REKOMENDACIJA
DĖL KIBERNETINIŲ INCIDENTŲ PREVENCIJOS

2024-12-30

Įvadas

Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) parengta rekomendacija skirta visuomenei. Šios rekomendacijos tikslas – **atkreipti visuomenės dėmesį į veiksmus, kurių reiktų imtis įvykus kibernetiniam incidentui, kurio metu yra pažeisti asmens duomenys.**

Kibernetinių incidentų tipai

Kibernetinis incidentas – įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.[1]

1. Išpirkos reikalaujančios kenkėjiško programinio kodo virusai (angl. *Ransomware*) (toliau – *Ransomware*). Šie virusai nuo kitų skiriasi savo agresyvumu – užvaldytoje sistemoje jie nesistengia užmaskuoti savo veiklos pėdsakų, svarbiausias jų tikslas yra užšifruoti sistemos savininkui svarbias bylas

[1] https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr

ar net visą failų sistemą, tikintis, kad savininkas bus pasiryžęs sumokėti išpirką jų atgavimui. *Ransomware* virusai plinta ir kompiuterines sistemas infekuoja dviem pagrindiniais būdais: platinami kartu su SPAM elektroniniais laiškais – atidarius prisegtus kenkėjiškus failus; per užkrėstas interneto svetaines (*Exploit Kits*) – parsiunčiami ir įrašomi išnaudojant programinės įrangos spragas. Šiuo metu *Ransomware* šeimos kenkėjiškas programinis kodas pirmauja pasaulyje pagal paplitimą.[2]

2. Fišingas (angl. *Phishing*) – socialinės inžinerijos forma, kai apgaule (dažnai apsimetus patikima institucija ar kitu asmeniu) siekiama išgauti prisijungimo prie sistemų duomenis ar kitą konfidencialią informaciją. Tam sukčiai naudoja elektroninius laiškus, suklastotus internetinius tinklalapius bei kitas priemones. Socialinės inžinerijos principais paremtos kibernetinės atakos – tai metodas, kai siekiama pasinaudoti žmogiškosiomis savybėmis ir išgauti tam tikrą jautrią informaciją, pvz.: prisijungimo duomenis prie socialinių tinklų paskyrų, informacinių sistemų, bankinių paskyrų, atlikti pavedimus, apkrėsti organizacijos tinklą ir pan.[3]

3. Kenkėjiška programinė įranga *Trojan.Malware.Obscu.Gen* yra kenkėjiškas programinis kodas, kitaip dar vadinamas Trojos arkliu (angl. *Trojan Horse*). Trojos arkliai – programos, turinčios kenkėjiškų funkcijų ir besislepiančios kitose programose. Kitaip nei virusai, Trojos arkliai savaime nesidaugina – juos paskleidžia kita kenkėjiška programinė įranga. Į kompiuterius dažniausiai patenka išnaudodami spragas naršyklėse arba parsiunčiami pačio vartotojo, juos pateikiant kaip naudingas programas. Užkrėstoje sistemoje atveria atgalines duris (angl. *Backdoor*), tokiu būdu įgalindamas nuotolinį įrenginio valdymą. Tipinio Trojos arklio funkcionalumas yra klaviatūros paspaudimų registravimas, procesų valdymas, bylų išsiuntimas, galimybė stebėti naudotoją ir kt.[4]

4. Sistemų trikdymo ataka (angl. DDoS) (toliau – DDoS). SNMP yra vienas populiariausių tinklo įrenginių valdymo protokolų. Dėl SNMP protokolo sukuriamų saugumo spragų įsilaužėliui gali būti sudarytos sąlygos atlikti sistemos trikdymo ataką (DOS), kai kuriais atvejais – gauti prieigą prie pažeisto įrenginio. [5]

5. Slaptažodžių parinkinėjimas (angl. *Brute Force*) atakos – tai bandymai atspėti vartotojo prisijungimo duomenis prie informacinės sistemos, įvedinėjant atsitiktines simbolių sekas ir dažnai naudojamas kombinacijas. Tam naudojami įvairūs programiniai įrankiai, kurie, priklausomai nuo sistemos apsaugos lygio, suteikia galimybę atlikti iki kelių tūkstančių spėjimų per minutę. Įsibrauti į sistemą yra

[2] Ransomware | Nacionalinis kibernetinio saugumo centras - NKSC
[3] Fisingo_atakos.pdf (nksc.lt)
[4] Trojan.Malware.Obscu.Gen | Nacionalinis kibernetinio saugumo centras - NKSC
[5] SNMP DDoS | Nacionalinis kibernetinio saugumo centras - NKSC

paprasta, jeigu žinomas jos prisijungimo adresas, o sugalvotas paskyros slaptažodis yra nesudėtingas arba labai panašus į prisijungimo vardą.[6]

Veiksmai, kurių turėtų imtis duomenų subjektai įvykus kibernetiniam incidentui, kurio metu yra pažeisti asmens duomenys

Nedelsiant pranešti apie incidentą. Svarbu nedelsiant pranešti apie duomenų pažeidimą atitinkamoms institucijoms. Vykdant tyrimus ir aptikus galimus Asmens duomenų teisinės apsaugos įstatymo pažeidimus, susijusius su asmens duomenimis, NKSC informaciją apie incidentą pagal kompetenciją perduoda Valstybinei duomenų apsaugos inspekcijai, o jei tyrimo medžiagoje yra nusikalstamos veikos požymių – Lietuvos kriminalinės policijos biuro Sunkaus ir organizuoto nusikalstamumo 5-ajai valdybai (Kiberpolicijai).

1. Jeigu susidūrėte su išpirkos reikalaujančios kenkėjiško programinio kodo virusais (angl. *Ransomware*):

Pirmas žingsnis – paties viruso pašalinimas. Šiuolaikiniai *Ransomware* virusai be failų užšifravimo pakeičia ir paties įrenginio sisteminius failus, registrų įrašus, tam, kad galėtų užšifruoti naujai sukurtus failus bei paleisti kenkėjiškus procesus po įrenginio perkrovimo. Pašalinus virusą reikia jį identifikuoti – tai galima padaryti pagal užšifruotų failų plėtinį (*Extension*) ar sukurtose instrukcijose failams atstatyti esančius indikatorius, tokius kaip kontaktinis el. pašto adresas, URL nuorodos ar tam tikri sakiniai. Juos įvedus į „Google“ paieškos laukelį dažniausiai pavyksta nustatyti *Ransomware* pavadinimą.

Nustačius, koks virusas užšifravo failus, galima rasti daugiau informacijos apie patį virusą, jo naudojamų šifravimo raktų stiprumą ir, svarbiausia, ar įmanoma šiuo metu atgauti jo užšifruotus failus. Visiems *Ransomware* virusams, kurių užšifruoti failai šiuo metu gali būti sėkmingai atšifruoti, yra sukurti atšifravimo įrankiai, kurių sąrašas skelbiamas čia. Šie įrankiai yra nuolat papildomi naujais raktais, todėl nepavykus atgauti užšifruotų duomenų, tai gali pavykti ateityje.

Bet kokiu atveju nereikėtų mokėti išpirkos norint atgauti prarastus duomenis, nes tai dar labiau paskatina nusikaltėlius plėtoti šį „verslą“ ir negarantuoja, kad sumokėjus duomenys bus atstatyti.[7]

---

[6] „Brute force“ atakos | Nacionalinis kibernetinio saugumo centras - NKSC
[7] Ransomware | Nacionalinis kibernetinio saugumo centras - NKSC

2. Jeigu susidūrėte su Fišingo (angl. *Phishing*) ataka[8]

Dažniausiai tokio pobūdžio atakos būna nukreiptos prieš bankų klientus, siekiant sužinoti jų prisijungimo prie elektroninės bankininkystės sistemų slaptažodžius ar kreditinių kortelių duomenis. Vėliau tokiu būdu gauta informacija gali būti panaudota vykdant nusikalstamas veikas: neteisėtus prisijungimus prie informacinių sistemų, pinigų vagystes iš sąskaitų ar elektroninėje erdvėje atsiskaitant už prekes svetimomis kortelėmis.

El. paslaugų naudotojai taip pat turi saugotis ir įprastų klastočių internete, kurios imituoja:

a) el. pašto paslaugą teikiančius tinklalapius (gmail.com, yahoo.com, hotmail.com ir kt.);

b) socialinius tinklalapius (facebook.com, vk.com);

c) itin populiarią užsienyje el. mokėjimų sistema „Paypal“ (paypal.com);

d) kitas populiarias interneto svetaines.

Rekomenduojama vartotojams[9]:

a) nespausti įtartinų ar neaiškių nuorodų, gautų su elektroniniais laiškais ar rastų įtartino turinio tinklalapiuose;

b) prieš vedant savo asmeninius duomenis internetinėse svetainėse, visada įsitikinti, kad svetainė nėra suklastota. Būtina atkreipti dėmesį į domeno vardą bei puslapyje esančių nuorodų adresus. El. bankininkystės sistemos visada naudoja saugų SSL ryšio protokolą, adreso pradžioje būtinai yra https ir galima patikrinti svetainės sertifikatą. Suklastotų svetainių adreso pradžia beveik visada būna http (be s);

c) turėti omenyje, kad bankai niekuomet neprašo pateikti ar keisti tik Jums žinomų banko internete ar mokėjimo kortelės slaptažodžių el. laiškais ar telefonu.

3. Jeigu susidūrėte su kenkėjiška programine įranga *Trojan.Malware.Obscu.Gen* Trojos arkliu (angl. *Trojan Horse*) rekomenduojama vartotojams[10]:

a) įdiegti arba atnaujinti naudojamas kompiuterio apsaugos sistemas;

b) pasinaudojant antivirusine programa atlikti pilną kompiuterio patikrą nuo virusų;

c) įdiegti naujausius operacinės sistemos ir naudojamų programų atnaujinimus;

d) nespausti įtartinų ar neaiškių nuorodų, gautų su elektroniniais laiškais ar rastų įtartino turinio tinklalapiuose.

[8] Phishing | Nacionalinis kibernetinio saugumo centras - NKSC
[9] https://esaugumas.lt/articles/duomenu-vagystes-phishing
[10] Trojan.Malware.Obscu.Gen | Nacionalinis kibernetinio saugumo centras - NKSC

Įrankiai patikrinimui:

http://www.f-secure.com/en_EMEA/security/security-lab/tools-and-services/online-scanner/

http://www.eset.com/us/online-scanner/

Primename, kad nežinomų (naujų) virusų antivirusinės programos nepažįsta, kol jie nėra įtraukti į duomenų bazę. Todėl internetinių skenerių parodymai ne visada 100 % tikslūs.[11]

4. Jeigu susidūrėte su Sistemų trikdymo ataka (angl. DDoS)[12]:

a) atnaujinti įrenginio programinę įrangą (angl. *firmware*);

b) nustatyti įrenginio sąranką taip, kad ryšys su kitais įrenginiais nebūtų nustatomas pagal nutylėjimą (angl. *default settings*);

c) nesant SNMP protokolo naudojimo būtinybės, rekomenduojame šią paslaugą išjungti.

Jei manote, kad patys nesugebėsite to padaryti, kreipkitės į specialistą.

Įrankiai patikrinimui: https://www.cert.lt/irankiai.html

5. Jeigu susidūrėte su slaptažodžių parinkinėjimo (angl. *Brute Force*) ataka[13]:

- Reikia naudoti sudėtingus slaptažodžius, kuriuos sudarytų atsitiktinės didžiosios bei mažosios raidės ir skaičiai;
- slaptažodyje nenaudoti savo gimimo metų, vardo, pavardės, slapyvardžio ar kitų su savimi susijusių ir kitiems žinomų, lengvai atspėjamų žodžių;
- prisijungimo puslapiui nenaudoti populiarių adresų (/admin, /cms, /wp-admin ir t. t.);
- naudoti CAPTCHA paveikslėlius, siekiant išvengti automatizuotų atakų;
- nustatyti, kad prie tinklalapių TVS būtų galima jungtis tik iš vidinio įmonės tinklo arba nustatytų IP adresų (pvz. naudojant .htaccess failą);
- nustatyti maksimalų nepavykusių prisijungimų kiekį per tam tikrą laiko intervalą, po kurio būtų laikinai išjungta galimybė prisijungti spėliojančiojo IP adresui arba laikinai užblokuota paskyra, prie kurios bandoma prisijungti.

Jeigu nurodyti problemos sprendimo būdai Jums atrodo per sudėtingi, siūlome kreiptis į specialistą.

---

[11] http://esaugumas.lt/lt/kompiuteriu-virusai/kenkejiskos-programines-irangos-tipai.html

[12] SNMP DDoS | Nacionalinis kibernetinio saugumo centras - NKSC

[13] „Brute force“ atakos | Nacionalinis kibernetinio saugumo centras - NKSC

Rekomendacijos

Atsižvelgusi į pastebimas tendencijas, kad dažnu atveju kibernetiniai incidentai įvyksta dėl nepakankamos duomenų apsaugos, VDAI teikia rekomendacijas visuomenei, kurios padės geriau apsaugoti asmens duomenis:

1. **Stiprūs slaptažodžiai**. Naudokite ilgus ir sudėtingus slaptažodžius, kuriuose būtų skaičiai, didžiosios ir mažosios raidės bei specialieji simboliai. Venkite naudoti tuos pačius slaptažodžius skirtingose platformose.
2. **Dviejų faktorių autentifikacija (2FA)**. Įjunkite dviejų faktorių autentifikaciją ten, kur tik įmanoma, ypač svarbioms paskyroms, pavyzdžiui, elektroniniam paštui, banko paskyroms ir socialinių tinklų paskyroms. Tai labai padidina saugumą, nes net ir atskleidus slaptažodį, prieigos be papildomo patvirtinimo gauti neįmanoma.
3. **Elektroniniai laiškai ir pranešimai**. Būkite atsargūs atidarydami neaiškios kilmės elektroninius laiškus ar spustelėdami juose esančias nuorodas. Duomenų vagystės (angl. *Phishing*) apgaule paremtos atakos dažnai naudojamos norint pavogti asmeninę informaciją.
4. **Atnaujinkite programinę įrangą**. Reguliariai atnaujinkite visus savo įrenginius, įskaitant kompiuterius, mobiliuosius telefonus ir planšetinius kompiuterius. Programinės įrangos atnaujinimai dažnai apima saugumo patobulinimus, kurie padeda apsisaugoti nuo naujų grėsmių.
5. **Įdiekite antivirusinę apsaugą**. Įsitikinkite, kad jūsų įrenginiuose veikia patikima antivirusinė programa, kuri nuolat skenuoja įrenginį ir apsaugo nuo kenkėjiškų programų.
6. **Rūpinkitės savo tinklo saugumu**. Naudokite stiprius slaptažodžius ir šifravimą namų ir darbo Wi-Fi tinklams. Venkite naudoti nesaugius viešus Wi-Fi tinklus jungiantis prie elektroninio pašto, socialinių tinklų, finansinių paslaugų paskyrų.
7. **Viešos prieigos**. Nenaudokite viešų kompiuterių prisijungimui prie bankų, namų ar įstaigos tinklų.
8. **Asmeninės informacijos apsauga**. Būkite atsargūs skelbdami asmeninę informaciją internete, ypač socialiniuose tinkluose. Neatskleiskite savo slaptažodžių, kreditinių kortelių ar asmens tapatybės duomenų. Asmeninė informacija gali būti išnaudojama sukčių atakoms.
9. **Naudojimo įpročiai**. Reguliariai tikrinkite savo finansinių paskyrų išrašus ir įjunkite pranešimus apie finansines transakcijas, kad galėtumėte greitai pastebėti bet kokias įtartinas veiklas.
10. **Atsarginių kopijų kūrimas**. Reguliariai darykite savo duomenų atsargines kopijas į saugias vietas (pvz., atskirai saugomas laikmenas). Tai apsaugos jūsų duomenis atsitiktinio praradimo atveju arba jei įvyktų kibernetinis išpuolis.