ATSAKINGO ATSKLEIDIMO SĄVOKOS, PROCESAS, KOMUNIKACIJOS PLANAS, PRINCIPAI IR TVARKA

Žygimantas Robertas Tamošauskas

http://kurklt.lt/projektai/atsakingas-kibernetinio-saugumo-spragu-atskleidimas-2/

Atsakingo atskleidimo sąvokos

Kibernetinio saugumo spraga – programinės įrangos, techninės įrangos arba internetinės paslaugos pažeidžiamumas, kuris gali būti išnaudotas kibernetinės atakos metu ir kelia grėsmę informacijos saugumui (ISO/IEC 29147:2014).

Kibernetinio saugumo subjektas – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas (LR Kibernetinio saugumo įstatymas).

Atsakingas kibernetinio saugumo spragos atskleidimas – procesas, kurio metu kibernetinio saugumo spragos atskleidimas koordinuojamas su kibernetinio saugumo subjektu, kurio sistemose buvo aptikta spraga (SANS institutas).

Spragų ieškotojas – asmuo ar organizacija, kuri identifikuoja galimą produkto ar internetinės paslaugos spragą. Tai gali būti mokslininkai, tyrėjai, kibernetinio saugumo įmonės, paslaugų naudotojai, institucijų atstovai ar koordinuojanti organizacija (ISO/IEC 29147:2014).

Koordinuojanti organizacija – galimas atsakingo atskleidimo proceso dalyvis, kuris gali padėti kibernetinio saugumo subjektams ir spragų ieškotojams tvarkyti ir atskleisti informaciją apie spragą (ISO/IEC 29147:2014).

Atsakingo atskleidimo proceso sudedamosios dalys

01 Atsakingo atskleidimo tvarkos parengimas ir paviešinimas

02 Pranešimų apie spragas priėmimo ir informacijos dalinimosi procesų parengimas

03 Pranešimų apie spragas priėmimas iš išorinių šaltinių

04 Pranešimo apie spragą gavimo patvirtinimas

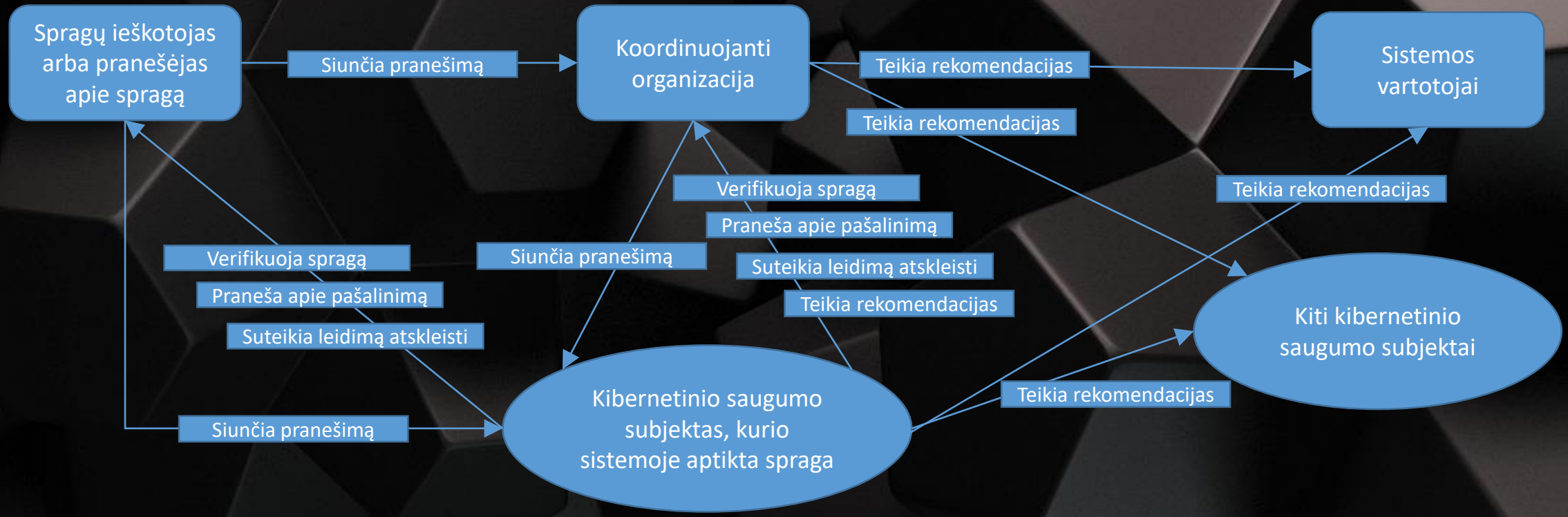
05 Spragos verifikavimas

06 Rekomendacijų teikimas sistemos vartotojams ir potencialiai paveiktiems kibernetinio saugumo subjektams

07 Spragos pašalinimas

08 Suteikiamas leidimas pranešėjui viešai dalintis informacija apie spragą

Atsakingo atskleidimo informacijos apsikeitimo planas



Lentelėje matoma, kad pranešėjas apie kibernetinio saugumo spragą gali rinktis apie ją informuoti atsakingo atskleidimo procesą koordinuojančią organizaciją arba atsakingo atskleidimo tvarką viešinantį kibernetinio saugumo subjektą. Gavusi pranešimą, koordinuojanti organizacija jį perduoda kibernetinio saugumo subjektui, kurio sistemoje aptikta spraga, ir jį įpareigoja per nustatytą laikotarpį verifikuoti spragos egzistavimo faktą, pranešti apie spragos pašalinimą ir suteikti leidimą apie šią spragą informaciją atskleisti viešai. Taip pat, kibernetinio saugumo subjektas tiesiogiai arba per koordinuojančią organizaciją teikia rekomendacijas, nukreiptas į spragos poveikio mažinimą, savo sistemos vartotojams. Rekomendacijomis dalinamasi ir su kitais kibernetinio saugumo subjektais, galimai susiduriančiais su panašaus tipo spragomis. Jeigu kibernetinio saugumo subjektas viešina atsakingo atskleidimo tvarką, pranešėjas gali kreiptis tiesiai į jį. Tokiu atveju, koordinuojančios organizacijos dalyvavimas nėra būtinas, o dvišalio proceso metu, kibernetinio saugumo subjektas spragą verifikuoja, praneša apie jos pašalinimą ir suteikia pranešėjui leidimą apie ją viešai atskleisti informaciją atsakingo atskleidimo tvarkoje numatytu būdu.

Atsakingo kibernetinio saugumo spragų atskleidimo praktikos principai

Žygimantas Robertas Tamošauskas

http://kurklt.lt/projektai/atsakingas-kibernetinio-saugumo-spragu-atskleidimas-2/

Atsakingo atskleidimo procese dalyvaujančių šalių įsipareigojimai

Kibernetinio saugumo subjektas arba koordinuojanti organizacija, priėmusi pranešimą apie spragą, prisiima šiuos įsipareigojimus:

- Per 3 darbo dienas pateikti pranešimo apie spragą gavimo patvirtinimą asmeniui, pateikusiam pranešimą apie spragą.
- Per 30 darbo dienų atlikti spragos verifikavimo procesą ir apie tai informuoti asmenį, pateikusį pranešimą apie spragą.
- Per 90 darbo dienų atlikti patvirtintos programinės įrangos spragos pašalinimą ir apie tai informuoti asmenį, pateikusį pranešimą apie spragą.
- Per 180 darbo dienų atlikti patvirtintos techninės įrangos spragos pašalinimą ir apie tai informuoti asmenį, pateikusį pranešimą apie spragą.
- Spragą pašalinus, suteikti leidimą apie ją pranešusiam asmeniui atskleisti informaciją apie atrastą spragą, išskyrus tuos atvejus kai pateikiamas motyvuotas paaiškinimas, kuriame nurodomi argumentai, dėl kurių informacija apie spragą neturėtų būti viešinama.
- Užtikrinti sąlygas konfidencialiam informacijos apie spragą perdavimui pasitelkiant kriptografinius protokolus.

Spragą aptikęs asmuo prisiima šiuos įsipareigojimus:

- Naudoja automatines spragų skenavimo priemones, tik tais atvejais, kai tai yra numatyta pagal dvišalę sutartį su kibernetinio saugumo subjektu, arba kai minėtas subjektas tokios įrangos naudojimą yra numatęs savo paviešintoje atsakingo atskleidimo tvarkoje.
- Netrikdo ir nekeičia kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbo.
- Nepiktnaudžiauja atrasta spraga, įsitikinus spragos egzistavimu, nutraukia su spragos paieška susijusią veiklą.
- Informacija apie sistemos spragą dalinasi tik su kibernetinio saugumo subjektu, kurio sistemoje aptikta spraga, arba koordinuojančia organizacija.
- Informaciją apie sistemos spragą viešina tik spragą pašalinus ir sulaukus kibernetinio saugumo subjekto, kurio sistemoje aptikta spraga, leidimo. Už pranešimą apie spragą gali būti skiriama premija arba paskatinimas, pvz. paminėjimas garbės lentoje.
- Nesiekia nereikalingai, daugiau nei to reikia patvirtinti spragai, stebėti, fiksuoti, perimti, įgyti kitų vartotojų duomenų.
- Imasi minimalių veiksmų, reikalingų įsitikinti spragos egzistavimu, naudojasi sistemos teikiamomis paslaugomis, o gavęs priėjimą prie svetimų duomenų, nedelsiant susisiekia su kibernetinio saugumo subjektu arba koordinuojančia organizacija.

Atsakingo atskleidimo proceso ribos ir pranešimas apie spragą

Su atsakingo atskleidimo procesu nesuderinamos šios veiklos:

- Galiojančių Lietuvos Respublikos įstatymų pažeidimas.
- Svetimų duomenų įgijimas, atskleidimas, perėmimas, dalinimasis, kopijavimas, naikinimas, saugojimas, fiksavimas ir daugkartinis arba ilgalaikis stebėjimas.
- Kibernetinių atakų vykdymas, galintis pakenkti sistemos palaikomų paslaugų ar duomenų konfidencialumui, prieinamumui arba vientisumui.
- Socialinė inžinerija nukreipta prieš sistemos vartotojus arba tvarkytojus.
- Dirbtinių sistemų trikdžių kėlimas arba sistemos darbo nutraukimas.
- Slaptažodžių laužimo atakų vykdymas.

Spragą aptikusiam asmeniui, rekomenduojama kibernetinio saugumo subjektui, viešinančiam atsakingo atskleidimo tvarką, arba koordinuojančiai organizacijai pateikti šią informaciją:*

- Išsamų spragos aprašymą, įskaitant išnaudojimo galimybes ir poveikį.
- Žingsnius, reikalingus spragos išnaudojimo galimybei atkurti.
- Paveiktus URL adresus, programėles, paveikto kodo fragmentą.
- IP adresus, kurie buvo naudojami atliekant tyrimą.
- Naudotojo ID, kuris buvo naudojamas spragai atskleisti.
- Visus failus, kuriuos buvo bandoma įkelti.
- Spragą aptikusio asmens kontaktinius duomenis.

*Spragą aptikęs asmuo turi teisę apie ją kibernetinio saugumo subjektui arba koordinuojančiai organizacijai pranešti anonimiškai. Kilus įtarimui, kad įvyko įstatymų pažeidimas, apie spragą pranešusio asmens teisė į anonimiškumą gali būti ribojama.

Visiems kibernetinio saugumo subjektams prieinamas atsakingo atskleidimo tvarkos šablonas

Žygimantas Robertas Tamošauskas

http://kurklt.lt/projektai/atsakingas-kibernetinio-saugumo-spragu-atskleidimas-2/

Atsakingo atskleidimo tvarkos šablonas

Sistemų saugumas – vienas iš mūsų svarbiausių prioritetų. Nors ir skiriame informaciniam saugumui labai daug dėmesio, suprantame, kad visada gali atsirasti kibernetinio saugumo spragų.

Norėtume, kad aptikę spragą, apie ją praneštumėte mums. Tokiu būdu, galėsime ją kiek įmanoma greičiau pašalinti. Norėtume paprašyti jūsų padėti mums geriau apsaugoti ne tik mūsų sistemas, bet ir mūsų klientus.

Iš jūsų tikimės, kad:

- Atsisiųsite informaciją apie atrastą spragą šiuo elektroninio pašto adresu: cert@pavyzdys.com, o siunčiamų duomenų saugumą užtikrinsite juos šifruodami mūsų PGP raktu, apsaugodami slaptažodžiu, arba kitais jums patogiais būdais.
- Nepiktnaudžiausite atrasta spraga, pvz. nebandysite parsisiųsti daugiau informacijos, nei tai yra reikalinga spragos egzistavimo įrodymui, nekeisite ir nešalinsite svetimų duomenų.
- Neviešinsite informacijos apie spragą tol, kol ji nebus pašalinta.
- Nenaudosite automatinių spragų skenavimo priemonių, socialinės inžinerijos, brukalo, atkirtimo nuo paslaugos atakų arba atakų prieš fizinį sistemų saugumą.
- Savo pranešime pateiksite pakankamą kiekį informacijos, kuri leistų atkurti spragą ir suteiktų mums galimybę ją pašalinti kiek įmanoma greičiau. Dažniausiai turėtų pakakti paveiktos sistemos IP arba URL adreso bei spragos aprašymo, tačiau sudėtingų spragų atkūrimui gali prireikti platesnio paaiškinimo.

Mes pažadame, kad:

- Pateiksime atsakymą į jūsų pranešimą per 3 darbo dienas. Šiame atsakyme įvertinsime jūsų pranešimą ir įvardinsime numatomą spragos pašalinimo datą.
- Jeigu vykdysite šioje tvarkoje aprašytus nurodymus, mes nesiimsime prieš jus jokių teisinių veiksmų, susijusių su jūsų pranešimu apie spragą.
- Užtikrinsime jūsų pranešimo konfidencialumą ir nesidalinsime jūsų asmeniniais duomenimis su trečiosiomis šalimis be jūsų sutikimo.
- Mes jus informuosime apie progresą šalinant spragą, apie kurią jūs pranešėte.
- Viešai atskleisdami informaciją apie jūsų praneštą spragą, įvardinsime jus kaip pranešėją, išskyrus tuos atvejus kai atsisakysite būti minimi.
- Norėdami atsidėkoti už jūsų pagalbą, pasiūlysime piniginį arba kitokį paskatinimą už pranešimus apie mums nežinomas saugumo spragas. Šis atlygis arba paskatinimas priklausys nuo spragos dydžio ir pateikto pranešimo kokybės.

Mes stengiamės pašalinti visas spragas kiek įmanoma greičiau, o tai atlikus, norėtume aktyviai dalyvauti viešame informacijos apie aptiktas spragas atskleidime.

Atsakingo atskleidimo tvarkos šablono pasirinktys

1. **Ankstesnėje skaidrėje aprašyta atsakingo atskleidimo tvarka gali būti perimta ir naudojama visų kibernetinio saugumo subjektų.** Norint naudoti šį tekstą, derėtų į jį įtraukti savo organizacijos pavadinimą, elektroninio pašto adresą ir PGP šifravimo raktą. Rekomenduojama šią tvarką viešinti organizacijos portale.
2. **Atsakingo atskleidimo lūkesčiai.** Tvarkoje rekomenduojama aiškiai įvardinti organizacijos nustatytus taikinius ir spragų ieškojimo metodus. Pateikta pavyzdinė tvarka turėtų būti tinkama daugeliui organizacijų, tačiau kai kurios iš jų gali turėti ypatingų lūkesčių, susijusių su savo produktais arba IT infrastruktūra. Tokiu atveju, rekomenduojama šiuos lūkesčius įvardinti atsakingo atskleidimo tvarkoje.
3. **Atsakingo atskleidimo tvarkos viešinimas koordinuojančios organizacijos portale.** Kibernetinio saugumo subjektai gali pasirinkti savo atsakingo atskleidimo tvarką įtraukti į koordinuojančios organizacijos portale talpinamą sąrašą. Šiame sąraše pateikiami kibernetinio saugumo subjektų, viešinančių atsakingo atskleidimo tvarkas, kontaktiniai duomenys ir jų viešinamų tvarkų turinys.
4. **Įsipareigojimas nesiimti teisinių veiksmų.** Kibernetinio saugumo subjektai atsakingo atskleidimo tvarkoje nurodo vieną iš šių punktų:
   - Nebus imamasi teisinių veiksmų prieš asmenį, kuris pranešė apie saugumo spragą atsižvelgdamas į paviešintą atsakingo atskleidimo tvarką.
   - Nėra galimybės garantuoti, kad prieš asmenį, kuris pranešė apie saugumo spragą, nebus imamasi teisinių veiksmų. Kiekvienas atvejis bus nagrinėjamas atskirai, o kilus įtarimams dėl piktnaudžiavimo spraga, apie šiuos įtarimus bus informuojamas pranešimą atsiuntęs asmuo.
5. **Trečiųjų šalių programinės įrangos naudojimas.** Atsakingo atskleidimo tvarkoje kibernetinio saugumo subjektas gali numatyti leidimą saugumo spragų ieškantiems ir apie jas pranešantiems asmenims spragų ieškoti pasitelkus trečiųjų šalių programinę įrangą, pvz. automatines spragų skenavimo priemones. Taip pat, gali būti nurodoma, kad tokios įrangos naudojimas nesuderinamas su paskelbta atsakingo atskleidimo tvarka.
6. **Saugumo spragų ieškojimo apimtis.** Atsakingo atskleidimo tvarkoje kibernetinio saugumo subjektas nurodo, kad paviešinta atsakingo atskleidimo tvarka galioja visoms jo sistemos arba pateikia sistemų sąrašą, kurioms galioja minėta tvarka.
7. **Saugumo spragų ieškojimo terminų numatymas.** Atsakingo atskleidimo tvarkoje rekomenduojama nurodyti jos galiojimo terminą. Kibernetinio saugumo subjektai gali viešinti trumpalaikę atsakingo atskleidimo tvarką, nustatytu laikotarpiu suteikiančią galimybę spragų ieškantiems ir apie jas pranešantiems asmenims saugumo spragų ieškoti ir apie jas pranešti tvarkoje numatytu būdu.
8. **Premija už atrastas spragas.** Kibernetinio saugumo subjektas gali savanoriškai numatyti atlygį arba kitokį paskatinimą, pvz. paminėjimą garbės lentoje, už pranešimus apie saugumo spragas.