KIBERNETINIS SAUGUMAS

ATMINTINĖ

Asmens duomenų saugumo pažeidimai dažnai glaudžiai susiję su kibernetiniais incidentais ir nusikaltimais.

Asmens duomenų saugumo pažeidimas (toliau – ADSP) sudaro sąlygas piktavaliams perimti asmens duomenis, kurie gali būti panaudojami kibernetiniams incidentams ir nusikaltimams vykdyti. 2020 m. Lietuvoje reikšmingiausi pagal paveiktų asmenų skaičių ir poveikį ADSP buvo susiję su informacinės visuomenės paslaugų ir duomenų pasiekiamumo prieinamumo trikdžiais bei vientisumo pažeidimais (pvz., 2020 m. liepos mėn. įvykęs e. sveikatos sistemos sutrikimas) bei su atvejais, kai, taikant socialinės inžinerijos metodus ir nesant kibernetinio saugumo higienos, buvo užvaldomos naudotojų paskyros siekiant finansinės naudos (pvz., 2020 m. kovo mėn. UAB „Vinted“ el. prekybos platformoje buvo prisijungta prie naudotojų paskyrų be jų žinios), taip pat platinant kenkimo programinę įrangą (toliau – PĮ). Ir nors per 2020 m. Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) gautų pranešimų apie ASDP skaičius nelabai (3,5 proc.) padidėjo, galima daryti prielaidą, kad apie nemažą dalį ADSP VDAI vis dar nėra informuojama, nes gana dažnai ADSP būna susiję su įvykusiais kibernetiniais incidentais, kurių skaičius kasmet auga. 2020 m. Lietuvoje daugeliu atvejų buvo prarastas asmens duomenų konfidencialumas, todėl kibernetinio saugumo priemonių taikymas ir jų laikymasis asmens duomenų apsaugos srityje yra viena iš ADSP prevencijos sąlygų.

Žemiau pateikiamos **Nacionalinio kibernetinio saugumo centro rekomendacijos kibernetinių incidentų prevencijai**:

Rizika	Rekomendacija
 **Naudotojas paspaus nuorodą į interneto svetainę, užkrėstą kenkimo kodu**	Užvesti pelės žymeklį ant nuorodos ir patikrinti, ar rodomas interneto svetainės adresas yra tikras, įsitikinti, kad adrese nėra įvelta gramatinių klaidų, adreso pavadinimas logiškas ir lengvai perskaitomas.
 **Naudotojas įves savo slaptažodį suklastotoje interneto svetainėje**	Įsitikinti, kad sesija su interneto svetaine yra šifruojama, t. y. naudojamas TLS sertifikatas (interneto svetainės adresas turi prasidėti „https“ žyma), naudoti kelių žingsnių autentifikavimo įrankius (pvz., slaptažodis, mobilusis įrenginys, pirštoantspaudas). Stengtis bankų, socialinių tinklų, el. pašto adresus suvesti naršyklėje patiems, išsisaugoti šių adresų nuorodas naršyklėje.
 **Naudotojas pats atskleis savo prisijungimo slaptažodžius piktavaliui**	Naudoti mažiausiai dviejų žingsnių autentifikavimą (angl. *2-factor-authentification* (2FA)), saugoti savo prisijungimo slaptažodžius, jokiais būdais nelaikyti jų atviru tekstu darbo vietoje, kompiuteryje ar mobiliajame telefone. Kritiškai vertinti reklamas internete ir elektroniniu paštu siunčiamuose laiškuose (ypač siūlomas dideles nuolaidas). Prašymus atlikti pinigines perlaidas tikrinti kitais būdais, pvz., pasitikslinti aplinkybes paskambinus telefonu.

Naudotojas įdiegs kenkimo PĮ	Neatidarinėti dokumentų turinio, siunčiamų failų ir PĮ, kurie yra atsiųsti ar parsisiųsti iš nepatikimo šaltinio (pvz., iš nelegalių PĮ platinimo šaltinių).
Naudotojas pasiduos piktavalio manipuliacijoms	Neatlikti skubotų veiksmų, nepasiduoti emocijoms, detaliai išsiaiškinti veiksmų, kuriuos prašoma atlikti, būtinumą.
Pasinaudojęs pažeidžiamumu, piktavalis įdiegs kenkimo PĮ į RIS	Naudoti legalią OS ir PĮ, naudoti antivirusinę PĮ, ja profilaktiškai skenuoti duomenis įrenginyje, nedelsiant įdiegti naujai išleistus OS, PĮ atnaujinimus.
Naudotojas parsisiųs kenkimo PĮ iš interneto šaltinių	Nesisiųsti failų iš nepatikimų šaltinių, naršyklėje įdiegti įskiepius suklastotoms interneto svetainėms atpažinti, parsisiųstus įtartinus failus skenuoti antivirusine PĮ, tikrinti failus dėl jų grėsmių žinomuose šaltiniuose, pvz., http://www.virustotal.com.

Kenkimo PĮ iš užkrėstos atminties laikmenos bus paleista automatiškai	Nesinaudoti nepatikimomis, nepatikrintomis atminties laikmenomis. Nuolat jas formatuoti, išjungti automatinį failų paleidimą, prieš atidarant laikmenoje esančius failus leisti antivirusinei PĮ nuskenuoti juos.
Kenkimo PĮ užšifruos kompiuteryje esančius duomenis	Periodiškai daryti atsargines duomenų kopijas, jas saugoti kitame įrenginyje, atskirai nuo tos vietos, kurioje jos buvo padarytos. Svarbią informaciją laikyti atskiroje laikmenoje ar laikmenose, neturinčiose tiesioginės sąsajos su internetu (pvz., išorinėje laikmenoje).
Kenkimo PĮ sukurs piktavaliui prieigą prie konfidencialios informacijos	Šifruoti konfidencialią informaciją, jeigu būtina, apsaugoti ją saugiu slaptažodžiu. Informacijai perduoti naudoti kriptografines priemones, pvz., elektroninių laiškų šifravimą.
Kompiuteris bus užkrėstas per RIS tinklą	Įstaigose naudoti tinklo segmentavimą, keletą filtravimo priemonių (pvz., tinklo ir darbo stoties ugniasienę), svarbias RIS atskirti fiziškai.

Nacionalinio kibernetinio saugumo centro rekomendacijos kibernetinių įvykių prevencijai:

- Rekomenduotina pramoninių valdymo sistemų saugumą užtikrinti šias sistemas izoliuojant atskiruose tinkluose, o jų išorinį pasiekiamumą apriboti ir kontroliuoti. Esant išorinio pasiekiamumo būtinybei, nuotolinę prieigą suteikti tik personalui iš konkrečių dedikuotų IP adresų (angl. *allowlist*), papildomai sustiprinant autentifikavimo priemones, pritaikant dviejų žingsnių autentifikavimą ar kitus mechanizmus.
- Maršrutizatorių savininkai raginami peržiūrėti savo prietaisų nustatymus. Jeigu belaidžio tinklo slaptažodį sudaro tik skaitmenys arba skaitmenys bei didžiosios raidės nuo A iki F, o slaptažodžio ilgis tėra 8–10 simbolių, tuomet būtina pasirūpinti savo prieigos saugumu, pakeičiant slaptažodį į patikimesnį. Saugų slaptažodį turėtų sudaryti bent 12–14 simbolių iš didžiųjų ir mažųjų raidžių, skaitmenų ir specialiųjų simbolių.
- Nuolat vykdyti elementarią kibernetinės saugos higieną – laiku atnaujinti PĮ, naudojant saugius slaptažodžius, tinkamai administruoti naudotojus ir jų teises, taikyti tinkamas žurnalinių įrašų bei duomenų kopijų politikas.

Siekdama padėti sumažinti riziką patirti ADSP, VDAI pateikia patarimų, kaip sustiprinti duomenų apsaugą.

Siūlomos įgyvendinti organizacinės priemonės:

- Supraskite, kokius duomenis turite, ir juos klasifikuokite. Negali apsaugoti informacijos, jei nežinai, kur ji saugoma ar kaip naudojama, kur laikomos atsarginės kopijos ir t. t. Įsitikinkite, kad žinote, kokie duomenys jūsų organizacijoje yra kritiškai svarbūs ar jautrūs, juos būtina suklasifikuoti pagal svarbos ar kritiškumo lygį.
- Užtikrinkite fizinę dokumentų ir įrenginių su duomenimis saugą – laikykite asmens duomenis saugiai, kad niekas neturėtų prieigos be jūsų leidimo.
- Nuolat laikykitės „švaraus stalo" ir „švaraus spausdintuvo" taisyklių, jokie dokumentai su asmens duomenimis neturi likti be jūsų priežiūros.
- Būtinai nurodykite atgalinį adresą, kai siunčiate siuntas ar pašto vokus su dokumentais, kad per klaidą juos gavęs kitas asmuo galėtų grąžinti siuntą jos neatidaręs.
- Mokykite darbuotojus laikytis geriausios duomenų saugumo praktikos, paaiškinkite duomenų saugumo svarbą ir informuokite apie neskelbtinus duomenis organizacijoje. Patarkite, kaip išvengti klaidų, dėl kurių gali įvykti ADSP. Saugumas turėtų būti organizacijos kultūros dalis.

Siūlomos įgyvendinti techninės priemonės:

- Prieigai prie sistemų turi būti nustatyta aiški slaptažodžių politika. Ji gali prasidėti nuo draudimo saugoti slaptažodžius sistemose jų neužšifravus, įpareigojimo laikytis slaptažodžių simbolių kiekio, keitimo dažnumo ir kitų reikalavimų bei perspėjimo nenaudoti to paties slaptažodžio skirtingoms paslaugoms ar įrenginiams.
- Tokios grėsmės kaip išpirkos reikalaujanti programinė įranga ar informacijos užvaldymas yra labai žalingi ir ilgai trunkantys pažeidimai, jie paprastai sukelia laikiną ar nuolatinį duomenų ir paslaugų neprieinamumą. Patikimos rezervinės kopijos yra būtinos norint atstatyti duomenis įvykus incidentui, organizacijoje turi būti aiškiai nustatyta, kaip yra atliekamas rezervinis kopijavimas.

- Viena iš efektyviausių saugumo priemonių – nuolat atnaujinti sistemas, nes gamintojai išleidžia saugos pataisas ir patobulinimus, kai aptinkamos problemos. Turi būti užtikrinami atnaujinimai ne tik įrenginių operacinėms sistemoms, bet ir taikomosioms programoms ar programėlėms įrenginiuose. Tai turėtų būti paskutinės gamintojo pateikiamos versijos. Dažnai atnaujinamų sistemų naujinimas turėtų būti dokumentuotas ir atsekamas.
- Kartais, atliekant techninės priežiūros darbus, programinės įrangos testavimą ar suteikiant vienkartinę prieigą prie sistemos, pritaikomi tokie nustatymai, kurie gali kelti pavojų saugumui. Šie laikini saugumo pakeitimai ar prieigos leidimai dažnai būna neprižiūrimi ir galiausiai tampa nuolatiniai, todėl atsiradusi saugumo spraga lieka atvira. Pavyzdžiui, dažnai tai būna prieigos prie duomenų bazės ar nuotolinio serverio per internetą suteikimas nesilaikant įprasto ar rekomenduojamo saugumo lygio ir nuostatų.
- Pagrindinė priemonė informacijos konfidencialumui užtikrinti yra nustatyti privalomą šifravimą, bent jau nešiojamiems prietaisams, nes juos galima lengvai pamesti arba juos gali pavogti. Ši rekomendacija taikoma ne tik nešiojamiesiems kompiuteriams, bet ir telefonams, planšetiniams kompiuteriams, USB atmintinėms, išoriniams standiesiems diskams ir rezervinėms kopijoms, saugomoms kur nors kitur.