

REKOMENDACIJOS DĖL PRIVATUMĄ STIPRINANČIŲ TECHNOLOGIJŲ

ĮVADAS

Sparčiai besivystančios informacinės technologijos pastaraisiais metais privertė kalbėti apie naujus žmonių bendravimo būdus – elektroninį paštą, elektroninę bankininkystę, elektroninę komerciją, elektroninį verslą ir net elektroninę visuomenę bei elektroninę vyriausybę. Visa tai neatsiejamai susiję su internetu ir pasauliniu voratinkliu WWW (World Wide Web). Tačiau šalia milžiniškų komunikavimo galimybių, didžiulės vertingiausios informacijos pasiūlos bei gausybės įvairiausių paslaugų, tenka kalbėti ir apie elektroninius nusikaltimus, elektronines vagystes ir kitokias veikas, kurios pažeidžia žmogaus teisę į privatų gyvenimą. Šiame kontekste ypač svarbūs yra asmens duomenų ir privatumo apsaugos klausimai. Galima kalbėti apie teisinius, psichologinius, organizacinius, technologinius ir kitokius privatumo apsaugos aspektus.

Asmens duomenų apsaugos teisinį reguliavimą reglamentuoja Asmens duomenų teisinės apsaugos įstatymas (toliau vadinama – ADTAI). Šių Rekomendacijų tikslas nėra teisinių asmens duomenų apsaugos aspektų aiškinimas, juo labiau, kad pasaulyje šioje srityje ryškėja dvi tendencijos. Europos Sąjungoje šią sritį reglamentuoja įstatymai, tuo tarpu JAV remiamasi pasitikėjimo bei savanoriškumo principais. Rekomendacijose siekiama duomenų subjektams ir duomenų valdytojams suprantamai aptarti privatumo apsaugos klausimus ir naujausių technologijų įtaką, užtikrinant asmens privatumo apsaugą.

Privatumo apsauga ir privatumą skatinančios technologijos (toliau – PST) šiose Rekomendacijose nagrinėjamos dviem aspektais:

1. PST naudojimas duomenų valdytojų veikloje.
2. PST naudojimas duomenų subjekto veikloje.

1 SKYRIUS. REKOMENDACIJOS DUOMENŲ VALDYTOJAMS

Kiekviena organizacija tvarkyti asmens duomenis automatinio būdu gali tik Vyriausybės nustatyta tvarka pranešusi Valstybinei duomenų apsaugos inspekcijai (toliau vadinama – Inspekcija), išskyrus ADTAI numatytus atvejus. Tačiau duomenų valdytojas, tvarkydamas asmens duomenis automatinio būdu arba tvarkydamas susistemintas duomenų rinkmenas, prisiima ir tam tikrus įsipareigojimus. Jis privalo užtikrinti asmens duomenų apsaugą. Pateikiame keletą rekomendacijų, kurios padės įgyvendinti šią prievolę.

1.1. *Pirma rekomendacija: Atidžiai susipažinkite su ADTAI ir įgyvendinkite visas duomenų saugos priemones*

Jūsų duomenų apsaugos plane ir nenutrūkstamos veiklos priemonių plane turi atsispindėti infrastruktūrinės priemonės (pastatai, techninė įranga), administracinės priemonės (darbo organizavimas, personalas, netikėtumų planavimas), techninės ir programinės priemonės (techninė įranga, programinė įranga), telekomunikacinės priemonės (techninė įranga, programinė įranga). Tinkamai parinktos ir įdiegtos apsaugos priemonės leis Jums apsaugoti nuo atsitiktinių objektyvių ir netyčinių subjektyvių aplinkybių rizikos, padės pašalinti veiksmų, susijusių su techninės ir programinės įrangos gedimu, padarinius, sumažins riziką, kylančią dėl darbuotojų klaidų bei neteisėtų tyčinių veiksmų. Su asmens duomenų apsaugos metodiniais nurodymais galite susipažinti Inspekcijos tinklalapyje www.ada.lt

1.2. Antra rekomendacija: Kompiuterizuotų darbo vietų apsaugai naudokite intelektualias (smart) korteles

Iš pirmo žvilgsnio intelektualiai (smart) kortelė labai panaši į kreditinę arba debetinę kortelę, tačiau ji neturi magnetinės juostelės. Visa informacija saugoma kortelėje.

Tokios kortelės privalumai:

- joje saugoma daugiau duomenų;
- ji apsaugota slaptažodžiu;
- ji gali įjungti mikroprocesorių, kuris atlieka tam tikrus procesus, pvz., šifravimą.

Kortelę galima naudoti kaip:

- saugią šifravimo raktų saugyklą;
- skaitmeninę pinigų saugyklą elektroninėje piniginėje;
- kortelė garantuoja saugumą viešuose interneto terminaluose, ekraniniuose telefonuose ir kompiuteriuose.

1.3. Trečia rekomendacija: Tinkamai apsaugokite savo organizacijos vietinį tinklą nuo išorės vartotojų

Paprasčiausias būdas apsaugoti organizacijos vidinį tinklą yra jungtis prie interneto per vadinamąją „ugnies užtvara“ („Firewall“).

Dar geriau, jeigu Jūs naudosite kombinuotą metodą ir kartu su „ugnies užtvara“ įsidięsite ir Proxy serverį. Jūs ne tik pagerinsite savo organizacijos tinklo saugumą, bet ir ženkliai paspartinsite darbą internete.

1.4. Ketvirta rekomendacija: Naudokite Virtualų privatų tinklą (toliau – VPT)

VPT sprendimai puikiai tinka šiuolaikiniam verslui: saugiai sujungia biurus skirtingose vietose, leidžia bendrauti su verslo partneriais, tiekėjais ir klientais, suteikia galimybę mobiliems darbuotojams per atstumą saugiai prisijungti ir naudotis visomis reikalingomis programinėmis funkcijomis.

VPT yra technologija, kurios pagalba sukuriamas saugus žinybinis tinklas, naudojantis viešuoju paslaugų teikėjų tinklu. Įmonės gali naudoti standartines skirtines linijas arba Frame Relay tinklą. VPT mechanizmas naudoja kryptuotą IP protokolą informacijai perduoti internetu. Standartiniai apsaugos protokolai ir mechanizmai (IPSec, PKI) užtikrina perduodamų duomenų pilnumą.

Siekiant, kad darbas su taikomosiomis programomis būtų saugiai perkeltas iš vietinio tinklo į VPT, jo sprendimas turi užtikrinti:

- suderinamumą – visi programiniai paketai ir protokolai turi veikti per VPT tinklą;
- saugumą – kompanijos vidinių IT resursų apsauga;
- valdymą – svarbiausias sistemos elementas, kuris tinklo administratoriui leidžia atlikti visas apsaugos, monitoringo ir administravimo funkcijas.

VPT technologijos privalumai:

- saugus prisijungimas prie interneto. Ypač aukšti apsaugos standartai: identifikacija, kodavimas ir „ugnies sienos“ funkcijos;
- nuotolinis prisijungimas prie vidinio tinklo. Galimybė dirbti namuose ar neturintiems pastovios darbo vietos;
- saugus nutolusių biurų sujungimas. Naudodama viešuosius tinklus, VPT technologija užtikrina tą pačią kokybę, kaip ir privatus nutolusių vietovių tinklas, o kaštai yra mažesni;
- saugus ekstranetas. Užtikrina patikimą bendravimą su klientais, partneriais ar tiekėjais.

1.5. *Penkta rekomendacija: Pirkdami ar kurdami informacinės sistemos programine įranga, įsitikinkite, kad joje įdiegtos naujausios PST*

Reikalaukite, kad produkto ar paslaugos tiekėjas pateiktų naudojamų PST sąrašą, pasiteiraukite, kokiais būdais užtikrinamas vartotojų anonimiškumas, ar naudojami pseudonimai? Gal galima naudoti elektroninį parašą arba biometrinius atpažinimo metodus ir techniką? Palyginkite šio produkto ar paslaugos tiekėjo ir kitų tiekėjų naudojamas PST. Nepasitikėkite tiekėju, kuris atmetinai žiūri į asmens duomenų apsaugą.

2 SKYRIUS. REKOMENDACIJOS DUOMENŲ SUBJEKTAMS

Kalbant apie duomenų subjekto privatumo apsaugą, tenka pripažinti, kad daugumoje atvejų privatumo saugojimas yra paties subjekto asmeninis reikalas. Nuo paties subjekto pozicijos ir požiūrio didžia dalimi priklauso jo privatumo užtikrinimas. Jeigu subjektas vardan patogumo, greičio ar laiko stokos aukoja savo privatumą, vargu ar padės ir pačios pažangiausios technologijos.

Internetas yra atviras pasaulinis tinklas, per kurį dalijamasi informacija, jungiamasi prie paprastų interneto puslapių, e-parduotuvių, perduodami nurodymai ir finansiniai pavedimai. Atrodo, kad vyksta tiesioginis bendravimas, tačiau taip nėra. Internete apie jo vartotojus yra surenkami milžiniški duomenų kiekiai, patiems vartotojams dažnai apie tai nieko nežinant. Jungiantis prie svetainės, svetainė surenka informaciją apie apsilankiusį interneto vartotoją. Svetainė taip pat žino IP adresą, iš kurio tinklalapio interneto vartotojas persikėlė. Informacija apie apsilankymus svetainėje paprastai yra saugoma ir gali būti naudojama informacijai kaupti apie srautus ir lankytojų veiklas. Todėl duomenų subjektams siūlome toliau pateikiamas rekomendacijas.

2.1. *Pirma rekomendacija: Susipažinkite su reikalavimais pateikti duomenis*

Įeidami į kiekvieną interneto puslapį, kuriame Jūsų prašo pateikti bet kokią informaciją apie asmenį arba registruotis, paskirkite keletą minučių ir atidžiai susipažinkite su reikalavimais pateikti asmens duomenis. Įsitikinkite, kad nėra renkami pertekliniai duomenys. Jeigu Jūs perkate knygą e-parduotuvėje, su šiuo procesu nesusiję duomenys neturėtų būti renkami. Parduotuvės neturėtų dominti Jūsų asmens kodas, išsilavinimas, tautybė ir panašiai. Pakaktų vardo, pavardės ir adreso kur pristatyti knygą. Patikrinkite, ar puslapyje yra nuoroda į skirsnį apie asmens duomenų apsaugą. Perskaitykite jį.

2.2. *Antra rekomendacija: Naudokite slapukų (cookies) ir „švyturėlių“ filtrus*

Interneto svetainėje yra papildomų galimybių rinkti informaciją, jeigu joje naudojami *slapukai*. Tai yra duomenų dalys, kurios gali būti saugomos tekstiniuose failuose, įrašomuose į interneto vartotojo kietąjį diską, o jų kopijos saugomos svetainėje. *Slapukai* yra standartinė *HTTP* srauto dalis ir todėl gali būti be kliūčių persiunčiami su IP srautu. *Slapukai* gali turėti unikalų numerį, kuris geriau susieja su asmeniu negu dinaminiai IP adresai. Tokie *slapukai* išplečia svetainių galimybę saugoti informaciją apie jų lankytojus. *Slapukas* gali būti reguliariai nuskaitomas svetainės, siekiant identifikuoti interneto vartotoją ir atpažinti jį/ją, kai jis/ji pakartotinai apsilanko, patikrinti galimus slaptažodžius, įrašyti ir analizuoti veiksmų eigą svetainėje seanso metu.

Filtravimo mechanizmas naudojamas visose populiariausiose interneto naršyklėse. Interneto vartotojas gali nustatyti vieną iš trijų *slapukų* filtravimo variantų:

- priimti kiekvieną *slapuką*;
- atmesti kiekvieną *slapuką*;
- pasiteirauti vartotojo kiekvienu konkrečiu atveju.

Labiausiai paplitusioje naršyklėje **Microsoft Internet Explorer** leidžiama turėti savas nuostatas kiekvienai iš 4 saugumo zonų: Internet (internetas), Local Intranet (vietinis intranetas), Trusted Sites (patikimos svetainės), Untrusted Sites (nepatikimos svetainės). Kiekvienai šių zonų galima nustatyti tam tikrą filtravimo variantą. Nuostatas galima rasti iš meniu Tools išrinkus Internet Options, po to spustelėjus žymelę Security. Kiekvienai zonai galima pasirinkti vartotojo lygmenį (Custom Level).

Tačiau *slapukų* uždraudimą sunku vertinti vienareikšmiškai, nes:

- *Slapukai* gali būti labai įvairaus pobūdžio: kai kurie *slapukai* yra naudingi ir neidentifikuojantys (pvz., pageidaujama kalba). Kiti yra identifikuojantys, tačiau gali būti naudojami laikantis konfidencialumo taisyklių. Galima teigti, kad *sesijos slapukai* mažiau kenkia konfidencialumui negu pastovūs, nuolatiniai *slapukai*. Interneto vartotojas tikriausiai nebūtų suinteresuotas atmesti visų *slapukų*.

- Kai kurios svetainės neleidžia į jas patekti vartotojams, kurie nenori priimti *slapukų*.

- Kai kurios svetainės (arba svetainės su nematomomis nuorodomis) siuntinėja daug *slapukų* ir, pasirinkus pasiteiravimo kiekvienu konkrečiu atveju variantą, interneto vartotojui reikės atmetinėti visus juos vieną po kito, o tai gali sukelti vadinamąjį „spragtelėjimų nuovargį“.

- Kai kuriais atvejais perspėjimo apie *slapukus* tekstas pasirodo esąs nepilnas ir gali suklaidinti vartotoją.

- Instaliuojant naują naršyklę, pirmoji svetainė, kurioje ketinama apsilankyti (paprastai tai automatiškai būna naršyklės programos gamintojo svetainė), gali atsiųsti *slapuką* dar prieš vartotojui suteikiant galimybę deaktyvuoti *slapukus*.

- *Slapukų* blokavimo mechanizmas neleidžia priimti naujų *slapukų*, tačiau neapsaugo nuo sisteminio ir nematomo jau gautų *slapukų* išsiuntimo.

- Paprastai daugumoje interneto naršyklių „pagal nutylėjimą“ yra nustatytas parametras „priimti visus *slapukus*“. Interneto vartotojas dažnai nežino, kad *slapukai* yra plačiai naudojami ir kokius jie kelia pavojus.

- Išjungus *slapukus*, švyturėliai ir toliau signalizuos apie apsilankymą svetainės puslapyje, tačiau pranešimų nebus galima susieti su *slapukų* informacija.

2.3. **Trečia rekomendacija:** Koduokite savo perduodamą informaciją

Kiekvienas duomenų subjektas nesunkiai gali užkuoduoti savo informaciją specialių programų pagalba. Tekstas, kurį galima skaityti nepanaudojus jokių specialių priemonių, vadinamas paprastu tekstu. Metodas, naudojantis paprastą tekstą ir paverčiantis jį gausybe nieko bendro tarp

savęs neturinčių simbolių, vadinamas šifravimu, o toks tekstas - užšifruotu tekstu. Pati šifravimo schema atrodytu maždaug taip:

-----	----->	/////	----->	-----
-				
paprastas	šifravimas	užšifruotas	iššifravimas	
paprastas				
tekstas		tekstas		tekstas

Kriptografija-tai mokslas, naudojantis matematikos metodus užšifruoti ir iššifruoti duomenims. Kriptografija leidžia saugoti ypač slaptą informaciją ir siųsti ją tokiais tinklais kaip internetas, taigi jos negali perskaityti niekas kitas, tik gavėjas.

Yra nusistovėjusi nuomonė, kad žmogus todėl šifruoja duomenis, kad daro kažką nelegalaus. Tačiau šiame informacijos amžiuje kiekviena gauta informacijos dalelytė gali būti panaudota prieš jus. Šifravimas yra taip pat labai svarbi elektroninės komercijos dalis. Norint įgyti klientų pasitikėjimą, turi būti užtikrintas jų duomenų saugumas.

Egzistuoja daugybė šifravimo algoritmų. Tai PGP, DES, RSA,MD5 ir kt. PGP (Pretty Good Privacy) yra stipriausia ir populiariausia šifravimo programinė įranga, leidžianti žmonėms keistis failais ir pranešimais, garantuojant informacijos saugumą. PGP pasižymi šiomis savybėmis:

- Pasinaudoti gauta informacija gali tik tas asmuo, kuriam ši informacija buvo skirta.
- Siunčiama informacija autentifikuojama: gavėjas informuojamas, kas iš tikrųjų siuntė pranešimą.
- Siuntimui nereikalingi saugūs kanalai.

Kriptografijos patikimumas priklauso nuo to, kiek laiko ir resursų bus sunaudota, norint iššifruoti tekstą. Patikima kriptografija yra kai užšifruotas tekstas, kurį labai sunku iššifruoti be specialaus iššifravimo įrankio.

Šifravimo algoritmas-tai matematinė funkcija, naudojama šifravimo ir iššifravimo procese. Algoritmo veikimui reikalingas slaptažodis. Slaptažodis gali būti žodis, numeris, frazė, įvairūs simboliai. To paties teksto užšifruoti skirtingais slaptažodžiais variantai skirsis vienas nuo kito. Taigi viso užšifruoto teksto saugumas priklausys nuo pasirinkto algoritmo ir slaptažodžio saugumo. Ankščiau, jei viena pusė norėjo nusiųsti įslaptintus duomenis kitai, turėjo pirma duomenis užšifruoti su raktu ir po to surasti būdą, kaip saugiai tą raktą nugabenti kitai pusei. Šią saugumo problemą išsprendė viešojo rakto kriptografija. Ji paremta tuo, kad yra sudaromi du raktai – viešas (naudojamas duomenims užšifruoti) ir privatus (naudojamas duomenims iššifruoti). Taigi jūs savo viešą raktą duodate kam tik panorėję, o privatą laikote saugiai (pvz., diske, CD-ROM ir t.t.). Žmonės, pasinaudoję Jūsų viešuoju raktu, užšifruos duomenis, kuriuos iššifruoti galėsite tik Jūs patys (pasinaudodami savo privačiu raktu).

PGP naudoja viešojo rakto kriptografiją. Prieš šifruodama duomenis, PGP programa suspaudžia (archyvuoja) tekstą. Tai svarbu saugumui: dauguma kriptanalizių panaudoja iškarpu sutapimą duomenų iššifravimui. Archyvuojant tekstą jis šiek tiek iškraipomas, taip sumažinamas tokio iššifravimo pavojus.

Rakto patikimumas priklauso ir nuo jo dydžio. Dydis matuojamas bitais. Pvz., 1028 bitų dydžio raktas laikomas labai dideliu. Viešojo rakto kriptografijoje kuo didesnis raktas, tuo saugesni duomenys.

Viešasis ir privatus raktai yra matematiškai susiję. Nustatyti privatą raktą turint tik viešąjį yra begalo sunku, tačiau, tai yra įmanoma. Todėl svarbu parinkti teisingą jūsų rakto dydį. Taip pat reikia numatyti, kas norės perskaityti Jūsų duomenis, ar labai jie tam pasiryžę, kiek laiko jie turi ir

maždaug kokius resursus jie gali panaudoti. Raktai yra užšifruoti ir saugomi dviejuose failuose jūsų diske. Šie failai vadinami viešas raktų žiedas („public keyring“) ir privatus raktų žiedas („private keyring“). Į viešą raktų žiedą galima dėti įvairių įmonių/žmonių viešuosius raktus. O į privatą žiedą - tik Jūsų privačius raktus. Jei prarasite savo privatą žiedą, nebegalėsite iššifruoti Jums skirtų duomenų.

Vienas didžiausių viešojo rakto kriptografijos privalumų yra galimybė sukurti savo skaitmeninį parašą. Tai užtikrina duomenų tikrumą ir patikimumą. Skaitmeninis parašas naudoja „maišymo“ („hash“) funkciją. Ši funkcija generuoja fiksuoto dydžio įrašą (pvz., 160 bitų) iš duotų duomenų. Įrašo dydis nepriklauso nuo duomenų dydžio. Funkcija atsakinga už duomenų patikimumo užtikrinimą. Pakitus nors vienam bitui, bus atkuriami visiškai kitokie duomenys.

Kol bus naudojama saugi maišymo funkcija, nėra jokios galimybės parašą suklastoti, nes patys menkiausi pakitimai sužlugdys autentiškumo procesą.

Kriptosistemose viešojo rakto trūkumas yra tas, kad žmogus turi būti tikras, jog šifruoja duomenis tikrojo gavėjo viešuoju raktu. Kitaip gali būti įvykdyta vadinamoji „žmogus viduryje“ (Man-in-the-middle) ataka—kitas asmuo pakiša jums savo viešąjį raktą, kuriame visa identifikacija atitinka Jūsų pažįstamo (ar šiaip partnerio) identifikaciją. Jūs nieko neįtardami tuo raktu užšifruojate slaptus duomenis. Tada kitam žmogui tereikia perimti šiuos duomenis ir iššifruoti.

Skaitmeniniai sertifikatai gali užtikrinti, kad viešasis raktas priklauso būtent tam žmogui. Sertifikatą galime įsivaizduoti kaip asmens pasą. Jūs jį turite saugoti, nes jums pametus pasą kitas žmogus gali apsimesti jumis.

PGP programas galima parsisiųsti iš <http://www.pgpi.com> svetainės.

2.4. ***Ketvirta rekomendacija: Naudokitės patikimomis naršyklėmis***

Patariame naudotis naršyklėmis, kurios palaiko 128 bitų SSL protokolą. SSL protokolas šiuo metu yra plačiausiai naudojamas metodas prekybinių sandėrių internete saugumui užtikrinti. SSL protokolas yra suderintas su dauguma tinklo serverių ir interneto naršyklių, pavyzdžiui, „Netscape Navigator“ bei „Microsoft Internet Explorer“.

SSL saugumą užtikrina keliomis charakteristikomis, kurios garantuoja jo tinkamumą elektroninės prekybos sandoriams internete:

- slaptumą garantuoja šifravimas, tačiau duomenys gali būti perimami trečiosios šalies, bet jų neįmanoma perskaityti, nes trečioji šalis neturi šifro rakto;
- duomenų vientisumas taip pat šifruojamas. Jeigu pranešimas gautas, bet neteisingai iššifruojamas, tuomet gavėjas žino, kad informacija perdavimo metu buvo sufalsifikuota;
- autentifikacija atliekama naudojant skaitmeninius sertifikatus. Jie yra saugių elektroninių sandorių pagrindas, nes identifikuoja sandorio dalyvius ir lengvai patikrina kitų dalyvių identifikaciją.


Norėdami įsitikinti, ar jūsų naršyklė palaiko 128 bitų SSL protokolą, galite nueiti į Microsoft Internet Explorer meniu Help>About. Raskite Cipher Strength eilutę. Joje esantis skaičius nurodo kodavimo rakto ilgį. Jei tas skaičius nelygus 128 (gali būti 40 ar 56), vadinasi jums reikia įdiegti priedą, kuris leis naudotis 128 bitų kodavimo raktu. Tai padaryti labai paprasta: paspaudę nuorodą Update Information, jūs pakliūsite į Microsoft svetainę, kur bus pasiūlyta atsisiųsti atitinkamą pataisą (dydis apie 150KB). Atsisiųskite ją ir įdiekite.

Įsitikinti, kad Jūsų pranešimai yra šifruojami ir perduodami saugiai, galite ir stebėdami naršyklės adreso eilutę:

NOT SECURE

Address:  http://www.paymybills.com

SECURE

Address:  https://www.paymybills.com

Naujausias naršyklių versijas jūs galite rasti:

- Microsoft interneto svetainėje: <http://www.microsoft.com/downloads/>
- Netscape interneto svetainėje: <http://www.netscape.com/download/>

2.5. Penkta rekomendacija: Naudokitės anonimiškumą užtikrinančiomis priemonėmis (anonymizers)

Šios priemonės užtikrina Jūsų anonimiškumą internete. Viena seniausių ir geriausių laikoma ANONYMIZER. Informacijos apie šią priemonę galite rasti puslapyje www.anonymizer.com. Galite pasinaudoti kanadietišku produktu FREEDOM arba kompanijos Bell Labs and AT&T Labs produktu CROWDS.

Siekiant anonimiškumo, galima naudotis ir tarpininkavimo (infomediary) produktais. Iš jų galima paminėti DigitalMe, Jotter, Lumeria ir kt.

2.6. Šešta rekomendacija: Saugokite ir dažnai keiskite savo slaptažodžius

Laikykitės pagrindinių saugių slaptažodžių sudarymo ir saugojimo principų.

Parengė:

Vaclovas Palubinskas
2003-07-22

Atnaujino:
Valstybinės duomenų apsaugos inspekcijos
Informacijos ir technologijų
vyr. specialistas
Zigmantas Medutis
2005-04-20