LIETUVOS RESPUBLIKOS
SVEIKATOS APSAUGOS MINISTERIJA

E. sveikata: sistemos spragos ir kibernetinis saugumas

Sveikatos apsaugos ministerijos
Duomenų apsaugos pareigūnė

Neringa Viliūnaitė
2018-10-25

Pagrindinės sąvokos

E. sveikata - Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema

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

Asmens duomenų saugumo pažeidimas – 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

Duomenų valdytojas (Ministerija) - fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones

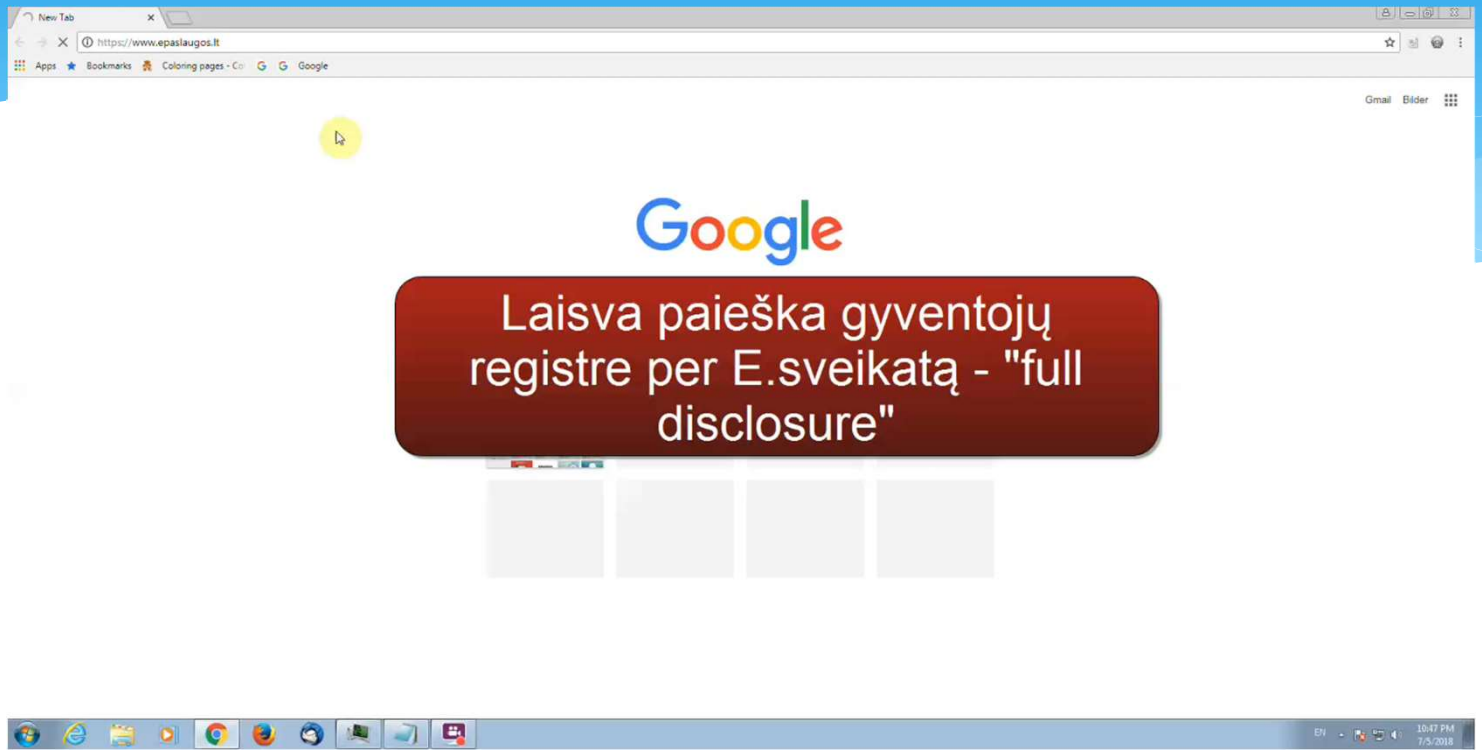
Duomenų tvarkytojas (VĮ Registrų centras – pagrindinis E. sveikatos tvarkytojas) - fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis

Duomenų subjektas - fizinis asmuo, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti ir kurio duomenys yra tvarkomi

Trumpai apie 2018-07-09 įvykusį kibernetinį incidentą

2018 m. liepos 9 d. 10 val. 32 min. VĮ Registrų centro IT pagalbos skyriuje buvo užregistruotas kibernetinis incidentas. Atlikus vertinimą, kibernetinis incidentas buvo patvirtintas, nustatyta, kad buvo atskleisti E. sveikatos sistemoje tvarkomų 20 asmenų duomenys. Gavus informaciją apie saugumo spragą, nedelsiant buvo išjungta prieiga prie E. sveikatos pacientų portalo. Pacientų portalas nevaidina kritinio vaidmens E. sveikatos struktūroje ir daugiau skirtas pacientų informavimui apie paciento įrašus, saugomus E. sveikatoje. Pašalinus saugumo spragą, portalas tapo vėl prieinamas.

Kibernetinio incidento vertinimo metu nustatyta, kad kelios dienos iki kibernetinio incidento registravimo, 2018 m. liepos 5 d. 23 val. 40 min. interneto svetainėje www.esec.lt buvo paskelbtas vaizdo įrašas apie minėtą saugumo spragą. Naujienų portalas „15 min“ apie tai viešai pranešė po keleto dienų 2018 m. liepos 9 d. 12 val. 11 min., prieš tai pateikęs informaciją VĮ Registrų centras.


New Tab
https://www.epaslaugos.lt
Apps
Bookmarks
Google
Gmail
Bilder
Google
Laisva paieška gyventojų registre per E.sveikatą - "full disclosure"

Trumpai apie 2018-07-09 įvykusį kibernetinį incidentą (2)

Saugumo spragą nustatęs asmuo, panaudodamas specialiąsias žinias, ne tik pažiūrėjo 20 asmenų duomenis, bet ir sukūrė metodinę medžiagą (filmuką), kaip galima pasinaudojant saugumo spraga gauti pacientų duomenis iš E. sveikatos, ir ją išplatino internete, taip sudarydamas galimybę prie duomenų prieiti ir specialių žinių neturintiems asmenims.

Saugumo spragos priežastys ir taikytos priemonės

E. sveikatos pacientų portale pacientui sudaryta galimybė įgalioti kitą asmenį atlikti tam tikrus veiksmus vietoje paties paciento. Įvedimo formoje buvo reikalaujama suvesti tokią informaciją, kuri vienareikšmiškai identifikuotų įgaliojamą asmenį – **turi būti tiksliai suvesti trys parametrai ir pagal šiuos parametrus asmuo ieškomas Gyventojų registre**. Jeigu toks asmuo Gyventojų registre yra, tai grąžinamas surasto asmens resursas (duomenys).

Pažeidimo atsiradimo priežastys:

Nors žiniatinklio forma reikalavo (privalomi laukai) nurodyti visus tris parametrus ir juos perduodavo į užklausą, tačiau **autorizuotam** naudotojui panaudojant specialias žinias **modifikavus** pačią užklausą, ji buvo vykdoma ir pagal vieną parametrą, t. y. paieška pagal vieną parametrą buvo vykdoma tik apėjus E. sveikatos numatytas įvedinių patikros ir kontrolės funkcijas. Tokiu būdu užklausą modifikavusiam asmeniui buvo pateiktas sąrašas asmenų. Grąžinant surasto asmens duomenis, buvo pateikiama daugiau duomenų, nei reikia užregistruoti įgaliotąjį asmenį (vardas, pavardė, asmens kodas, gimimo data, lytis, šeiminė padėtis, adresas, telefono numeris, elektroninės sveikatos istorijos numeris).

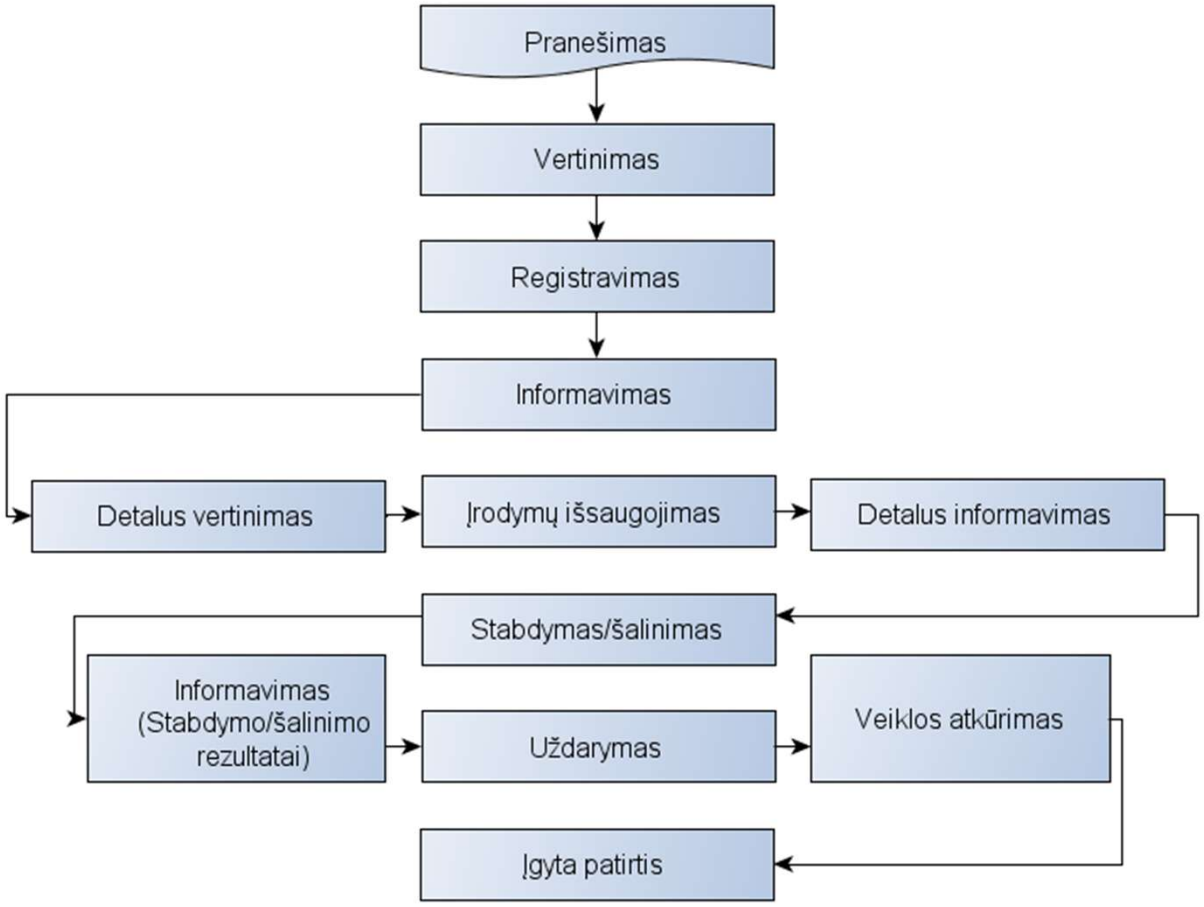
Taikytos priemonės:

Pakeista programinė įranga taip, kad pagal pateiktą užklausą grąžinami asmens duomenys tik tuo atveju, kai užklausoje nurodyti trys privalomi parametrai atitinka ieškomą asmenį.

Atsakyme į užklausą yra pateikiama „nukarpyta“ informacija, t. y. grąžinami ne visi E. sveikatoje kaupiami asmenį identifikuojantys duomenys, o tik trys laukai, kurie buvo nurodyti paieškoje kaip parametrai, bei asmens ID E. sveikatoje. Šio ID užtenka užregistruoti įgaliotąjį asmenį.

Taip pat buvo peržiūrėta, ar nėra daugiau vietų, kur panašios funkcijos būtų naudojamos.

Kibernetinio incidento valdymo standartinė schema



Kibernetinio incidento valdymas: informavimas

Apie kibernetinį incidentą VĮ Registrų centras (E. sveikatos pagrindinis tvarkytojas) pranešė Ministerijai ir Nacionaliniam kibernetinio saugumo centrui (pareiga pranešti nustatyta Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2016-04-20 nutarimu Nr. 387, 4.2.2 ir 4.8 papunkčiuose; Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, pavirtinto Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716, 33 punkte).

Kibernetinio incidento valdymas: informavimas (2)

Ministerija (E. sveikatos valdytojas) pranešė Valstybinei duomenų apsaugos inspekcijai pareiga pranešti nustatyta Bendrojo duomenų apsaugos reglamento 33 straipsnyje) bei padedama VĮ Registrų centras - Duomenų subjektams, kurių duomenys buvo atskleisti (pareiga pranešti nustatyta Bendrojo duomenų apsaugos reglamento 34 straipsnyje).

Kibernetinio incidento valdymas: informavimas (3)

Ministerija, įgyvendindama teisės aktuose nustatytą pareigą ir siekdama, kad būtų sumažinta rizika neigiamoms pasekmėms fizinių asmenų laisvėms ir teisėms kilti, pranešė apie incidentą, galimai turintį nusikalstamos veikos požymių policijai ir nurodė VĮ Registrų centras aukščiau nurodytam subjektui pateikti visą su incidentu susijusią informaciją (pareiga pranešti nustatyta Lietuvos Respublikos kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 4 punkte, Informacijos, reikalingos kibernetiniams incidentams, galimai turintiems nusikalstamos veikos požymių, užkardyti ir tirti, pateikimo, policijos nurodymų vykdymo bei kibernetinių incidentų tyrimo tvarkos aprašo, 12 punkte).

Trumpai apie 2018-10-03 įvykusį kibernetinį incidentą

2018 m. spalio 2 d. Laisvės TV laidoje „Karštos kėdės“ buvo pateikta informacija, kad E. sveikatoje pacientai turi galimybę matyti gydytojų asmens duomenis (įskaitant ir asmens kodą). Laidos metu tiksli informacija apie saugumo spragą nebuvo pateikta.

2018 m. spalio 3 d. VĮ Registrų centras IT pagalbos tarnyboje buvo užregistruotas incidentas dėl galimai nesaugaus tinklapio adreso (*URL „Uniform Resource Locator“*) E. sveikatoje, t. y. nustyta, kad pagal pateiktą užklausą turi būti gražinamas vieno specialisto duomenų rinkinys, tačiau modifikavus, nutrinant identifikatorių, gražinamas daugiau duomenų apimantis ir daugiau kaip vieno specialisto sąrašas. Atlikus pirminį incidento vertinimą nustatyta, kad E. sveiktoje pacientų portale pastebėta saugumo spraga sukėlė grėsmę E. sveikatoje tvarkomų sveikatos specialistų asmens duomenų konfidencialumui.

Kibernetinio incidento valdymas

VĮ Registrų centro specialistai nustatė ir pašalino galimas saugumo spragas, dėl kurių pacientams galėjo būti suteikta galimybė netiesiogiai pamatyti daugiau gydytojų asmens duomenų, nei yra numatyta E. sveikatos techniniuose reikalavimuose. Atsižvelgiant į tai, kad tiksli informacija apie saugumo spragą (kuri E. sveikatos dalis yra pažeidžiama) VĮ Registrų centras nebuvo pateikta, todėl buvo tikrinami visi įmanomi variantai ir ieškoma, ar nėra daugiau saugumo spragų, kurias išnaudojus pacientams galėtų būti suteikta galimybė netiesiogiai susipažinti su gydytojų asmens duomenimis.

VĮ Registrų centras 2018-10-04 apie šį incidentą teisės aktų nustatyta tvarka informavo Nacionalinį kibernetinio saugumo centrą, o Ministerija 2018-10-05 – Valstybinę duomenų apsaugos inspekciją. Pradiniame kibernetinio incidento tyrimo etape nebuvo nustatyta, kad šis incidentas, galimai turi nusikalstamos veikos požymių, tyrimo eigoje paaiškėjus, kad šis incidentas turi nusikalstamos veikos požymių apie jį teisės aktuose nustatyta tvarka bus pranešta policijai.

Situacija šiuo metu

VĮ Registrų centras teigimu paviešintos spragos šiuo metu yra pašalintos.

VĮ Registrų centras siekdamas įvertinti E. sveikatos saugumą planuoja įsigyti „Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos saugumo audito“ paslaugas.

VDAI ir NKSC rekomendacijos

Ministerija gavo VDAI ir NKSC rekomendacijas, kuriomis turėtų vadovautis VĮ Registrų centras:

* užtikrinti, kad tvarkant asmens duomenis E. sveikatoje būtų įgyvendintos tinkamos techninės ir organizacinės duomenų saugumo priemonės;
* siekiant išvengti analogiškų ar panašių duomenų saugumo pažeidimų ateityje, peržiūrėti duomenų saugumo priemones bei imtis papildomų, kad būtų užtikrintas tinkamas duomenų saugumas;
* Atlikti E. sveikatos saugos atitikties auditą ir informuoti VDAI, NKSC ir Ministeriją apie planuojamo atlikti E. sveikatos saugos atitikties audito rezultatus, kai jis bus atliktas;
* nustačius duomenų subjektus, kurių asmens duomenų saugumas buvo pažeistas, Bendrojo duomenų apsaugos reglamento nustatyta tvarka informuoti apie asmens duomenų saugumo pažeidimą. Jeigu paaiškėtų, kad tai pareikalautų neproporcingai daug pastangų, tokiu atveju taikyti Bendrojo duomenų apsaugos reglamento 34 straipsnio 3 dalį ir apie asmens duomenų saugos pažeidimą pranešti viešai paskelbiant arba taikant panašią priemonę, kuria duomenų subjektai būtų informuojami efektyviai. Pranešti VDAI ir Ministerijai apie šio pranešimo įgyvendinimą;
* nedelsiant kreiptis į E. sveikatos gamintoją/kūrėją su prašymu ištaisyti programavimo klaidas;
* pateikti informaciją NKSC apie E. sveikatos gamintojo/kūrėjo garantinius įsipareigojimus;
* pateikti NKSC E. sveikatos testavimo metodiką/scenarijus ir jų bandymų (testavimų) rezultatus.

Įgyta patirtis

E. sveikatos sistemoje yra tvarkomi pacientų sveikatos duomenys ir jų apsaugai yra skiriamas ypatingas dėmesys. Ministerija dės visas pastangas, kad būtų užtikrintas žmonių sveikatos duomenų saugumas, todėl reaguojame ir reaguosime į visus galimus pažeidimus ir tą darysime vadovaudamiesi Bendruoju duomenų apsaugos reglamentu ir kitais teisės aktais, reglamentuojančiais duomenų apsaugą. Tai yra Ministerijos, kaip duomenų valdytojos pareiga pacientams. Ir būsime dėkingi visiems asmenims, kurie padės mums vykdyti šią pareigą ir kurie apie pastebėtas spragas praneš jas panaikinti turinčioms institucijoms. Kuo daugiau bus tokių žmonių, tuo mes visi būsime saugesni ir tuo labiau gerbsime savo valstybę.

Turime būti pasiruošę galimiems scenarijams ir sudaryti galimybes pranešti apie žinomas saugos spragas tinkamu būdu.

LIETUVOS RESPUBLIKOS
SVEIKATOS APSAUGOS MINISTERIJA

Ačiū už dėmesį

Neringa Viliūnaitė
duomenu.apsauga@sam.lt