja naudoti VDAI patvirtintą pranešimo apie ADSP formą ir pildant pranešimą pateikti išsamią informaciją apie įvykusį ADSP.

Taip pat VDAI, susipažinusi su ADSP pranešimų turiniu, dažnai nustato, kad pavojus asmens teisėms ir laisvėms dėl įvykusio ADSP yra vertintas formaliai, t. y. nurodoma, kad pavojus kilo arba nekilo, tačiau nepateikiant argumentacijos, dėl kokių priežasčių daromos tokios išvados. VDAI atkreipia dėmesį, kad įvykus ADSP ir atliekant pavojaus duomenų subjektų teisėms ir

laisvėms vertinimą, duomenų valdytojas turėtų vadovautis BDAR preambulės konstatuojamąja dalimi, rekomendacija[1] bei gairėmis[2].

ADSP, keliantys didelį pavojų duomenų subjektų teisėms ir laisvėms

VDAI nuomone, ADSP, keliantys didelį pavojų duomenų subjektų teisėms ir laisvėms, yra atvejai, kai dėl įvykusio ADSP gali įvykti tapatybės vagystė, duomenų subjektui gali kilti materialinės ar nematerialinės žalos grėsmė (sveikatos duomenų atskleidimas, asmens dokumentų kopijų praradimas ar finansinių duomenų praradimas), konfidencialumo pažeidimas, kai atkleidžiama medicininė informacija šalims, kurios neturi teisės gauti tokios informacijos ir dėl to atitinkamai kyla pasekmės.

Pavyzdžiui, 2023 m. duomenų valdytojui „X“ įvyko ADSP, kai informacija apie duomenų subjektų apsilankymus pas psichiatrą ir diagnozes buvo paskelbta viešai. Dėl tokio pobūdžio ADSP gali kilti didelis pavojus duomenų subjektų teisėms ir laisvėms, nes tokios informacijos viešas paskelbimas gali turėti tiesioginės neigiamos įtakos asmeniui (darbinei veiklai, socialiniam gyvenimui).

Taip pat, kai duomenų valdytojo naudojami serveriai, kuriuose laikomi nešifruoti asmens duomenys yra užšifruojami, kyla pavojus duomenų subjektams. Jeigu nėra atsarginių kopijų ir negalima atkurti saugotų asmens duomenų, šie duomenys gali turėti tiesioginę įtaką duomenų subjekto materialinei padėčiai (pvz., dėl neišmokamų išmokų) arba šis ADSP įvyksta ligoninėje, atitinkamai pažeistų duomenų ir nukentėjusių duomenų subjektų daug, nes ligoninės paprastai tvarko didelį kiekį sveikatos duomenų. Be to, išlieka pavojus dėl rimtų su pacientų duomenų konfidencialumu susijusių padarinių. Todėl tokiu atveju, nors būtų padaryta atsarginė duomenų kopija ir duomenis būtų galima atkurti per kelias dienas, pavojus duomenų subjektų teisėms ir laisvėms išlieka didelis.

Dėl duomenų subjektų informavimo. VDAI atkreipia dėmesį, kad dažniausiai pasitaiko šios klaidos:

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

[2] 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.

Nėra nurodoma, kokių veiksmų pats duomenų subjektas gali imtis, kad sumažintų ADSP pasekmes (pavyzdžiui, blokuotų kredito kortelę ir pan.).

Nenurodomi duomenų apsaugos pareigūno arba kito kontaktinio asmens, galinčio suteikti daugiau informacijos, duomenys. Atkreiptinas dėmesys į tai, kad BDAR nustatyta, kad pranešime duomenų subjektui be kontaktinių duomenų privalo būti pateiktas ir kontaktinio asmens vardas bei pavardė.

Informacija apie įvykusį ADSP duomenų subjektui pateikiama sudėtinga kalba, naudojant sudėtingus terminus ir pan. VDAI pažymi, kad teikiant pranešimą duomenų subjektui, informacija turi būti pateikiama aiškia ir paprasta kalba, kad duomenų subjektas suprastų esminę informaciją, susijusią su įvykusiu ADSP.