REKOMENDACIJOS
DĖL VIEŠŲJŲ ELEKTRONINIŲ RYŠIŲ PASLAUGŲ IR TINKLŲ SAUGUMO UŽTIKRINIMO

ĮVADAS

1. Saugumo supratimas nuolat kinta šiandieniame informacinių technologijų pasaulyje. Saugumo politika turėtų apimti organizacines bei technines apsaugos priemones ir turėtų būti nuolatos tikslinama bei remtis LST ISO/IEC 17799: 2002 standartu. Standartinės darbo procedūros turėtų būti nuolat atnaujinamos atsižvelgiant į technologijų ir verslo vystymąsi.

2. Šis dokumentas dėl viešųjų elektroninių ryšių paslaugų ir tinklų saugumo užtikrinimo yra rekomendacinio pobūdžio ir yra skirtas viešųjų elektroninių ryšių paslaugų teikėjams (toliau – paslaugų teikėjai), viešųjų ryšių tinklų tiekėjams (toliau – tinklų tiekėjai), abonentams ir faktiniams elektroninių ryšių paslaugų naudotojams (toliau – paslaugų naudotojai).

3. Šių Rekomendacijų tikslas – supažindinti paslaugų teikėjus ir tinklų tiekėjus, abonentus ir paslaugų naudotojus su galimomis asmens privatumo pažeidimo grėsmėmis, pateikti metodinius nurodymus dėl naudotinų apsaugos priemonių.

BENDROSIOS NUOSTATOS

4. Lietuvos Respublikos elektroninių ryšių įstatymo (Žin., 2004, Nr. 69-2382) (toliau – Elektroninių ryšių įstatymas) 62 straipsnio 1 dalis nustato, kad „viešųjų elektroninių ryšių paslaugų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų paslaugų saugumui užtikrinti, o prireikus – kartu su viešųjų ryšių tinklų teikėjais imtis tokių pat priemonių viešųjų ryšių tinklų saugumui užtikrinti. Šios priemonės turi užtikrinti iškilusią grėsmę atitinkantį saugumo lygį“. Tai yra, atsižvelgiant į naujausius technikos laimėjimus, paslaugų teikėjų pasirinktos priemonės turi užtikrinti tokį saugumo lygį, kuris atitiktų atsiradusią riziką.

5. Elektroninių ryšių įstatymo 62 straipsnio 2 dalis numato, kad „iškilus ypatingai elektroninių ryšių tinklo ar jo dalies saugumo pažeidimo grėsmei, viešųjų elektroninių ryšių paslaugų teikėjas privalo informuoti abonentus apie tokią grėsmę ir tais atvejais, kai paslaugų teikėjo taikomos priemonės nepanaikina grėsmės kilmės priežasčių, taip pat informuoti abonentus apie visas įmanomas gelbėjimo priemones ir nurodyti tikėtinas jų kainas“. Paslaugų teikėjai, jeigu reikia – kartu su tinklo tiekėju turėtų imtis tinkamų priemonių savo paslaugų saugumui užtikrinti ir pranešti abonentams apie kiekvieną galimą tinklo saugumo pažeidimo riziką. Tokia rizika pirmiausia gali kilti atviruoju tinklu, pavyzdžiui, internetu arba analoginiu viešuoju judriuoju telefono ryšio tinklu teikiamoms elektroninių ryšių paslaugoms.

Tinklo tiekėjai ir paslaugų teikėjai turi imtis visų prieinamų techninių ir organizacinių priemonių, kad užtikrintų jų tinklo, paslaugų ir surinktų bei perduodamų duomenų fizinį ir loginį saugumą, išvengtų neleistino neįgaliotų naudotojų prisijungimo arba pranešimų turinio perėmimo.

6. Itin svarbu, kad paslaugų teikėjas abonentus ir paslaugų naudotojus išsamiai informuotų apie galimą grėsmę, kurios pašalinti jis nepajėgia. Paslaugų teikėjai, siūlantys viešai prieinamas elektroninių ryšių paslaugas internetu, turėtų informuoti abonentus ir naudotojus apie tai, kokiomis priemonėmis abonentai ir paslaugų naudotojai galėtų apsaugoti savo pranešimus, pavyzdžiui, apie specialią šifravimo techniką, padedančią apsaugoti elektroninių pranešimų konfidencialumą ir vientisumą. Reikalavimas pranešti abonentams ir paslaugų naudotojams apie konkrečią riziką saugumui neatleidžia paslaugų teikėjo nuo įsipareigojimo savo lėšomis imtis tinkamų ir skubių priemonių, kad pašalintų bet kokią naują, nenumatytą riziką saugumui ir atkurtų normalų paslaugos saugumo lygį.

7. Informacija abonentui ar paslaugų naudotojui apie riziką saugumui turėtų būti teikiama nemokamai, išskyrus nominalias išlaidas, kurias abonentas ar paslaugų naudotojas gali patirti gaudamas ir rinkdamas informaciją, pavyzdžiui, atsisiųsdamas elektroninio pašto pranešimą.

PASLAUGŲ TEIKĖJAMS IR TINKLŲ TIEKĖJAMAS REKOMENDUOJAMOS BENDROSIOS ORGANIZACINĖS PRIEMONĖS

8. Tinklų tiekėjai ir paslaugų teikėjai, tvarkantys srauto duomenis, turėtų patvirtinti elgesio taisykles, saugaus duomenų tvarkymo taisykles ar kt., kurių tikslas būtų užkirsti kelią neteisėtam duomenų tvarkymui.

9. Tinklų tiekėjai ir paslaugų teikėjai elektroninių duomenų bazėse turėtų įdiegti apsaugos sistemas, kurios neleidžia prieiti prie duomenų asmenims, kurie neturi teisės tokią informaciją gauti.

10. Paslaugų teikėjai turėtų surinkti ir saugoti tik tuos srauto duomenis, kurie yra reikalingi paslaugoms teikti arba kurie yra reikalingi įrodymui šių paslaugų teikimo bei jų apmokestinimui.

11. Atkreiptinas dėmesys į Elektroninių ryšių įstatymo 64 straipsnio 5 dalį, pagal kurią tvarkyti srauto duomenis turi teisę tik tinklų tiekėjų ir paslaugų teikėjų įgalioti asmenys, tvarkantys apskaitą, valdantys srautą, teikiantys informaciją abonentams ar paslaugų naudotojams, kovojantys su pažeidimais bei apgavystėmis, vykdantys paslaugų teikėjo elektroninių ryšių paslaugų rinkodarą ar teikiantys pridėtinės vertės paslaugas. Šie darbuotojai turėtų pasirašyti konfidencialumo pažymėjimus ir būti pasirašytinai supažindinami su šių Rekomendacijų 8 punkte paminėtomis taisyklėmis.

12. Teisė susipažinti su informacija, kuri negali būti viešai platinama, turėtų būti suteikta asmenims, kuriems dėl jų vykdomų funkcijų tokia informacija yra būtina jų pareigų vykdymui.

Organizacijoje turi būti paskirti darbuotojai, kurie turi prieigos prie duomenų teisę. Tinklų tiekėjai ir paslaugų teikėjai turėtų užtikrinti pakankamas prieigos prie duomenų kontrolės priemones ir informuoti savo darbuotojus apie būtinybę jų laikytis.

13. Tinklų tiekėjai ir (ar) paslaugų teikėjai turėtų tinkamai informuoti abonentus ir paslaugų naudotojus apie konkrečias asmens duomenų, kurie apie juos yra renkami ir tvarkomi, kategorijas, įstatyminę šiuos veiksmus reglamentuojančią bazę, kokiais tikslais šie duomenys yra renkami ir tvarkomi, šių duomenų panaudojimą bei saugojimo terminus.

14. Asmens duomenų perdavimas tarp tinklo operatorių ir paslaugų teikėjų leidžiamas tuo atveju, kai tai būtina operacijų vykdymui arba sąskaitų išrašymui.

15. Paslaugų teikėjai turėtų savo abonentus bei paslaugų naudotojus supažindinti su iškylančiomis grėsmėmis bei saugumo galimybėmis, informuoti apie taikomas naujausias technologijas.

PASLAUGŲ TEIKĖJAMS IR TINKLŲ TIEKĖJAMAS REKOMENDUOJAMOS BENDROSIOS TECHNINĖS PRIEMONĖS

16. Paslaugų teikėjai ir tinklų tiekėjai turėtų naudoti tinkamas procedūras ir turimas technologijas, pageidautina sertifikuotas, skirtas asmenų privatumo apsaugai, ypač užtikrindami duomenų apsaugą nuo neteisėto tvarkymo, taip pat fizinę ir loginę viešųjų tinklo ir šiuo tinklu teikiamų paslaugų apsaugą.

17. Paslaugų teikėjai turėtų informuoti naudotojus apie su interneto naudojimu susijusią riziką prieš jiems tampant paslaugų abonentais ar pradedant naudotis paslaugomis. Rizika gali būti susijusi su duomenų apsauga, tinklo saugumu ar kitokia privatumui keliama rizika, pavyzdžiui, slaptas duomenų rinkimas, įrašymas ir kiti veiksmai.

18. Paslaugų teikėjai turėtų informuoti abonentus ir paslaugų naudotojus apie technines priemones, kuriomis jie galėtų teisėtai naudotis, norėdami sumažinti duomenų ir susirašinėjimo saugumui kylančią riziką, pavyzdžiui, šifravimą ar elektroninį parašą. Siūlomos techninės priemonės turėtų būti prieinamos už abonentui ir paslaugų naudotojui priimtiną kainą.

19. Viešųjų ryšių tinklų ir paslaugų teikimo sistemos turėtų būti naudojamos taip, kad reikalingas asmens duomenų kiekis būtų griežtai apribotas iki minimumo. Kiekviena veikla, kuria siekiama teikti kitokias viešąsias elektroninių ryšių paslaugas, negu pranešimo perdavimas ir sąskaitų už tai pateikimas, turi būti grindžiama tik apibendrintais srauto duomenimis, pagal kuriuos neįmanoma nustatyti abonento ar naudotojo asmens tapatybės.

20. Paslaugų teikėjai turėtų informuoti vartotojus apie programas, leidžiančias anonimiškai vykdyti paieškas ir naršyti po internetą.

21. Elektroninis paštas šiuo metu pakeičia tokias tradicines ryšių priemones, kaip teleksas ir laiškai, tačiau skiriasi nuo tradicinių ryšių priemonių savo sparta, pranešimų sandara, oficialumo laipsniu ir pažeidžiamumu dėl nesankcionuotų veiksmų. Interneto paslaugų teikėjai, ypač žiniatinklio WEB pašto paslaugų teikėjai, turėtų siūlyti galimybę pritaikyti šifravimo lygį. Taip pat neturėtų būti draudžiama pseudoniminė ar anoniminė prieiga prie viešų paslaugų.

22. Elektroninio pašto paslaugų teikėjai turėtų numatyti, kokių reikia kontrolės metodų, kad būtų sumažinta elektroninio pašto sukeliama rizika saugumui. Saugumui rizika kyla dėl šių priežasčių :

a) pranešimai tampa pažeidžiami dėl nesankcionuotos kreipties, paslauga modifikuojama arba paneigiama;

b) pažeidžiamumas dėl klaidų, pavyzdžiui, neteisingo adreso;

c) ryšių terpės pokyčio įtaka elektroninio pašto veiklai, pavyzdžiui, padidėjusi pranešimų sparta arba padidėjęs perduodamų pranešimų perdavimo kiekis, kuriuos sukelia tam tikrų modifikacijų elektroninio pašto virusai.

d) iš išorės prieinamų paskelbtų personalo sąrašų įtaka neprašytų komercinių pranešimų siuntimui.

23. Elektroninio pašto paslaugų teikėjai turėtų įgyvendinti technines saugumo priemones dėl elektroninio pašto naudojimo, įskaitant:

a) apsaugą nuo elektroninio pašto atakų, pavyzdžiui, virusų perėmimą;

b) elektroninio pašto priedų apsaugą.

24. Interneto svetainių, kuriose vyksta elektroninė prekyba ar teikiamos kitokios paslaugos, savininkai turi korektiškai save autentifikuoti, t.y. pateikti įrodymus, kad svetainės yra tas, kuo ir skelbiasi esančios (pvz., elektroniniai sertifikatai).

25. Elektroninių operacijų metu turėtų būti renkami tik tie asmens duomenys, kurie yra būtini operacijoms atlikti.

26. Elektroninių operacijų atlikimo metu sandorio konfidencialumo ir vientisumo užtikrinimui turėtų būti naudojamos šifravimo technologijos. Pavyzdžiui, paslaugų teikėjai turėtų naudoti pažangią Interneto saugumo sistemą, žinomą kaip Secure Socket Layer (toliau – SSL), siunčiamų duomenų kodavimo sistemą. Ši sistema iš esmės užtikrina perduodamos informacijos slaptumą, autentiškumą, vientisumą ir priėmimą, turi aukščiausią įmanomą saugumo lygį. Paslaugų naudotojas apie saugumo lygį turėtų būti informuojamas visuose tvarkymo etapuose. Pavyzdžiui, perduodant duomenis iš naudotojo įrangos į interneto svetainę, galima būtų naudoti automatines informacijos procedūras, esančias naršyklėje, pavyzdžiui, specifinių rakto ar pakabinamos spynos piktogramų pasirodymas, naudojant SSL ryšio saugumą užtikrinančius protokolus.

27. Visi naudotojų veiksmai bei duomenų pakeitimai turėtų būti registruojami tarnybinių stočių ar kompiuterinių sistemų istorijos žurnaluose: skaitymas, pakeitimas, trynimas, perdavimas, kopijavimas, administravimo veiksmai, vartotojų administravimas, spausdinimas, kita informacija. Pageidautina, kad istorijos žurnalo įrašų saugojimo trukmė būtų nurodyta įmonės duomenų saugos nuostatuose ar kitose dokumentuose.

28. Tinklų tiekėjai ir (ar) paslaugų teikėjai turėtų stebėti duomenų srautus ir nustatyti nukrypimus ar bandymus neteisėtai naudotis sistema, naudojant naujausios kartos kombinuotas įsibrovimų aptikimo sistemas (toliau – ĮAS).

29. Paslaugų teikėjai paslaugų saugumo užtikrinimui turėtų naudoti užkardų (anglų k. – Firewall) ir specialių filtrų (anglų k. – proxy) sistemas.

30. Paslaugų teikėjai turėtų naudoti labai patikimumas ir našias serverių sistemas, nenutrūkstamo maitinimo šaltinius, RAID (anglų k. – Redundant Array of Independent Disks) diskų masyvus.

31. Tinklo operatoriai ir paslaugų teikėjai, teikdami abonentams ir paslaugų naudotojams mobilių telefonų paslaugas, turėtų juos informuoti apie ryšių slaptumui kylančią riziką, kuri tenka besinaudojantiems viešuoju judriojo ryšio tinklu, ypač jeigu nenaudojamas kodavimas. Mobilių telefonų tinklų abonentams ir paslaugų naudotojams turi būti pasiūlytos kodavimo galimybės arba alternatyvios saugumo priemonės.

32. Tinklo operatoriai ir paslaugų teikėjai, teikdami trumpųjų žinučių (tolau – SMS) paslaugas mobilių telefonų naudotojams, turėtų uždrausti interneto portalų sujungimą su SMS centrais, kurie nekontroliuoja siuntėjo numerio. Pavyzdžiui, SMS centras neturi tokių galimybių arba yra taip sukonfigūruotas, kad portalo lankytojas, kuris siunčia žinutę gali nurodyti aplikacijai bet kokį numerį, kuris bus laikomas siuntėjo numeriu.

Gavėjas turi turėti galimybę bet kuriuo atveju nustatyti SMS centro (žr. message details), per kurį buvo gautas SMS pranešimas, numerį. Žinant, SMS centro numerį, galima susisiekti su to centro operatoriumi ir per jį sužinoti, kokia aplikacija išsiuntė tą žinutę, o aplikacijos savininkai turėtų atsakyti, koks registruotas portalo lankytojas tai padare. Tuo tikslu portalo savininkas turėtų registruoti portalo lankytojus, kurie siunčia SMS žinutes.

33. Paslaugų teikėjai, teikdami SMS paslaugas mobilių telefonų naudotojams, kartu su tinklo tiekėjais turėtų užtikrinti pakankamus tinklų resursus, kad visi abonentai gautų jiems siųstas žinutes.

34. Bevielių elektroninių ryšių tinklai (anglų k. – WLAN), pasižymintys tokiais privalumais kaip mobilumas, žemesnės įdiegimo kainos, tampa vis populiaresni. Tačiau atsiranda grėsmių, susijusių su bevielių technologijų naudojimu, ypač dėl to, kad radijo bangos atviros įsilaužimui, jeigu nėra imtasi tinkamų saugumo priemonių. Šios grėsmės apima: slaptą pasiklausymą, įveikimą bendrų užkardų ir elektroninio pašto filtravimą, kurie taip pat susiję su bendraisiais tinklais, vietos nustatymo duomenų bei kitų asmens duomenų, susijusių su abonentu ar paslaugos naudotoju, perėmimą, neteisėtą prieigą prie bendrųjų tinklų.

35. Bevielių elektroninių ryšių tinklų tiekėjai (toliau – bevielių tinklų tiekėjai) turėtų žinoti ir informuoti abonentus ir paslaugų naudotojus apie bevielių ir nešiojamų prietaisų (nešiojamieji kompiuteriai) techninę ir saugumo reikšmę.

36. Bevielių tinklų tiekėjai turėtų atlikti rizikos įvertinimą ir plėtoti saugumo politiką, prieš tai atsižvelgus į bevielio tinklo išsidėstymą, siekiant užtikrinti, kad jie galės valdyti bei mažinti riziką jų informacijos, sistemos veikimo ir veikimo nenutrūkstamumo atžvilgiu.

37. Siekiant garantuoti bevielių tinklų saugumą, bevielių tinklų tiekėjai turėtų sukurti saugumo valdymo metodus ir priemones.

38. Bevielio tinko tiekėjai turėtų informuoti naudotojus, kaip konfigūruoti bevielius prietaisus, siekiant užtikrinti aukštą saugumo lygį ir konfidencialumą.

39. Bevielių tinklų tiekėjai turėtų reguliariai tikrinti neatskiriamas saugumo savybes, pavyzdžiui, autentiškumo patvirtinimą ir šifravimą, kurios būdingos bevielėms technologijoms. Autentiškumo patvirtinimas turėtų būti pagrįstas didesne prieigos kontrole reguliariai keičiant slaptažodžius.

40. Jei bevieliu elektroninių ryšių tinklu yra siunčiami ypatingi duomenys, tuomet yra būtina didesnė apsauga, t. y. būtinas duomenų šifravimas.

PASLAUGŲ NAUDOTOJAMS REKOMENDUOJAMOS BENDROSIOS ORGANIZACINĖS IR TECHNINĖS SAUGUMO PRIEMONĖS

41. Kad paslaugų naudotojas netaptų nelegalaus tinklalapio lankymo auka, jis turi įsitikinti, jog svetainė, kurioje jis lankosi, yra legali. Tam paslaugų naudotojas turi nukopijuoti adresą interneto tinklalapio, kurį jis nori aplankyti, ir parašyti adreso lange. Šis būdas pasižymi tuo, kad paslaugų naudotojas mano, jog lankosi tikrame tinklalapyje, kai iš tiesų tai piktaviliškai sukurtas panašus puslapis. Tokia technika ypač pavojinga, kai imituojamas kurio nors banko puslapis. Internetiniai langai, kurie idealiai nukopijuoja gerai žinomų bankų puslapių apipavidalinimą ir funkcijas tampa vis dažnesni.

42. Paslaugų naudotojas turi įsitikinti, kad turi patikimą antivirusinę programą, kuri atsinaujina bent kartą per dieną. Tai apsaugos jo kompiuterį nuo specialių kodų, kol jis naršys internete. Yra begalės virusų, kurie gali įsibrauti į kompiuterį naršant internete. Kad tai padarytų, jie išnaudoja pažeidžiamas vietas ir pasilieka kompiuteryje paslaugų vartotojams to net neįtariant. Tai gali būti tiek specialūs kodai, tiek įvairūs Trojos virusai, sukurti asmeninės informacijos kopijavimui iš pažeistų kompiuterių.

43. Paslaugų naudotojas turėtų padidinti apsaugos zoną iki vidutinės arba aukštos. Tai jis gali padaryti puslapio, kuriame naudotojas lankosi įrankių juostoje.

44. Java Applets ir Java Scripts programinės priemonės taip pat gali sukelti pavojų. Taip pat dauguma programų naudotojo kompiuteryje, kurios atrodo visiškai nepavojingos, gali būti skirtos sistemos informacijos kopijavimui ir atsiuntimui naudotojams. Siekiant nuo to apsisaugoti, rekomenduojama apriboti įrankių juostas lange, kuriuo naudojamasi.

45. Kai paslaugų naudotojas dirba su internetu, jis turi pasitikrinti, ar visi veiksmai vyksta per apsauginį serverį. Yra keli būdai, kaip nustatyti tokių serverių tipus. Vienas iš jų – tai adresas, kuris yra viršutinėje lango skiltyje ir prasideda https://. Kitas – spynos arba rakto ikona, pasirodžiusi lange. Jeigu spyna užrakinta arba raktas sveikas (nesulaužytas), serveris yra saugus.

Viena iš grėsmių, su kuriomis susiduria paslaugų naudotojas naršydamas internete, yra programišiai, randantys priėjimą prie mažų tekstinių failų paslaugų naudotojų kompiuteriuose. Tam jie panaudoja puslapio, kuris yra lankomas, serverį. Tokiu būdu gauta informacija dažniausiai yra susieta su registracijos vardais ir slaptažodžiais, naršymo prioritetais.

46. Prieš parsisiųsdamas programą iš interneto, paslaugų naudotojas turėtų atkreipti dėmesį į pasirodžiusius interneto langus, kurie dažniausiai jie nepavojingi, tačiau būna tokių, kurie prašo leidimo įrašyti programą. Būtent tada paslaugų naudotojas gali įsileisti programą – šnipą į kompiuterį ar tinklą. ,,Spyware“ yra programa – šnipas, kuri patenka į kompiuterį nepastebėta, paslaugų vartotojui naršant internete. Paslaugų naudotojas, prieš įdiegdamas iš interneto parsisiųstą programą, turėtų perskaityti viską, kas parašyta pasirodžiusiame lange, ir įsitikinti, ar ten nėra įtartinų priedų.

47. Paslaugų naudotojas turėtų reguliariai tikrinti savo kompiuterį, naudodamasis antivirusine bei ,,anti-spyware“ programomis, kurios blokuoja bet kuriuos šnipų patekimo į kompiuterį kelius bei įspėja naudotoją, jeigu jis buvo ar yra šnipinėjamas. Naudotojas visuomet turėtų tikrinti failų, gautų elektroniniu paštu, plėtinius ir niekuomet neatidarinėti failų su galūne .exe. Juose dažniausiai būna programa – šnipas.

48. Paslaugų naudotojai, norintys apsaugoti savo privačią korespondenciją bei kitą neskelbtiną informaciją, turėtų naudoti šifravimo programą, iš kurių labiausiai paplitusi yra ,,Pretty Good Privacy“ (toliau – PGP**)**. Naudojant PGP, informacija apsaugoma nuo pakeitimų (PGP tuoj pat įspėja, jei nors viena laiško raidė skiriasi nuo siuntėjo parašyto originalo) bei garantuojama, kad laišką tikrai išsiuntė jį pasirašęs siuntėjas, kadangi tik jis vienas žino slaptąjį pasirašymo raktą.

Parengė:
Valstybinės duomenų apsaugos inspekcijos

Registro, IT ir ryšių skyriaus
vyr. specialistas (telekomunikacijų)
Zigmantas Medutis
2004-12-28
Atnaujino:
Valstybinės duomenų apsaugos inspekcijos
Informacijos ir technologijų
vyr. specialistas
Zigmantas Medutis
2005-04-20