VALSTYBINĖS DUOMENŲ APSAUGOS INSPEKCIJOS
REKOMENDACIJOS IR PATARIMAI
KAIP REIKĖTŲ ELGTIS SUSIDŪRUS SU ĮSILAUŽIMU Į INTERNETO SVETAINĘ

2025-01-22
Vilnius

Valstybinė duomenų apsaugos inspekcija, reaguodama į kibernetines atakas bei siekdama apsaugoti asmens duomenis, stiprinti kibernetinį saugumą, sumažinti jų skaičių ir kontroliuoti galimą žalą, primena, kaip reikėtų elgtis susidūrus su įsilaužimu į interneto svetainę.

ĮSILAUŽIMĄ PATYRUSIEMS SVETAINIŲ VALDYTOJAMS

Operatyviosios atminties atvaizdo sukūrimas:

1. Operatyviosios atminties analizė užima svarbią vietą kibernetinio incidento tyrime. Siekdami apeiti kibernetinio saugumo priemones, pasislėpti ar paslėpti įkalčius, piktavaliai stengiasi žalingą programinį kodą įdiegti tiesiai į įrenginio operatyviąją atmintį. Dažniausiai operatyviojoje atmintyje žalingas programinis kodas saugomas neužkoduotas ar neužšifruotas. Aptikus žalingą programinį kodą ir jį išanalizavus pavyksta nustatyti, kokius veiksmus atliko piktavaliai ar kokį tikslą jie norėjo pasiekti.
2. Siekiant neprarasti kibernetinio incidento tyrimui svarbios informacijos, kuri gali būti išlikusi įrenginio operatyviojoje atmintyje, rekomenduojame pirmiausia (neatliekant jokių kitų veiksmų) sukurti ir išsaugoti operatyviosios atminties atvaizdą.
3. Operatyviosios atminties atvaizdas gali būti išsaugotas skirtingais formatais: „aff4“, „raw“ ar „dmp“. Rekomenduojame naudoti „raw“ formatą.

Disko atvaizdo sukūrimas:

1. Įvykus kibernetiniam incidentui neretai siekiama kaip galima greičiau atstatyti darbo ar tarnybinės stoties veikimą, o tik po to pagalvojama apie detalesnį tyrimą. Siekiant išsiaiškinti kibernetinio incidento priežastį ir sumažinti tikimybę tokių incidentų pasikartojimui, visada reikėtų atlikti jo tyrimą.
2. Norint išsaugoti kuo daugiau informacijos, susijusios su kibernetiniu incidentu, visada rekomenduojame sukurti ir išsaugoti įrenginio „kietojo“ disko atvaizdą (angl. *image*). Toks būdas laiko atžvilgiu nėra efektyvus, tačiau minimizuoja informacijos (įkalčių / artefaktų) praradimą ar sugadinimą. Reikėtų pažymėti, kad disko atvaizdai užima daug vietos, tad reikėtų pasirūpinti vieta / disku, kur bus saugomas disko atvaizdas.
3. Disko atvaizdas gali būti išsaugotas skirtingais formatais: „E01“, „raw“, „smart“ ar „aff“. Rekomenduojame naudoti „E01“ ar „raw“ formatus.

Įvykus kibernetiniam incidentui svetainės valdytojas privalo:

1. Imtis skubių priemonių šiam incidentui suvaldyti ir galimoms neigiamoms pasekmėms užkardyti.
2. Detaliai išnagrinėti galimas kilusio kibernetinio incidento priežastis ir imtis atitinkamų veiksmų, kad jie nepasikartotų ateityje.

Būtina prisiminti, kad, vadovaujantis Kibernetinio saugumo įstatymu, tam tikri subjektai, pavyzdžiui, teikiantys elektroninės prekyvietės paslaugas, apie įvykusius kibernetinius incidentus privalo nedelsdami informuoti ir Nacionalinį kibernetinio saugumo centrą.

Asmens duomenų apsaugos požiūriu, svarbu įvertinti tai, kad:

1. Kibernetinis incidentas gali lemti asmens duomenų saugumo pažeidimą, pavyzdžiui, tuo atveju, jeigu svetainėje buvo tvarkomi ir asmens duomenys.
2. Ar kibernetiniu incidentu netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama

prieiga. Jeigu taip, tai svetainės valdytojui kyla Bendrajame duomenų apsaugos reglamente (BDAR) numatytos pareigos.

Pagal BDAR svetainės valdytojas privalo:

1. Imtis veiksmų padėčiai ištaisyti ir tokį atvejį detaliai užfiksuoti savo vidiniuose dokumentuose.
2. Jeigu dėl duomenų saugumo pažeidimo gali kilti pavojus fizinio asmens teisėms ir laisvėms, svetainės valdytojas privalo per 72 val. pranešti apie asmens duomenų saugumo pažeidimą priežiūros institucijai – Valstybinei duomenų apsaugos inspekcijai, o jei kyla didelis pavojus, pranešti reikia ir patiems asmenims, kuriuos toks incidentas galėjo paveikti.

Paskyros ir slaptažodžiai:

1. Naudotojų slaptažodžiai privalo būti bent 12 simbolių ilgio.
2. Neturi būti slaptažodžio sudarymo taisyklių, ribojančių leidžiamų simbolių tipą, t. y. turi būti leidžiama naudoti visus simbolius, įskaitant nelotyniškas raides, tarpus ir specialiuosius simbolius.
3. Turi būti galimybė naudotojams patiems pasikeisti savo slaptažodį.
4. Keičiant ar kuriant naują slaptažodį, naudotojui turi būti galimybė laikinai pamatyti visą savo įvestą užmaskuotą slaptažodį. Negali būti naudojamos slaptažodžio priminimo užuominos arba žiniomis pagrįstas autentifikavimas (vadinamieji „slapti klausimai“, angl. *secret questions*).
5. Prisijungimo duomenų atkūrimo funkcionalumas negali atskleisti dabartinio naudotojo slaptažodžio.
6. Naudotojų slaptažodžiai duomenų bazėje turi būti saugomi naudojant saugius kriptografinius maišos algoritmus.
7. Negali būti bendro naudojimo paskyrų, kuriomis naudotųsi daugiau nei vienas asmuo.
8. Negali būti paskyrų su naudotojo vardais (angl. *username*) pagal nutylėjimą (pvz. „admin“, „administrator“, „administratorius“, „user“, „naudotojas“ ir pan.).
9. Negali būti naudojami naudotojų vardai ir slaptažodžiai, kuriuos Paslaugų teikėjas naudoja kitose savo ar klientų sistemose. (Pvz., negali būti naudojamas paskyros arba duomenų bazės vardas ar slaptažodis, kurį Paslaugų teikėjas naudoja pas kitą klientą).
10. Negali būti naudojami naudotojų vardai ir slaptažodžiai, kurių sudarymo algoritmas būtų nuspėjamas. (Pvz., kai naudotojo vardas ar slaptažodis skirtingiems Paslaugų teikėjo klientams skiriasi tik keliais simboliais.)
11. Negali būti naudojami naudotojų vardai ir slaptažodžiai, kuriuos sudarytų bet kokie Perkančiosios organizacijos požymiai ar jų dalys (pvz., pavadinimas, adresas, įmonės kodas ar jų dalys).

INTERNETO SVETAINIŲ LANKYTOJAMS

Naršant internete, patariama:

1. Nenaršyti ir ypač nesuvedinėti jokių duomenų internetinėse svetainėse, kurios nenaudoja duomenų šifravimo, t. y. neturi adreso pradžioje *„https“.*
2. Visuomet įsitikinti, ar svetainėje paskelbta privatumo politika (angl. *website privacy policy*).
3. Įsitikinti, kad svetainės valdytojas skelbia savo kontaktinę informaciją.
4. Turėti įsidiegus programinę įrangą, kuri blokuotų neįprastą tinklalapių veiklą, „iššokančius“ langus bei siūlymus atsisiųsti ir įdiegti neaiškios kilmės dokumentus ar programas.
5. Užėjus į įtarimų keliančią interneto svetainę, nespausti jokių nuorodų, prie jų nesijungti naudojantis asmeninių paskyrų (pavyzdžiui, socialinių tinklų, el. pašto paslaugų ir pan.) prisijungimo duomenimis, nevesti jokios asmeninės informacijos.
6. Nepasitikėti pateikta informacija apie galimus laimėjimus ar kitus prizus, kai prašoma pateikti asmens duomenis, mokėjimų kortelių duomenis ar kitą asmeninę informaciją ar atsisiųsti papildomas aplikacijas, kad galėtumėte atsiimti savo laimėjimus ar prizus.

Net jei svetainė turi SSL sertifikatą, privatumo politiką, kontaktinę informaciją, ji vis tiek gali būti nesaugi, jei yra užkrėsta kenkėjiška programine įranga.

<u>Apie tai, kad svetainė užkrėsta kenkėjiška programine įranga</u>, <u>galima sužinoti iš tam tikrų kibernetinių atakų požymių:</u>

1. **Turinio iškraipymo ataka** (angl. *defacement*).
   Ši ataka lengvai atpažįstama – kibernetiniai sukčiai pakeičia svetainės turinį savo vardu, logotipu ir (arba) ideologiniais vaizdais, iššaukiančia reklama ar pan.
2. **Iššokantys langai** (angl. *suspicious pop ups*).
   Reikia būti atsargiems dėl iššokančių langų, kurie pateikia su svetainės turiniu nesusijusią informaciją. Greičiausiai bandoma privilioti svetainės lankytoją spustelėti ir netyčia atsisiųsti kenkėjiškas programas.
3. **Kenkėjiška reklama** (angl. *malvertising*).
   Dažniausiai kenkėjišką reklamą nesunku atpažinti. Paprastai ji atrodo neprofesionali, joje yra rašybos, gramatikos klaidų, reklamuojami „stebuklingi“ išgydymai ar garsenybių skandalai. Svarbu atminti, kad ir tvarkingoje reklamoje ar skelbimuose, atitinkančiuose Jūsų naršymo istoriją, taip pat gali būti kenkėjiškų programų, todėl reikia būti atsargiems ir ieškoti dominančių dalykų patikimose paieškos sistemose.
4. **„Fišingo“ rinkiniai** (angl. *phishing kits*).
   Tai yra svetainės, imituojančios dažniausiai lankomas svetaines, pvz., bankininkystės svetaines, socialinių tinklų svetaines ir pan., siekiant apgauti vartotojus perimant privačią informaciją. Reikia atkreipti dėmesį į naršyklėje matomą svetainės adresą, ar svetainės vardas (URL adresas) neturi gramatinių klaidų, ar jis nėra neįprastos sandaros.
5. **Kenkėjiškas peradresavimas** (angl. *malicious redirect*).
   Jei įvedant URL adresą esate nukreipiami į kitą svetainę, ypač į tą, kuri atrodo įtartina, jus paveikė kenkėjiškas peradresavimas, kuris dažnai naudojamas kartu su „fišingo“ rinkiniais. Nenaršykite tokioje svetainėje, perkraukite naršyklę prieš tolesnį naršymą internete.
6. **Paieškos šlamštas** (angl. *SEO spam*).
   Neįprastų nuorodų atsiradimas svetainėje, dažnai komentarų skiltyje, yra tikras paieškos šlamšto ženklas.
7. **Įspėjimai paieškos sistemose.**
   Populiarios paieškos sistemos tikrina svetaines dėl kenkėjiškų programų ir deda įspėjimą apie tai. Neverta ignoruoti šių įspėjimų, nes jie vienareikšmiškai parodo, kad svetainė užkrėsta kenkėjiška programine įranga.

Geros dienos.

Pagarbiai

EB Law & Consulting
EB Teisė ir konsultacijos

Josifas Lovkys
Teisininkas -konsultantas
UAB „EB teisė ir konsultacijos“
Ukmergės g. 369A, 8 a., LT-12142, Vilnius
Mob. +370 698 11214
El. paštas: dap@eblaw.lt