DUK. Įsilaužimai į interneto svetaines – kaip reikėtų elgtis?

2019-09-17

Valstybinė duomenų apsaugos inspekcija, reaguodama į informaciją dėl įsilaužimų į 100 privataus ir viešojo sektoriaus interneto svetainių, primena, kaip reikėtų elgtis susidūrus su tokiu atveju.

Įsilaužimą patyrusiems svetainių valdytojams

Įvykus kibernetiniam incidentui svetainės valdytojas privalo:

- Pirmiausia imtis skubių priemonių šiam incidentui suvaldyti ir galimoms neigiamoms pasekmėms užkardyti;
- Tuomet jis turėtų 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:

- Kibernetinis incidentas gali lemti asmens duomenų saugumo pažeidimą, pavyzdžiui, tuo atveju, jeigu svetainėje buvo tvarkomi ir asmens duomenys;
- 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:

- Imtis veiksmų padėčiai ištaisyti ir tokį atvejį detaliai užfiksuoti savo vidiniuose dokumentuose;
- 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.

Pranešimą Valstybinei duomenų apsaugos inspekcijai patariama pateikti užpildant **„Pranešimo apie asmens duomenų saugumo pažeidimą rekomenduojamą formą“>>. Taip pat galite pasidomėti papildoma informacija>> apie duomenų saugumo pažeidimus ir inspekcijos rekomendacijomis>>.**

Interneto svetainių lankytojams

Naršant internete, patariama:

- Nenaršyti ir ypač nesuvedinėti jokių duomenų internetinėse svetainėse, kurios nenaudoja duomenų šifravimo, t. y. neturi adreso pradžioje „*https“;*
- Visuomet įsitikinti, ar svetainėje paskelbta privatumo politika (angl. *website privacy policy*);
- Įsitikinti, kad svetainės valdytojas skelbia savo kontaktinę informaciją;
- Turėti įsidiegus programinę įrangą, kuri blokuotų neįprastą tinklalapių veiklą, „iššokančius“ langus bei siūlymus atsisiųsti ir įdiegti neaiškios kilmės dokumentus ar programas;
- 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;
- 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. Apie tai, kad svetainė užkrėsta kenkėjiška programine įranga, galima sužinoti iš tam tikrų kibernetinių atakų požymių:

- **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.;
- **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;
- **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;

- **„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;
- **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 tolimesnį naršymą internete;
- **Paieškos šlamštas** (angl. *SEO spam*). Neįprastų nuorodų atsiradimas svetainėje, dažnai komentarų skiltyje, yra tikras paieškos šlamšto ženklas;
- **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.