Elektroninės informacijos sauga: dokumentų apžvalga ir praktiniai patarimai LIMIS naudotojams

Donatas Snarskis

Lietuvos dailės muziejus

Nuotolinės paskaitos turinys

1) Elektroninės informacijos saugą reglamentuojančių teisės aktų ir dokumentų apžvalga;
2) Kibernetinių incidentų tipai;
3) Patarimai ir rekomendacijos LIMIS naudotojams.

Bendrieji teisės aktai

- Lietuvos Respublikos elektroninių ryšių įstatymas (Žin., 2004, Nr. 69-2382);
- Lietuvos Respublikos kibernetinio saugumo įstatymas (TAR, 2014, Nr. 2014-20553);
- Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas (Žin. 2011, Nr. 163-7739);
- Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Žin., 2008, Nr. 22-804);
- Lietuvos Respublikos vidaus reikalų ministro įsakymas „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ (Žin., 2013, Nr. 106-5251);
- Lietuvos vyriausiojo archyvaro įsakymas „Dėl elektroninių dokumentų valdymo taisyklių patvirtinimo“ (TAR, 2016, Nr. 2016-17170);
- Valstybinės duomenų apsaugos inspekcijos direktoriaus įsakymas „Dėl bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms patvirtinimo “(Žin. 2008, Nr. 135-5298).

LIMIS veikimą ir duomenų saugą reglamentuojantys dokumentai

- Lietuvos integralios muziejų informacinės sistemos (LIMIS) nuostatai (patvirtinti LDM direktoriaus 2013 m. lapkričio 22 d. įsakymu Nr. V.1-122);
- Lietuvos integralios muziejų informacinės sistemos (LIMIS) duomenų saugos nuostatai (patvirtinti LDM direktoriaus 2015 m. gruodžio 7 d. įsakymu Nr. V.1-98);
- Lietuvos integralios muziejų informacinės sistemos (LIMIS) veiklos tęstinumo valdymo planas (patvirtintas LDM direktoriaus 2016 m. rugsėjo 6 d. įsakymu Nr. V.-71);
- Lietuvos integralios muziejų informacinės sistemos (LIMIS) saugaus elektroninės informacijos tvarkymo taisyklės (patvirtintos LDM direktoriaus 2016 m. rugsėjo 6 d. įsakymu Nr. V.-71);
- Lietuvos integralios muziejų informacinės sistemos (LIMIS) naudotojų administravimo taisyklės (patvirtintos LDM direktoriaus 2016 m. rugsėjo 6 d. įsakymu Nr. V.-71);
- Asmens duomenų tvarkymo Lietuvos dailės muziejaus valdomoje ir tvarkomoje Lietuvos integralioje muziejų informacinėje sistemoje (LIMIS) taisyklės (patvirtintos LDM direktoriaus 2016 m. lapkričio 24 d. įsakymu Nr. V.1-99).

Pagrindinės sąvokos

- **LIMIS valdytojas ir tvarkytojas – Lietuvos dailės muziejus.** Svarbiausios funkcijos ir atsakomybės elektroninės informacijos saugos srityje:
  - rūpinasi LIMIS duomenų sauga, duomenų saugos teisės aktų plėtojimu ir įgyvendinimu;
  - prižiūri, kaip laikomasi LIMIS duomenų saugos reikalavimų;
  - užtikrina programinės įrangos ir į LIMIS perduotos elektroninės informacijos apsaugą;
  - administruoja LIMIS duomenų bazes;
  - stebi LIMIS veiklą ir sutrikus ją atkuria;
  - atsako už LIMIS informacijos tvarkymo teisėtumą ir informacijos saugą;
  - skiria LIMIS saugos įgaliotinį ir LIMIS administratorius;
  - registruoja LIMIS duomenų tvarkytojus ir LIMIS naudotojus;
  - organizuoja elektroninės informacijos registravimo ir teikimo mokymus LIMIS naudotojams.
- **LIMIS duomenų tvarkytojai (duomenų teikėjai)** – Lietuvos Respublikos **juridiniai asmenys (muziejai), sudarę sutartis su Lietuvos dailės muziejumi dėl darbo su LIMIS**, kaupiantys savo elektroninių katalogų duomenis LIMIS duomenų bazėse, viešinantys sklaidai skirtus duomenis LIMIS viešosiose prieigose ir teikiantys LIMIS saugomą skaitmeninį turinį į kitas duomenų bazes. LIMIS duomenų tvarkytojų sąrašas yra tvirtinamas ir periodiškai atnaujinamas Lietuvos dailės muziejaus direktoriaus įsakymu.
- **LIMIS naudotojai** – LIMIS duomenų **tvarkytojų paskirti darbuotojai**, kurie savo funkcijoms atlikti naudojasi LIMIS ištekliais.

LIMIS duomenų tvarkytojų funkcijos ir atsakomybė

- Paskiria savo institucijoje LIMIS naudotojus ir duomenis apie juos pateikia LIMIS-C administratoriui;
- Institucijose, kur yra įdiegtos LIMIS-M tarnybinės stotys, paskiria darbuotojus, atsakingus už LIMIS-M tarnybinių stočių priežiūrą ir jų tinkamą naudojimą;
- Užtikrina į LIMIS duomenų bazes pateikiamų duomenų tinkamą įvedimą, **duomenų teisingumą, saugumą ir konfidencialumą** savo įstaigoje ir saugų duomenų perdavimą kompiuterių tinklais (automatiniu būdu) į LIMIS duomenų bazes;
- Užtikrina LIMIS valdytojo ir tvarkytojo priimtų teisės aktų ir rekomendacijų įgyvendinimą;
- Teikia pasiūlymus LIMIS valdytojui ir tvarkytojui dėl duomenų saugos tobulinimo.

Organizaciniai ir techniniai reikalavimai LIMIS duomenų tvarkytojams

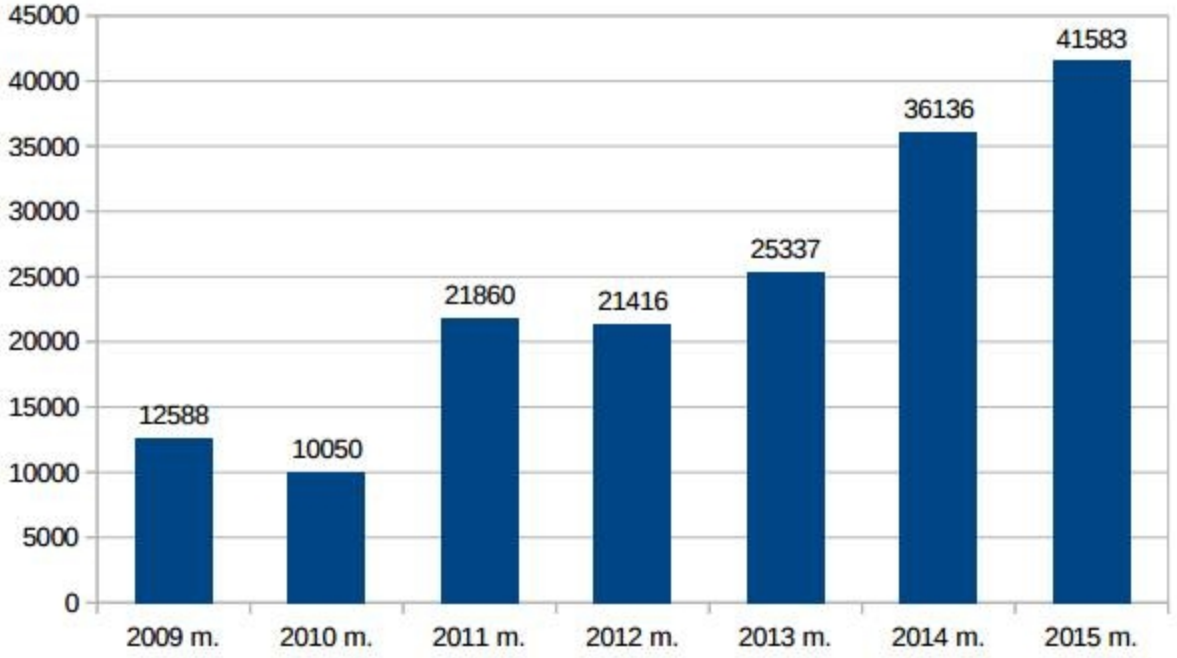
- Visos LIMIS tarnybinės stotys ir LIMIS naudotojų darbo vietos turi būti **apsaugotos nuo kenksmingos programinės įrangos** (virusų, programinės įrangos, skirtos šnipinėti, nepageidaujamo elektroninio pašto ir pan.);
- Dirbant su LIMIS kompiuteriuose **draudžiama naudoti programinę įrangą, nesusijusią su** LIMIS administratorių, LIMIS duomenų tvarkytojų ar LIMIS naudotojų **atliekamomis funkcijomis**;
- LIMIS administratorių ir LIMIS naudotojų stacionarių darbo vietų kompiuterius leidžiama naudoti tik LIMIS tvarkytojo ir LIMIS duomenų tvarkytojų patalpose;
- Darbui su LIMIS naudojami nešiojamieji kompiuteriai ir kiti įrenginiai negali būti palikti be priežiūros, palikti veikiantys neužrakintose patalpose, matomi automobilyje, viešbučio kambaryje (išskyrus užrakintus seife). Kelionių lėktuvais metu nešiojamieji įrenginiai turi būti laikomi rankiniame bagaže. Visi nešiojamieji įrenginiai turi būti apsaugoti saugiais slaptažodžiais, jei įmanoma, turi būti aktyvuotas bazinės įvesties / išvesties sistemos (angl. *Basic Input/Output System* (BIOS)) slaptažodis;
- Kilus įtarimui, kad su duomenimis yra vykdoma neteisėta veikla, privalo nedelsdami apie tai informuoti LIMIS-C administratorių.

LIMIS naudotojų atsakomybė

- LIMIS naudotojai, pasirašę konfidencialumo pasižadėjimą, užregistruojami LIMIS-C, jiems suteikiami naudotojų vardai, slaptažodžiai bei prieigos teisės pagal jų pareigybių aprašymuose nustatytas funkcijas;
- Visi LIMIS naudotojai privalo turėti darbo kompiuteriu įgūdžių bei būti **išklausę bendruosius darbo su LIMIS mokymo kursus**;
- LIMIS naudotojai, teikiantys duomenis į LIMIS duomenų bazes, turi būti **susipažinę su saugos dokumentais**;
- LIMIS duomenų tvarkytojų paskirti LIMIS naudotojai **privalo rūpintis tvarkomos informacijos saugumu ir tinkamu jos įvedimu** į LIMIS;
- Apie įvykusį informacijos saugos incidentą LIMIS naudotojai privalo nedelsdami žodžiu ar raštu pranešti LIMIS-C administratoriui.

Gerardas Bagdonavičius. Plėšrūnas narve. Šiaulių „Aušros“ muziejaus eksponatas.
Nuoroda internete: http://www.limis.lt/greita-paieska/perziura/-/exhibit/preview/150000012089354

Kibernetiniai incidentai Lietuvoje: statistika (1)



CERT-LT incidentų elektroninėje erdvėje tyrimų skaičiaus dinamika
Šaltinis: 2015 m. CERT-LT veiklos ataskaita, P. 3. Nuoroda internete: https://www.cert.lt/doc/2015.pdf

Incidentų tipai: kenkėjiška programinė įranga (1)

- **Kompiuterių virusai** – savaime besidauginančios kenkimo programos. Plitimo būdai:
  - kartu su „užkrėstomis“ bylomis;
  - elektroniniu paštu;
  - kopijuojant save ir perkeliant į atminties laikmenas arba vidiniame tinkle.

  Padariniai:
  - sunaikina ar sugadina kompiuteryje esančią informaciją;
  - gali atlikti atakas prieš kitus kompiuterius;
  - nulemia kompiuterių ir tinklų perkrovas;
  - gali perimti kompiuterio valdymą.
- **Trojos arkliai** – kitose programose besislepianti kenkėjiška programa. Patenka į sistemą per spragas naršyklėje arba juos pateikiant kaip naudingą programą. Dažniausiai nesidaugina. Tipiniai Trojos arklio funkcionalumai:
  - klaviatūros paspaudimų registravimas;
  - kompiuterio procesų valdymas;
  - bylų išsiuntimas;
  - galimybė stebėti naudotoją;
  - ir kt.

Incidentų tipai: kenkėjiška programinė įranga (2)

- **Išpirkos reikalaujanti programinė įranga (angl. *ransomware*)** – kenkėjiška programa, reikalaujanti išpirkos už kompiuterio veikimo ar duomenų atgavimą.
- **Botnet tinklai** – kompiuterių-zombių tinklai. Užkrėtus daug kompiuterių, sudaromas tinklas, kuris vėliau panaudojamas įvairioms funkcijoms:
  - paskirstyto atsisakymo aptarnauti (angl. *Distributed Denial of Service*, DDoS) atakoms, siekiant sutrikdyti veiklą;
  - banko prisijungimo ir konfidencialių duomenų perėmimas;
  - nepageidaujamų laiškų (angl. *spam*) siuntimas.
- Kibernetinės atakos realiu laiku: http://map.norsecorp.com/

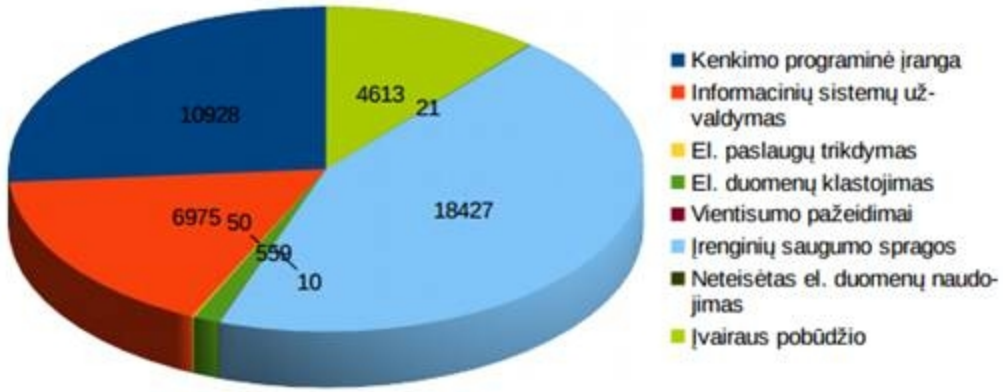
Kiti incidentų tipai

- **Nepageidaujami elektroniniai laiškai (angl. *spam*)** – be gavėjo sutikimo dideliais kiekiais siunčiami elektroniniai laiškai.
  - Komerciniais ir reklaminiais tikslais;
  - Kenkėjiškas *spam*
- **Duomenų vagystės (angl. *password fishing, „phishing“*)** – pasinaudojant žmogiškuoju faktoriumi, per fiktyvius internetinius puslapius arba nepageidaujamus el. laiškais bandoma išgauti konfidencialią naudotojų informaciją (prisijungimų prie sistemų slaptažodžius, elektroninės bankininkystės ar kreditinių kortelių duomenis).
- **Šnipinėjimo programos** – į kompiuterį ar kitą įrenginį įdiegta programa, kurios tikslas – rinkti informaciją apie naudotoją be jo žinios.

Kibernetiniai incidentai Lietuvoje: statistika (2)

Pranešimų pobūdis	2015 metų laikotarpis				
	I ketv.	II ketv.	III ketv.	IV ketv.	iš viso
Apie kenkimo programinę įrangą	3 051	2 579	2 612	2 686	10 928
Apie informacinių sistemų užvaldymą	1 494	1 278	1 686	2 517	6 975
Apie el. paslaugos trikdymo atakas	18	14	11	7	50
Apie el. duomenų klastojimą	257	83	103	116	559
Apie vientisumo pažeidimus	1	2	2	5	10
Apie įrenginių saugumo spragas	4 856	4 698	4 490	4 383	18 427
Apie neteisėtą el. duomenų naudojimą	5	8	8	0	21
Įvairaus pobūdžio	2025	865	796	927	4 613

CERT-LT 2015 m. nagrinėti pranešimai pagal tipus
Šaltinis: 2015 m. CERT-LT veiklos ataskaita, P. 1. Nuoroda internete: https://www.cert.lt/doc/2015.pdf



Techninės rekomendacijos LIMIS duomenų tvarkytojams

- LIMIS naudotojų kompiuteriuose privalo būti įdiegtos tinklinės antivirusinės programos;
- LIMIS naudotojų kompiuteriuose naudojama tik sertifikuota ir legali programinė įranga, būtina atliekamoms funkcijoms įvykdyti;
- LIMIS naudotojų teisė naudotis programine įranga yra valdoma – reguliariai tikrinamos LIMIS naudotojų darbo vietos ir jiems priskirtos teisės. Naudotojų, kurių darbo vietose priskirtos administratoriaus teisės, sumažinti iki būtino minimumo;
- Apriboti arba blokuoti naudotojų galimybes paleisti vykdomąsias bylas ir dll bibliotekas iš interneto naršyklių ir naudotojo aplinkos laikinai saugomų bylų katalogų;
- Iki būtino minimumo riboti visų tipų išorinių kompiuterinių laikmenų naudojimą pasirenkant duomenų perkėlimo tinklu alternatyvas, o prieš vykdant veiksmus su šiose laikmenose esančiomis rinkmenomis užtikrinti jų patikrinimą nuo kenksmingos programinės įrangos;
- Svarbiausios kompiuterinės įrangos techninė būklė nuolat stebima;
- Informacinės sistemos naudotojai apmokomi dirbti su programine įranga.

Patarimai LIMIS naudotojams: žinios ir budrumas

- Suvokite, kad Jūs esate sudedamoji informacinės sistemos saugumo grandis.
- Būkite įtarūs!
- Neatidarinėkite neaiškių internetinių nuorodų arba įtartinų bylų, prisegtų prie elektroninių laiškų, ypač, jei nepažįstate siuntėjo.

Patarimai LIMIS naudotojams: prevencija

- Naudokite antivirusinę programą ir užkardą (angl. *firewall*).
- Reguliariai atnaujinkite operacinę sistemą ir naudojamą programinę įrangą.
- Naudokite stiprius slaptažodžius.
  - Nenaudokite to paties slaptažodžio kelioms svetainėms ar informacinėms sistemoms.
- Turėkite atsarginę duomenų kopiją.

Patarimai LIMIS naudotojams: tinkama elgsena

- Naudokite tik savo USB atminties laikmenas.
- Naudodamiesi svetimu kompiuteriu:
  - pabaigę darbus, atsijunkite nuo autorizacijos reikalaujančių svetainių;
  - neišsaugokite savo prisijungimo informacijos;
  - ištrinkite interneto istoriją.
- Neužmirškite kibernetinio saugumo principų naudodamiesi išmaniaisiais įrenginiais.
- Nepalikite nešiojamų įrenginių be priežiūros.

Naudingos nuorodos

- www.cert.lt
- www.esaugumas.lt

Ačiū už dėmesį!

donatas.s@limis.lt