Pamokos iš užsienio: atsakingo kibernetinio saugumo spragų atskleidimo praktika

Žygimantas Robertas Tamošauskas

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

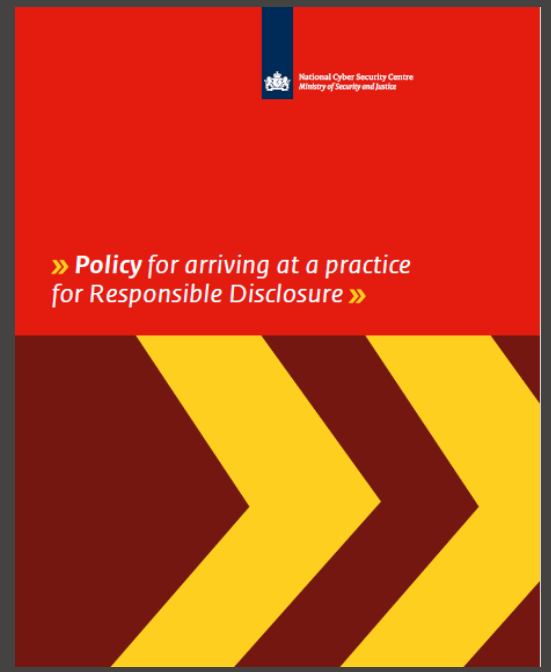
Turinys

Kurk Lietuvai


Nyderlandai
Nuo atsakingo prie
koordinuoto atskleidimo

Atsakingo atskleidimo praktikos kūrimo strategija

2013 m. Nyderlandų saugumo ir teisingumo ministras Ivas Opsteltenas savo šalies parlamentui pateikė Atsakingo atskleidimo praktikos kūrimo strategiją. Dokumente buvo pateiktos atsakingo kibernetinio saugumo (KS) spragų atskleidimo praktikos kūrimo gairės ir aprašyti kertiniai atsakingo atskleidimo tvarkos elementai. Strategija buvo paruošta Nyderlandų Saugumo ir teisingumo ministerijai konsultuojantis su pranešėjais apie KS incidentus bei viešojo ir privataus sektorių organizacijomis.



Svarbiausi Atsakingo atskleidimo praktikos kūrimo strategijos elementai:

- Pabrėžiama, kad atsakingo atskleidimo praktika neprieštarauja Nyderlanduose galiojantiems teisės aktams. Teigiama, kad strategija, tai – įrankis, siūlantis organizacijoms dirbti kartu su platesne kibernetinio saugumo bendruomene. Organizacijoms rekomenduojama paruošti ir paviešinti „atsakingo spragų atskleidimo tvarką“ – dokumentą, nustatantį atsakingo atskleidimo proceso eigą ir jame dalyvaujančių šalių teises ir pareigas.

- Apibrėžiamos kertinės sąvokos susijusios su atsakingo atskleidimo praktika bei nustatomos atsakingo atskleidimo procese dalyvaujančių šalių atsakomybės.

Kurk Lietuvai

Atsakingo atskleidimo praktikos kūrimo strategijoje numatytos suinteresuotų šalių atsakomybės:

1. **Organizacija, kurios IT arba ryšių sistemose buvo aptikta spraga:** rengia savo atsakingo KS spragų atskleidimo tvarką, joje nustato reagavimo į pranešimą apie KS spragą veiksmų planą. Konsultacijų su pranešėju metu, nustato spragos viešinimo terminą. Rekomenduojami viešojo atskleidimo terminai: 60 dienų programinės įrangos spragai, 180 dienų techninei spragai.

2. **Pranešėjas apie aptiktą KS spragą:** konfidencialiai ir kiek įmanoma skubiau praneša apie spragą organizacijai arba Nyderlandų Nacionaliniam kibernetinio saugumo centrui, nesiima neproporcingų daromai naudai žalingų veiksmų.

3. **Nyderlandų Nacionalinis kibernetinio saugumo centras:** pripažįsta, kad atsakingas atskleidimas yra dvišalis procesas, kuriame dalyvauja organizacija ir pranešėjas. Skatina privataus sektoriaus subjektus ruošti ir viešinti subjekto lūkesčius atitinkančias atsakingo KS spragų atskleidimo tvarkas.

Nuo atsakingo prie koordinuoto spragų atskleidimo

Praėjus penkeriems metams nuo 2013 m. Atsakingo atskleidimo praktikos kūrimo strategijos paviešinimo, Nyderlandų Nacionalinis kibernetinio saugumo centras 2018 m. spalio mėn. paviešino Koordinuoto spragų atskleidimo gaires. Centro vadovybės teigimu, atnaujintose gairėse atsispindi nuo 2013 m. strategijos paviešinimo įsisavintos pamokos.

2013

2016

2018

1140 pranešimai apie KS spragas

Atsakingo atskleidimo gairių nauda:

- CIO Platform Nederland kibernetinio saugumo vadovų asociacijos duomenimis, nuo 2013 m. strategijos paviešinimo, pradėjo augti organizacijų, naudojančių atsakingo atskleidimo praktiką, skaičius.
- Nyderlandų kibernetinio saugumo vertinime už 2018 m. minima, kad tarp 2017 m. gegužės mėn. ir 2018 m. balandžio mėn. Nyderlandų Nacionalinis kibernetinio saugumo centras, kuris viešina atsakingo atskleidimo tvarką, taikomą visoms centrinės valdžios IT arba ryšių sistemoms, sulaukė 1140 pranešimų apie KS spragas.

Kurk Lietuvai

Koordinuoto spragų atskleidimo gairės:

Kertinis gairių elementas – teisiniai koordinuoto atskleidimo aspektai:

- Siekiant suderinamumo su Tarptautinės standartizacijos organizacijos publikuotais KS spragų atskleidimo standartais (ISO/IEC 29147:2014 ir ISO/IEC 29147:2018), 2013 m. strategijoje minimas atsakingas atskleidimas buvo pervadintas į koordinuotą atskleidimą.
- Lyginant su 2013 m. strategija, gairėse daugiau dėmesio skiriama teisiniams koordinuoto atskleidimo aspektams. Pripažįstama, kad spragos atradimas gali būti susijęs su įstatymo pažeidimais.
- Pabrėžiama, kad KS spragų ieškojimo ir viešinimo procese organizacija ir pranešėjas apie spragą gali vadovautis dvišaliu tarpusavio susitarimu, nustatytu pagal organizacijos skelbiamą koordinuoto atskleidimo tvarką (KAT). Ši tvarka turėtų apibrėžti koordinuoto spragų atskleidimo procese dalyvaujančių šalių veiklos ribas, teises ir atsakomybes. Tokiu būdu, KAT taptų spragos atskleidimo procesą reguliuojančių dokumentu. Laikantis šiame dokumente nustatytų veiklos principų, šalys išvengtų baudžiamosios arba administracinės atsakomybės taikymo. KAT taikančioms organizacijoms taip pat rekomenduojama į dokumentą įtraukti įsipareigojimą nesikreipti į teisėsaugą, jeigu koordinuotas spragos atskleidimas buvo vykdomas pagal tvarkoje įvardintas sąlygas.
- Gairėse nurodoma, kad esant kreipimuisi į teisėsaugą, Nyderlandų teisėsaugos atstovai įvertina KAT dokumento egzistavimo faktą ir nepradeda tyrimo jei nustatoma, kad pranešėjas apie KS spragą laikėsi KAT nustatytų normų.
- Gairėse atkreipiamas dėmesys į Nyderlandų prokuratūros paviešintą, jos veiklos kryptis atskleidžiantį, kreipimąsi į visuomenę, kuriame teigiama, kad, teisinių veiksmų prieš asmenį, pranešusį apie KS spragą, imamasi tik įvertinus šias tris aplinkybes:

    1. Ar pranešėjo veiksmai tarnavo svarbiam viešajam interesui?
    2. Ar pranešėjo veiksmų žala buvo neproporcingai didelė, lyginant su daroma nauda?
    3. Ar pranešėjas galėjo identifikuoti KS spragą pasitelkdamas mažiau drastiškus veiksmus?

- Gairėse pabrėžiama, kad nuo 2013 m. Atsakingo atskleidimo praktikos kūrimo strategijos paviešinimo, teisinė Nyderlandų praktika rodo, kad šalies teisėsauga atsižvelgia į minėtąsias tris aplinkybes ir tais atvejais kai organizacija, kurios KS spraga buvo atskleista, neviešina KAT.

Latvija

Bandymas sukurti valstybės reglamentuojamą atsakingo spragų atskleidimo procesą

Siekis įteisinti atsakingo spragų atskleidimo procesą

Užduotis pavesta darbo grupei

2016 m. Kovo mėn. Latvijos Krašto apsaugos ministerija sudarė darbo grupę, kurios tikslas buvo įteisinti atsakingo spragų atskleidimo procesą (ASAP).

Įstatymų pakeitimus buvo ketinama takyti valstybės mastu. Išimtys savivaldybėms ir kritinės infrastruktūros subjektams numatytos nebuvo.

Iki tol, buvo svarstoma kurti premijų už spragas programą (angl. „bug bounty program“) numatančią pinigines premijas už KS spragų identifikavimą, tačiau šios iniciatyvos buvo atsisakyta dėl nepakankamų resursų jos ilgalaikiam palaikymui.

Darbo grupei buvo keliami du tikslai:

1. Įtraukti atsakingo spragų atskleidimo proceso apibrėžimą į Informacinių sistemų saugumo įstatymą
2. Pakeisti Baudžiamąjį kodeksą suteikiant teisines garantijas asmenims, vykdantiems veiklą pagal nustatytas atsakingo spragų atskleidimo proceso normas

ASAP įteisinimas – novatoriška ir reikalinga iniciatyva

Pasaulyje nėra ASAP įteisinusios valstybės, todėl neįmanoma atlikti lyginamosios teisės aktų analizės arba pritaikyti užsienio šalių praktikoje naudojamų įstatymų.
ASAP įteisinimas buvo grindžiamas Kibernetinio saugumo strategija, kurios 4.2 punkte įvardintas „prevencinių priemonių, kurios sumažintų kriminalinių nusikaltimų kiekį“ poreikis. ASAP įteisinimas prisidėtų prie šio punkto įgyvendinimo, nes tyrėjams būtų suteikta galimybė ieškoti spragų išvengiant teisinės atsakomybės.

Atsakingo spragų atskleidimo proceso etapai

Siekiant Informacinių sistemų saugumo įstatyme apibrėžti atsakingo spragų atskleidimo procesą (ASAP), buvo atliekamos konsultacijos su Latvijos IT ir ryšių sistemų saugumo ekspertais. Šių konsultacijų metu, buvo identifikuotos penkios ASAP sudedamosios dalys:

1. **KS spragos aptikimas.** Darbo grupė nustatė, kad aptikimo fazė prasideda „iš karto po aptikimo arba ne ilgiau kaip 5 dienos iki pranešimo“. Nuspręsta, kad „tyrėjas sustabdo aptikimo procesą surinkęs būtiną kiekį informacijos spragos patvirtinimui“. Svarbu: jeigu teisėsauga pradėtų tyrimą dėl įsilaužimo, tyrėjui nespėjus pranešti apie spragą, tyrėjas nebūtų atleistas nuo teisinės atsakomybės. Priimtas sprendimas, kad tyrėjams, aptikimo stadijoje naudojantiems „specialius įrankius arba programas“, nebūtų suteikiama galimybė išvengti teisinės atsakomybės.
2. **Pranešimas apie KS spragą.** Nustatyta, kad pranešimas turėtų būti teikiamas Latvijos Respublikos informacinių technologijų saugumo incidentų prevencijos institucijai (CERT). Nuspręsta pranešimo formą apibrėžti įstatymiškai.
3. **Pranešimo apie KS spragą verifikavimas.** Šis etapas prasideda pranešimą perdavus CERT ir baigiasi CERT jį patvirtinus arba paneigus. Patvirtinus spragos egzistavimo faktą, CERT apie tai praneša kibernetinio saugumo subjektui (KSS) bei spragą aptikusiam asmeniui. Laiko apribojimai verifikacijos procesui nustatyti nebuvo.
4. **Reagavimas į pranešimą apie KS spragą.** Toks reagavimas susideda iš keturių dalių
    a. CERT rekomendacijos dėl spragos pašalinimo
    b. KSS veiksmai dėl spragos pašalinimo
    c. KSS informuoja CERT per 90 dienų apie spragos pašalinimą
    d. CERT informuoja spragą aptikusį asmenį apie pasiektus rezultatus
5. **KS spragos atskleidimas.** Asmeniui, aptikusiam spragą, paliekama teisė informaciją apie šią spragą viešinti gavus CERT pranešimą apie spragos pašalinimą. Svarbu: nuspręsta, kad, „jeigu spragą aptikęs ir atsakingai apie ją pranešęs asmuo informaciją apie šią spragą viešina nesulaukęs informacijos iš CERT apie šios spragos pašalinimą ir keldamas grėsmę IT arba ryšių sistemų vientisumui arba prieinamumui, šiam asmeniui gresia teisinė atsakomybė“.

Kurk Lietuvai

Bandymas pakeisti Latvijos baudžiamąjį kodeksą

Siekdama ASAP įteisinimo, Latvijos Krašto apsaugos ministerijos sudaryta darbo grupė pateikė siūlymą pakeisti šalies baudžiamojo kodekso 241 (3) straipsnį, jį papildant tokia formuluote:

> „Asmeniui negrės teisinė atsakomybė jei bus nustatyta, kad asmuo veikė vadovaudamasis ASAP aprašymu bei atsakingai perdavė CERT pranešimą apie KS spragą sistemose, kuriose tvarkoma informacija susijusi su politiniu, kariniu, ekonominiu, socialiniu arba kitokiu valstybės saugumu“.

Latvijos Vidaus reikalų ministerijos ir policijos kritika:

- Ministerijos ir policijos atstovų teigimu, nebuvo atlikta pakankama išsami rizikos analizė, todėl ASAP įteisinimas galėtų sukelti netikėtas ir nenuspėjamas pasekmes.
- Abiejų institucijų atstovai išreiškė poziciją, kad palaikytų ASAP įteisinimą tik tuo atveju, jei į šio proceso aprašymą, asmenims, norintiems ieškoti KS spragų, būtų įtraukta registracijos prievolė. Institucijų teigimu, asmenims, ieškantiems KS spragų, neturėtų būti suteikta galimybė veikti anonimiškai.

Kurk Lietuvai

Jungtinės Amerikos Valstijos

Atsakingo atskleidimo iniciatyvos, tvarkos ir teisės aktai

Gynybos departamentas – atsakingo atskleidimo Jungtinėse Valstijose pradininkas

„Įsilaužimas į Pentagoną“ buvo pirmojo Jungtinių Valstijų gynybos departamento organizuojama tokio tipo iniciatyva skirta suteikti „etiniams hakeriams“ galimybę prisidėti prie visuomenei prieinamų Pentagono sistemų saugumo užtikrinimo. Iniciatyvos rėmuose teisėtai pamėginti įveikti Pentagono kompiuterinių sistemų apsaugą galėjo specialią biografijos patikrą perėję JAV piliečiai. „Etinius hakerius“ vienijanti organizacija „HackerOne“ prisidėjo prie šios iniciatyvos vykdymo ir kūrimo. 24 dienas trukusios pilotinės iniciatyvos metu, buvo identifikuotos 138 KS spragos. Pentagono skaitmeninės gynybos tarybos atstovai šį rezultatą įvertino kaip „viršijantį visus lūkesčius“, todėl buvo nuspręstą tokio pobūdžio KS spragų paieškas Gynybos departamente taikyti plačiau.

Kurk Lietuvai

Jungtinių Valstijų gynybos struktūros atsakingo atskleidimo iniciatyvas vykdo periodiškai

JAV gynybos departamento iniciatyva	Pradžia	Pabaiga	Aptikta spragų	Registruotų „etiniu hakerių“ skaičius	Išmokėtas atlygis (JAV doleriais)
Įsilaužimas į Pentagoną (angl. „Hack the Pentagon“)	2016/04/18	2016/05/12	138	1410	75 000
Įsilaužimas į JAV ginkluotąsias pajėgas (angl. „Hack the Army“)	2016/11/30	2016/12/21	118	371	100 000
Įsilaužimas į JAV karines oro pajėgas (angl. „Hack the Air Force“)	2017/05/30	2017/06/23	207	270	130 000
Įsilaužimas į JAV karines oro pajėgas 2.0 (angl. „Hack the Air Force 2.0“)	2017/12/09	2018/01/01	106	27	103 883
Įsilaužimas į JAV gynybos komandiruočių sistemą (angl. „Hack the Defense Travel System“)	2018/04/01	2018/04/29	100	19	80 000
Įsilaužimas į JAV karines jūrų pajėgas (angl. „Hack the Marine Corps“)	2018/08/12	2018/08/31	150	105	151 542
Įsilaužimas į JAV karines oro pajėgas 3.0 (angl. „Hack the Air Force 3.0“)	2018/10/19	2018/11/22	120	30	130 000

Kurk Lietuvai

Gynybos departamentas viešina spragų atskleidimo tvarką

Po sėkmingos „įsilaužimo į Pentagoną“ baigties, JAV gynybos departamentas paviešino oficialią spragų atskleidimo tvarką, kuri, JAV gynybos sekretoriaus Eštono Karterio teigimu, suteikia kompiuterių saugumo tyrėjams „legalų būdą prisidėti prie departamento kibernetinio saugumo“. Organizacijos „HackerOne“ duomenimis, nuo 2016 m. lapkričio mėn., kai departamentas paviešino minėtąją tvarką, nustatančią atsakingo atskleidimo taisykles, daugiau nei 600 KS tyrėjų atsakingai pranešė apie beveik 3000 KS spragų, iš kurių net 100 buvo pripažintos „kritinės reikšmės“.

Gynybos departamento KS spragų atskleidimo tvarka buvo parengta remiantis Jungtinių Amerikos Valstijų kodekso šešto skyriaus 1501(7) ir 1501(17) straipsniuose minimomis sąvokomis:

- Remiantis 6 U.S.C. 1501(7): „apsaugos priemonė“ yra „veiksmas, įrenginys, procesas, žymė, metodas arba kita priemonė“, kuri „aptinka, pašalina arba mažina žinomą arba įtariamą kibernetinio saugumo grėsmę arba saugumo spragą informacinėje sistemoje“.
- Remiantis 6 U.S.C. 1501(17): „saugumo spraga“ yra „bet kokia įrenginio, programinės įrangos, proceso arba procedūros savybė, kuri leidžia arba palengvina saugumo kontrolės anuliavimą“.

2016 m. lapkričio mėn. JAV gynybos departamentui paviešinus atskleidimo

600 KS tyrėjų

3000 pranešimų

100 kritinių spragų

Kurk Lietuvai

Gynybos departamento spragų atskleidimo tvarkoje nustatyti apribojimai:

KS spragų ieškantis asmuo privalo:

- Apsiriboti testavimu siekiant aptikti spragą arba su spraga susijusį rodiklį.
- Apsiriboti dalinimusi informacija apie spragą arba su spraga susijusiu rodikliu su Gynybos departamentu.
- Identifikuoti spragą pasitelkiant minimalius, šios spragos egzistavimo patvirtinimui reikalingus, veiksmus. Identifikavus spragą arba su spraga susijusį rodiklį draudžiama šią spragą išnaudoti arba vykdyti kenkėjišką veiklą.
- Vengti tyčinio priėjimo prie bet kokios Gynybos departamento informacinėse sistemose esančios informacijos, išskyrus tuos atvejus kai ši informacija yra tiesiogiai susijusi su spraga ir priėjimas prie informacijos yra būtinas siekiant įrodyti spragos egzistavimą.
- Jokiomis aplinkybėmis neperimti jokių duomenų.
- Nekelti pavojaus Gynybos departamento darbuotojų arba trečiųjų šalių privatumui ir saugumui.
- Nekelti pavojaus Gynybos departamento darbuotojų, subjektų arba trečiųjų šalių intelektinei nuosavybei ir kitiems komerciniams arba finansiniams interesams.
- Informacija apie spragą arba duomenis gautus išnaudojus spragą viešinti draudžiama, išskyrus tuos atvejus kai gaunamas rašytinis Gynybos departamento leidimas tokius duomenis viešinti.
- Nenaudoti DoS atkirtimo nuo paslaugos testavimo.
- Nenaudoti socialinės inžinerijos ir tikslingo internetinio sukčiavimo nukreipto prieš Gynybos departamento darbuotojus arba rangovus.
- Neteikti didelio kiekio prastos kokybės pranešimų
- Iškilus neaiškumams dėl tolimesnio testavimo, susisiekti su Gynybos departamento komanda.

Svarbu: spragų atskleidimo tvarkoje teigiama, kad „jeigu veikla, susijusi su saugumo tyrimu ir spragų atskleidimu, bus vykdoma pagal šios tvarkos nustatytus apribojimus“ JAV gynybos departamentas „nesiims ir nerekomenduos imtis teisinių veiksmų susijusių su minėta veikla“.

Atsakingą atskleidimą reglamentuojantys Jungtinių Valstijų teisės aktai

Kaip matoma lentelėje, Jungtinėse Valstijose šiuo metu yra keturi įstatymo projektai susiję su atsakingo KS spragų atskleidimo praktikos įteisinimu. Vienas iš jų, SAUGIŲ technologijų aktas (dokumento nr. H.R.7327), jau sulaukė Kongreso bei prezidento patvirtinimo ir tapo galiojančiu. Svarbu pabrėžti, kad dalis lentelėje matomų Įsilaužimo į vidaus saugumo departamentą akto (dokumento nr. S.1281) ir Privataus ir viešojo sektorių bendradarbiavimo kibernetinio saugumo srityje akto (dokumento nr. H.R.6735) formuluočių buvo perkeltos į įsigaliojusį SAUGIŲ technologijų aktą.

Dokumento Nr.	JAV įstatymo projektas	Pateikimo data	Statusas
S.1281	Įsilaužimo į vidaus saugumo departamentą aktas (angl. „Hack the Department of Homeland Security Act of 2018“)	2017/05/25	Patvirtintas Senato, perduotas Atstovų Rūmams
H.R.5433	Įsilaužimo į valstybės departamentą aktas (angl. „Hack Your State Department Act“)	2018/04/05	Patvirtintas Atstovų Rūmų, perduotas senatui
H.R.6735	Privataus ir viešojo sektorių bendradarbiavimo kibernetinio saugumo srityje aktas (angl. „Public-Private Cybersecurity Cooperation Act“)	2018/09/07	Patvirtintas Atstovų Rūmų, perduotas senatui
H.R.7327	SAUGIŲ technologijų aktas - Kibernetinių pajėgumų stiprinimas pasitelkiant rizikos atskleidimo technologijas aktas (angl. „Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act“ – „SECURE Technology Act“)	2018/12/19	Patvirtintas Kongreso ir Prezidento, galiojantis teisės aktas

Kertinės SAUGIŲ technologijų akto formuluotės

SAUGIŲ technologijų akte:

- Nustatyti reikalavimai JAV vidaus saugumo departamento spragų atskleidimo tvarkai (angl. „vulnerability disclosure policy“)
- Nustatytas „premijų už spragas programos“ (angl. „bug bounty program“) sąvokos apibrėžimas
- Numatyta įpareigoti JAV vidaus saugumo departamentą per 90 dienų parengti atsakingo KS spragų atskleidimo tvarką
- Numatyta įpareigoti JAV vidaus saugumo departamentą per 180 dienų parengti premijų už spragas programą

Jungtinių Valstijų valstybės departamento spragų atskleidimo tvarka:

Senato priimtame Įsilaužimo į valstybės departamentą akte (dokumento nr. H.R.5433) Jungtinių Valstijų valstybės departamentui buvo numatyti panašūs reikalavimai į tuos, kurie šiuo metu jau keliami JAV vidaus saugumo departamentui. Šiam teisės aktui įsigaliojus, valstybės sekretoriui bus pavesta paruošti atsakingo spragų atskleidimo programos gaires ir procesus, suteikiančius saugumo tyrėjams galimybę legaliai pranešti apie spragas valstybės departamento sistemose.

SAUGIŲ technologijų akte įteisintos sąvokos

Remiantis įsigaliojusiu H.R.7327 SAUGIŲ technologijų aktu, premijų už spragas programa yra iniciatyva, pagal kurią:

a. „Asmenims, organizacijoms arba įmonėms suteikiama laikina galimybė JAV vidaus saugumo departamento atitinkamose informacinėse sistemose identifikuoti spragas ir apie jas pranešti“
b. „Tinkami asmenys, organizacijos arba įmonės gauna kompensaciją už tokius pranešimus“

Remiantis įsigaliojusiu H.R.7327 SAUGIŲ technologijų aktu, spragų atskleidimo tvarka:

a. „galioja asmenims, organizacijoms arba įmonėms pranešančioms apie saugumo spragas atitinkamose vidaus saugumo departamento informacinėse sistemose“
b. nustato „atitinkamas departamento informacines sistemas, kuriose asmenims, organizacijoms arba įmonėms leidžiama ieškoti spragų“
c. nustato „sąlygas ir reikalavimus pagal kuriuos asmenys, organizacijos arba įmonės gali veikti ieškodamos saugumo spragų ir apie jas pranešdamos“
d. nustato „kaip asmenys, organizacijos arba įmonės gali atskleisti departamentui spragas, aptiktas atitinkamose departamento informacinėse sistemose“
e. nustato „kaip departamentas gali susisiekti su asmenimis, organizacijomis arba įmonėmis pranešusiomis apie saugumo spragas“
f. nustato „procesą, kuriuo vadovausis departamentas viešai atskleisdamas saugumo spragas apie kurias buvo pranešta“

Teisingumo departamentas viešina atsakingo atskleidimo programos kūrimo gaires

2017 m. liepos mėnesį JAV teisingumo departamento baudžiamasis padalinys paruošė ir paviešino Spragų atskleidimo programos internetinėms sistemoms gaires (angl. A Framework for a Vulnerability Disclosure Program for Online Systems). Šiame dokumente buvo nustatyti ir detaliai aprašyti keturi žingsniai, kuriais JAV kibernetinio saugumo subjektai gali vadovautis kurdami savo atsakingo KS spragų atskleidimo programas:

1. Spragų atskleidimo programos kūrimas
2. Spragų atskleidimo programos administravimas
3. Spragų atskleidimo tvarkos paruošimas siekiant tiksliai apibrėžiant organizacijos tikslus
4. Spragų atskleidimo programos vykdymas

„Etiniai hakeriai“ ir KS paslaugas teikiančios kompanijos

Bendradarbiavimo veikimo modelis ir atsakingo atskleidimo tvarkos taikymas

Atvejo analizė: „HackerOne“

„Etiniai hakeriai“ yra KS spragų ieškantys asmenys bei IT ir ryšių sistemų saugumo tyrėjai siekiantys prisidėti prie bendros kibernetinio saugumo situacijos gerinimo. Kibernetinio saugumo paslaugas teikiančios tarptautinės kompanijos, tokios kaip „HackerOne“, „Synack “ ir „Bugcrowd“ grindžia savo verslo modelį „etinių hakerių“ veikla.

„HackerOne“ yra privati kompanija vienijanti daugiau nei 200 000 „etinių hakerių“ ir yra viena didžiausių tokio tipo organizacijų pasaulyje. Šios kompanijos pagrindinis tikslas – tarpininkauti tarp viešojo ir privataus sektorių kibernetinio saugumo subjektų (KSS) ir „etinių hakerių“. Štai kaip atrodo šios kompanijos veiklos modelis:

1. Viešojo arba privataus sektoriaus kibernetinio saugumo subjektas sudaro sistemų saugumo testavimo sutartį su „HackerOne“
2. „HackerOne“ atstovai padeda kibernetinio saugumo subjektui parengti organizacijos tikslus atspindinčią spragų atskleidimo tvarką
3. „Etiniai hakeriai“ registruojasi „HackerOne“ platformoje, kurioje yra akredituojami ir reitinguojami
4. Registruotiems „etiniams hakeriams“ suteikiama galimybė ieškoti KS spragų „HackerOne“ klientų valdomose IT arba ryšių sistemose
5. Aptikus spragas „HackerOne“ klientų IT arba ryšių sistemose, „HackerOne” koordinuoja šių spragų atsakingą atskleidimą ir pašalinimą
6. Asmenims, aptikusiems KS spragas ir prisidėjusiems prie atsakingo jų atskleidimo, išmokamos premijos („bug bounty“)

bugcrowd

Synack

hackerone

Atsakingo atskleidimo tvarkos (AAT) taikymo paplitimas

Žurnalas „Forbes“ kasmet sudaro 2000 didžiausių pasaulio privataus sektoriaus organizacijų sąrašą. Iš šių organizacijų:

120
taiko atsakingo atskleidimo tvarką

14%
5 iš 36 koncernų („General Electric“, „Siemens“, „Honeywell International“, „ABB“, „Phillips“) taiko AAT

8%
2 iš 34 avialinijų („United Airlines“, „Lufthansa“) taiko AAT

10%
3 iš 31 automobilių ir sunkvežimių gamintojų („General Motors“, „Tesla“, „Fiat Chrysler Automobiles“) taiko AAT

1
„Starbucks“ yra vienintelis „Forbes“ sąraše esantis restoranas taikantis AAT

54%
didžiausių IT sprendimus kuriančių kompanijų taiko AAT

15%
3 iš 20 finansinių paslaugų teikėjų („Visa“, „MasterCard“, „PayPal“) taiko AAT

9%
6 iš 64 pasaulio didžiausių bankų („JPMorgan Chase“, „Citigroup“, „ING Group“, „Danske Bank“, „Swedbank“, „Royal Bank of Scotland“) taiko AAT

Išvados

Nyderlandų Nacionalinis kibernetinio saugumo centras viešina du oficialius, tačiau teisinės galios neturinčius, rekomendacinio pobūdžio dokumentus, kuriuose apibrėžiamos atsakingo atskleidimo proceso sąvokos, nustatoma proceso eiga bei jame dalyvaujančių šalių teisės ir pareigos.

Minėtuose dokumentuose, Nyderlandų privataus sektoriaus organizacijos skatinamos ruošti ir skelbti organizacijos tikslus ir lūkesčius atitinkančias atsakingo atskleidimo tvarkas, pateikiami tokių tvarkų pavyzdžiai.

Nyderlandų Nacionalinis kibernetinio saugumo centras viešina atsakingo atskleidimo tvarką, taikomą visoms centrinės valdžios IT arba ryšių sistemoms. 2017-2018 m. centras sulaukė 1140 pranešimų apie KS spragas.

Esant kreipimuisi į teisėsaugą, Nyderlandų prokuratūra atsižvelgia į atsakingo atskleidimo tvarkos egzistavimo faktą. Tais atvejais kai tokios tvarkos nėra, prokuratūra, savo paviešintose veiklos gairėse, teigia, kad atsižvelgia į spragą aptikusio asmens veiksmų suderinamumą su atsakingo atskleidimo praktika.

Išvados

Latvijos Krašto apsaugos ministerija sudarė darbo grupę, kuriai buvo pavesta parengti įstatymo pakeitimus įteisinančius atsakingo spragų atskleidimo procesą.

Latvijoje buvo siekiama įtraukti atsakingo spragų atskleidimo proceso apibrėžimą į Informacinių sistemų saugumo įstatymą bei pakeisti Baudžiamąjį kodeksą, suteikiant teisines garantijas asmenims, vykdantiems veiklą pagal nustatytas atsakingo spragų atskleidimo proceso normas.

Konsultacijų su Latvijos IT ir ryšių sistemų saugumo ekspertais metu, buvo identifikuoti 5 atsakingo spragų atskleidimo proceso etapai:

1. KS spragos aptikimas
2. Pranešimas apie KS spragą
3. Pranešimo apie KS spragą verifikavimas
4. Reagavimas į pranešimą apie KS spragą
5. KS spragos atskleidimas

Nuspręsta, kad pranešimai apie KS spragas turėtų būti teikiami Latvijos Respublikos informacinių technologijų saugumo incidentų prevencijos institucijai (CERT), kuri, patvirtinus arba atmetus pranešimą, koordinuotų tolimesnio proceso eigą.

Latvijos Vidaus reikalų ministerijos ir policijos atstovų teigimu, atsakingo spragų atskleidimo proceso įteisinimas būtų įmanomas, jeigu įstatymo pakeitimuose būtų numatyta registracijos prievolė asmenims norintiems ieškoti KS spragų.

Išvados

„Įsilaužimas į Pentagoną“ buvo pirmoji JAV organizuojama premijų už atrastas KS spragas iniciatyva skirta suteikti registruotiems „etiniams hakeriams“ galimybę prisidėti prie visuomenei prieinamų viešojo sektoriaus sistemų saugumo. JAV jau vyko 7 panašios iniciatyvos.

2018 m. JAV vidaus saugumo departamentas buvo įstatymiškai įpareigotas parengti atsakingo atskleidimo tvarką. Planuojama įpareigoti tokią tvarką parengti ir JAV valstybės departamentą.

JAV gynybos departamentas viešina atsakingo atskleidimo tvarką, kurioje nurodoma, kad departamento atstovai nesiims teisinių veiksmų prieš asmenį, atskleidusį KS spragą pagal departamento nustatytą tvarką.

Jungtinėse Valstijose šiuo metu yra keturi įstatymo projektai susiję su atsakingo KS spragų atskleidimo praktikos įteisinimu.

JAV įstatymai apibrėžia šias, su atsakingu atskleidimu susijusias, sąvokas:

1. Premijų už spragas programa
2. Spragų atskleidimo tvarka
3. Apsaugos priemonė
4. Saugumo spraga

JAV teisingumo departamentas viešina atsakingo atskleidimo programos kūrimo gaires taikomas privataus ir viešojo sektoriaus kibernetinio saugumo subjektams.

Kibernetinio saugumo paslaugas teikiančios tarptautinės kompanijos, tokios kaip „HackerOne“, „Synack “ ir „Bugcrowd“ grindžia savo verslo modelį „etinių hakerių“ veikla. Šių kompanijų pagrindinis tikslas – tarpininkauti tarp viešojo ir privataus sektorių kibernetinio saugumo subjektų ir „etinių hakerių“.

Atsakingo atskleidimo tvarką taiko 120 iš 2000 didžiausių pasaulio kompanijų, patenkančių į žurnalo „Forbes“ sąrašą. Labiausiai atsakingo atskleidimo tvarką taikyti linkusios yra IT sprendimus kuriančios kompanijos.

Šaltiniai

https://www.cyberscoop.com/bug-bounty-programs-hackerone-public-companies/
https://www.wired.com/story/hack-the-pentagon-bug-bounty-results/
https://www.govinfo.gov/app/details/USCODE-2015-title6/USCODE-2015-title6-chap6-subchapI-sec1501
https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/
https://www.hackerone.com/blog/Hack-The-Army-Results-Are-In
https://www.hackerone.com/disclosure-guidelines
https://www.afcea.org/content/Blog-defense-department-launches-hack-army-bug-bounty-program
https://www.hackerone.com/blog/Best-Yet-Come-DOD-Awards-New-Hack-Pentagon-Contract-HackerOne
https://www.fedscoop.com/hack-the-air-force-3-results-hackerone/
https://www.justice.gov/criminal-ccips/page/file/983996/download
https://www.cyberscoop.com/doj-vulnerability-disclosure-program-cfaa-bug-bounty/
https://www.iiotconnection.com/congress-passes-cyber-supply-chain-security-legislation/
https://www.congress.gov/bill/115th-congress/house-bill/7327
https://www.congress.gov/bill/115th-congress/house-bill/5433
https://www.congress.gov/bill/115th-congress/house-bill/6735
https://www.congress.gov/bill/115th-congress/senate-bill/128

Šaltiniai

https://www.hackerone.com/product/overview
https://www.sciencedirect.com/science/article/pii/S0267364917303606
https://www.youtube.com/watch?v=6xjPryrjH3c
https://cert.lv/en
https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/news/responsible-disclosure-guideline/1/Responsible%2BDisclosure%2BENG.pdf
https://www.enisa.europa.eu/news/member-states/coordinated-vulnerability-disclosure-guidelines-published-by-ncsc
https://www.enisa.europa.eu/news/member-states/WEB_115207_BrochureNCSC_EN_A4.pdf
https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure
https://www.ncsc.nl/english/security
https://www.holland-controls.com/responsible-disclosure
https://www.knb.nl/english/responsible-disclosure
https://www.thehaguesecuritydelta.com/responsible-disclosure
https://www.ceps.eu/system/files/CEPS%20TFRonSVD%20with%20cover_0.pdf
https://www.cio-platform.nl/l/en/library/download/urn:uuid:23494658-bba3-4422-9b96-bb14fa2418af/ciopublicatie2016+ceginfosec+coordinated+vulnerability+disclosure+policy+and+procedure+-+eng+v1.0.pdf?format=save_to_disk&ext=.pdf