Vilniaus universitetas
Tarptautinis žinių ekonomikos ir žinių vadybos centras

Rolandas Dirgėla
Informacinių sistemų vadybos studijų programos studentas

ŽMOGIŠKASIS VEIKSNYS INFORMACIJOS SISTEMŲ APSAUGOJE

MAGISTRO DARBAS

Vadovas lekt. Saulius Jastiuginas

Vilnius 2007

Rolando Dirgėlos magistro darbas
(magistranto (-ės) vardas, pavardė)

tema
Žmogiškasis veiksnys informacijos sistemų apsaugoje

parengtas gynimui.

_____ _____
(data) (vadovo parašas)

Darbas įregistruotas _____ centre

_____
(data) (administratorės parašas)

Magistro darbą ginti leidžiu

_____ (centro direktoriaus parašas) _____
(data)

Recenzentu skiriu _____

_____ _____
(data) (Direktoriaus parašas)

Darbą recenzavimui gavau

_____ _____
(data) (recenzento parašas)

Di 295 Dirgėla, Rolandas
Žmogiškasis veiksnys informacijos sistemų apsaugoje: magistro darbas / Rolandas Dirgėla, informacijos sistemų vadybos studijų programos studentas; mokslinis vadovas S. Jastiuginas; Vilniaus universitetas. Tarptautinis žinių ekonomikos ir žinių vadybos centras. – Vilnius, 2007. – 63,lap.: Santr. Angl. Bibliogr.:p. 54

UDK 004:316.3

Saugi informacijos sistema, informacijos sistemų pažeidžiamumai, saugumo politika, socialinė inžinerija.

Magistro darbo objektas – žmogiškojo veiksnio įtaka informacijos sistemų apsaugai. Darbo tikslas – parodyti žmogaus, kaip informacinės sistemos dalies, svarbą apsaugos procesuose, kur apsauga yra ne papildomas darbas, bet pačio darbo dalis. Pagrindiniai uždaviniai: apibrėžti kas yra informacijos sistema ir kokia informacijos sistema yra saugi; išanalizuoti metodus, kuriais pažeidžiamas informacijos sistemų saugumas pasinaudojant žmogiškuoju faktoriumi; apibrėžti informacijos saugumo politikos sampratą, jos prasmes ir principus; saugumo politikos orientuotos į žmogiškąjį faktorių sukūrimas ir diegimas; praktinio tyrimo pagalba prognozuoti padėtį informacinių sistemų apsaugoje, Lietuvoje veikiančiose įmonėse.

Tik visus organizacijos lygius apimanti, tinkamai pasirinkta ir įdiegta saugumo politika gali efektyviai apsaugoti nuo išorinių ir vidinių saugumo grėsmių. Išnagrinėjus informacijos sistemų pažeidžiamumus susijusius su žmogiškuoju faktoriumi buvo prieita prie išvados, kad žmogiškasis veiksnys informacijos sistemų apsaugoje nėra įvertintas tinkamai, dėl savo unikalumo, kuris sukelia didelius sunkumas kuriant ir diegiant saugumo politiką. Dauguma organizacijų pasitenkina technologiniais informacijos sistemų apsaugos sprendimais ir tik paviršutiniškai paliečia darbuotojus. Silpnėjant kultūriniams barjerams tarp šalių ir tautų, šiuolaikinės globalizacijos akivaizdoje tokie informacijos sistemų pažeidžiamumai Lietuvoje taps dažnesni ir subtilesni, jei nesiimsime atitinkamų veiksmų. Atlikus tyrimą Lietuvoje veikiančioje finansinėje organizacijoje buvo atskleista reali padėtis informacijos sistemų apsaugoje, kuri pasitvirtino nagrinėjant literatūrą. Išryškintos silpnosios ir stipriosios apsaugos pusės bei prognozuota situacija kitose Lietuvoje veikiančiose įmonėse.

Magistro darbas gali būti naudingas įmonėms siekiančioms patobulinti saugumo politiką ir žmonėms, kurie domisi ir nori gilinti žinias informacijos sistemų apsaugoje.

ĮVADAS 5

1. SAUGI INFORMACIJOS SISTEMA 8

2. INFORMACIJOS SISTEMŲ PAŽEIDŽIAMUMAI 12

2.1. SOCIALINIŲ INŽINIERIŲ TIKSLAI 13
2.2. SOCIALINIŲ INŽINIERIŲ TAIKINIAI 14
2.3. KAIP VEIKIA SOCIALINIAI INŽINIERIAI 15
2.4. PSICHOLOGIJA SOCIALINĖJE INŽINERIJOJE 20

3. SAUGUMO POLITIKA 24

3.1. SAUGUMO POLITIKOS PRASMĖ IR PRINCIPAI 24
3.2. SAUGUMO KŪRIMAS 26
3.3. SAUGUMO REIKALAVIMŲ NUSTATYMAS IR RIZIKOS VALDYMAS 27
3.4. PRIEŽIŪROS METODŲ PARINKIMAS 32
3.5. KAIP APSISAUGOTI 33

4. PRAKTINĖ DALIS 36

4.1. DARBUOTOJŲ APKLAUSA 36
4.2. SUVAIDINTA SITUACIJA 43

5. ESAMA SITUACIJA IR PROGNOZĖS 50

IŠVADOS 51

BIBLIOGRAFINIŲ NUORODŲ SĄRAŠAS 53

SUMMARY 57

PRIEDAI 58

Įvadas

Ne taip senai visi priklausėme agrarinei visuomenei, po agrarinės sekė pramoninė, popramoninė ir pagaliau susiformavo informacinė visuomenė. Nenuostabu kodėl ji taip vadinasi, kai Šekspyro amžininkas per visą gyvenimą gaudavo tiek informacijos kiek dabar išspausdina šiokiadienio New York Times. Informacinė visuomenė, taip dabar madinga ir peršama vadinti visuomenė ir jos daleles žmones, kurie ieško, kaupia, perdirba skleidžia informaciją. Pastaruoju metu didėjant kompiuterių ir interneto paslaugų vartotojų grupėms informaciniai procesai įgyja milžiniška greitį, o pati informacija tampa neįkainojama. Kelių mygtukų paspaudimu galime sužinoti ar dabar lyja Buenos Airėse, o gal atsirado lėktuvo bilietas už vieną eurą iš Frankfurto į Lisaboną. Žmonės ieško informacijos, ją renka, perka ir naudoja. Jie nenori atsilikti nuo gyvenimo tempo, ko pasekoje prarandama beveik viskas – padėtis visuomenėje, klientai, reputaciją, pinigai ir t.t. Atsilikusieji pasmerkti misti pernykščiais informaciniais produktais, kurių vitaminus jau senai pasisavino pirmūnai, įgavę dar didesnį informacinį pagreitį. Perfrazuojant citatą galime sakyti – nusivarę arkliai nusišauna patys. Taigi tokiose lenktynėse, kur kas pirmesnis, tas galingesnis ir turtingesnis, informacijos siekiama pasitelkiant visas įmanomas priemones, tiek legalias tiek nelegalias. Sparčiai tobulėjant apsaugos sistemoms ir technologijoms įsibrovėliams darosi vis sunkiau įveikti jas pasinaudojant programos spragomis, ar technologiniais netobulumais. Tiesa, neįveikiamų sistemų nėra, tik surasti kelią ir įsibrauti į ją gali užtrukti arba kainuoti daug daugiau, nei nauda, kurią gaus įsibrovėlis. Taigi piktavaliai nusitaikė į silpniausią apsaugos grandinės žiedą – žmogų. Konfidencialios informacijos atskleidimas pažeidžiant informacijos sistemų saugą, kai įsibrovėlis pasinaudoja žmogiškuoju veiksniu, t.y. žmogaus baime, nežinojimu, stresu, pavydu ir t.t. Tai yra savybėmis, kurios nesikeičia visą žmonijos gyvavimo laikotarpį ir kurias turi kiekvienas iš mūsų nepaisant amžiaus, lyties ar užimamų pareigų. Reiškinys, kai pažeidžiamas informacijos sistemos saugumas pasinaudojant žmogumi vadinamas socialine inžinerija.

Socialinė inžinerija ir socialiniai inžinieriai žinomi jau daugiau nei dvidešimt metų. Problema išlieka aktuali ir dabar, nes įmonės nors ir žinodamos apie socialinius inžinierius, lėšas skirtas informacijos sistemų apsaugai leidžia naujesnėms ir geresnėms saugos sistemos įsigyti, pamiršdamos darbuotoją, kuris naudojasi šiomis sistemomis. Vienareikšmės apsaugos, kuri tiktų visiems, nuo socialinių inžinierių atakų nėra, nes kiekvienas informacinės sistemos vartotojas yra individas, tik jam būdingais bruožais, kuriais ir stengiasi pasinaudoti piktavaliai. Kompanijos nukentėjusios nuo socialinių inžinierių atakų nelinkusios skleisti informacijos apie tai, kad buvo pažeistas saugumas, nei kaip jis buvo pažeistas ir kokius nuostolius patyrė. Čia galime įžvelgti kompanijų baimę prarasti gerą vardą, klientus ir pinigus,

nes niekas nenorės pripažinti, kad taip lengvai buvo pažeistas informacijos sistemų saugumas. Kiekvienas iš mūsų linkęs slėpti faktus apie apgavystę, į kurią pažvelgę vėliau, suprantame, kad – „suvystė, kaip mažą vaiką“. Todėl proga pasimokyti iš kitų klaidų ne visada bus, taigi pasikliauti dažniausiai turėsime tik savo sumanumu ir išradingumu diegiant informacijos sistemų saugos politiką, orientuotą į žmogiškąjį faktorių.

Darbo tikslas – parodyti žmogaus, kaip informacinės sistemos dalies, svarbą apsaugos procesuose, kur apsauga yra ne papildomas darbas, bet pačio darbo dalis. Apibendrinus teorines ir praktines žinias teikti pasiūlymus kaip apsisaugoti nuo socialinių inžinierių atakų, bei prognozuoti kokia situacija Lietuvoje veikiančiose įmonėse. Siekiant užsibrėžto tikslo padės iškelti uždaviniai:

- Apibrėžti kas yra informacijos sistema ir kokia informacijos sistema yra saugi;
- Išanalizuoti metodus, kuriais pažeidžiamas informacijos sistemų saugumas pasinaudojant žmogiškuoju faktoriumi;
- Apibrėžti informacijos saugumo politikos sampratą, jos prasmes ir principus;
- Saugumo politikos orientuotos į žmogiškąjį faktorių sukūrimas ir diegimas;
- Praktinio tyrimo pagalba prognozuoti padėtį informacinių sistemų apsaugoje, Lietuvoje veikiančiose įmonėse.

Pirmoje dalyje apžvelgiami informacijos sistemų apibrėžimai, bei išskiriamos sudedamosios dalys. Žinodami kas yra informacijos sistema ir identifikavę dalis, galima nuspręsti ką stengiamės apsaugoti. Taigi galime apibūdinti kokius požymius atitinkanti sistema laikoma saugia.

Antroje dalyje, siekiant surinkti ir apibendrinti žinias į vieną visumą, pateikiama informacija apie dažniausiai naudojamas socialinių inžinierių veiklos būdus ir taktikas pažeidžiant informacijos sistemos saugumą. Nes tik žinodami, kaip veikia ir kur taikosi socialiniai inžinieriai galėsime pasirinkti teisingus ir veiksmingus kovos būdus. Priemonės ir kovos būdai pateikiami apibendrintai, siekiant paaiškinti bendrus principus, kuriuos kiekvienas pagal savo galimybes galės pritaikyti savo informacijos sistemų saugumui patobulinti.

Trečiojoje dalyje kalbama apie saugumo politikos, kurios taikinyje socialinė inžinerija, sukūrimo ir įdiegimo svarbą. Aptariami saugumo politikos prasmė ir principai, kuriais vadovaujantis politika taps efektyvi ir nebus našta organizacijai. Taip pat apibrėžiami saugumo politikos kūrimo etapai, kurie padės geriau suprasti sudėtingus, bet būtinus saugumo procesus. Detaliau nagrinėjama svarbiausias saugumo politikos kūrimo etapas rizikos valdymas. Skyrius baigiamas bendrais patarimais, kaip ir ko siekti, kad saugumo politika netaptų nenaudojamu taisyklių rinkiniu, o veiksminga priemone prieš socialinę inžineriją.

Paskutinėje dalyje aptariamas atliktas praktinis tyrimas ir jo rezultatai. Tyrimas, kuris susideda iš dviejų dalių, t.y. anketavimas, kurio pagalba sieksiu išsiaiškinti, kaip darbuotojai supranta duomenų apsaugą informacinėje sistemoje, bei suvaidinta situacija, kuri turėtų atskleisti tikrąją padėtį informacijos sistemų apsaugos procesuose, padės preliminariai nuspręsti kokia situacija yra kitose Lietuvoje veikiančiose įmonėse, bei prognozuoti tolesnes tendencijas informacijos sistemų saugoje.

1. SAUGI INFORMACIJOS SISTEMA

Pradėdami kalbėti apie žmogiškojo faktoriaus įtaką informacijos sistemų apsaugai, reiktų apibrėžti, kas yra informacijos sistema ir kokia informacijos sistema yra saugi. Informacijos sistemos apibrėžimų esą įvairių, priklausomai nuo to, kokios krypties, humanitarinių ar tiksliųjų mokslų, atstovas ją įsivaizduoja ir kokiems procesams teikia pirmenybę. Humanitarinės pakraipos atstovas informacijos sistemas apibrėžia, kaip struktūrizuotą procesą ar procedūrą, pagal kurią duomenys ar informacija kaupiama, organizuojama ir pateikiama vartotojams. Tiksliųjų mokslų atstovas informacijos sistemas apibrėžia kitaip. Informacijos sistema – visa infrastruktūra, organizacija, personalas ir komponentai, kurie padeda rinkti, apdoroti, saugoti, perduoti, vaizduoti, platinti ir archyvuoti informaciją. Informacijos sistema – junginys tarpusavyje sąveikaujančių komponentų:

- Kompiuterinė sistema
- Žmonės
- Procedūros
    - Duomenų įvedimas
    - Duomenų apdorojimas
    - Informacijos išvedimas
    - Informacijos saugojimas
- Duomenys ir informacija
- Ryšio priemonės

Negalime vienareikšmiškai teigti, jog kažkuris vienas iš teiginių yra teisingas, o kiti klaidingi. Kiekvienas iš jų savaip apibrėžia informacijos sistemą, parodydamas sistemos daugialypiškumą. Kaip tiksliųjų mokslų atstovas priimtiniausiu informacijos sistemos apibrėžimu laikau paskutinįjį, kuriuo ir naudosiuos tolesnėje darbo eigoje.

Išsiaiškinus, kas yra informacijos sistema, turime nuspręsti kokia informacinė sistema laikoma saugia. Nesukels daug ginčų teiginys, kad svarbiausia ir labiausiai saugotina informacinėje sistemoje yra duomenys, informacija.

Informacijos saugumas pagal ISO 17799 standartą yra apibūdinamas kaip išlaikymas:

- konfidencialumo: užtikrinimo, kad informacija būtų prieinama tik tiems, kurių prieiga prie jos yra sankcionuota;
- vientisumo: informacijos ir jos apdorojimo metodų tikslumo ir užbaigtumo garantijos;
- prieinamumo: užtikrinimo, kad įgalioti vartotojai, kai reikia, turi prieigą prie informacijos ir susijusio turto.

Taigi saugi informacinė sistema yra, jei informacija joje išlaiko konfidencialumą, vientisumą ir prieinamumą.

Organizacijos ir jų informacijos sistemos bei tinklai vis dažniau susiduria su saugumo grėsmėmis iš įvairių šaltinių, įskaitant kompiuterinį sukčiavimą, šnipinėjimą, sabotažą, vandalizmą, gaisrą ir potvynį. Tokie nuostolių šaltiniai kaip kompiuterio virusai, įsibrovimas į duomenų bazę ir paslaugos atsižadėjimo atakos tampa vis dažnesnės, ambicingesnės ir įmantresnės.

Priklausomumas nuo informacijos sistemų ir paslaugų reiškia, kad organizacijos yra vis labiau pažeidžiamos saugumo grėsmių. Viešųjų ir privačių tinklų prisijungimai bei informacijos išteklių skirstymas dar labiau apsunkina prieigos vykdymo priežiūrą. Paskirstytųjų sistemų naudojimo tendencija susilpnina vykdomą centrinės priežiūros veiksmingumą.

Dauguma informacijos sistemų suprojektuotos nesaugiai. Techninėmis priemonėmis gali būti laiduotas ribotas saugumas, todėl jis turėtų būti palaikomas tinkamu valdymu ir procedūromis. Nustatant, kuriuos priežiūros metodus taikyti, reikia kruopščiai planuoti ir daug dėmesio skirti detalėms. Saugumas ir jo užtikrinimas yra kompleksinis veiksmas, kuris niekada negali būti įgyvendintas iki galo ir susideda iš daugelio žingsnių. Tai reiškia, jog kiekviename iš jų, siekiant efektyvaus saugumo reikia žinoti ko sieki ir ką darai. Pagalba nenukrypti į šalis pasiekiama įgyvendinimo kontrole, kuri garantuoja teisingą kryptį saugumo link. Labai svarbus saugumo aspektas yra aukščiausiųjų vadovų palaikymas. Informacijos saugumo priežiūra yra daug pigesnė ir veiksmingesnė, jeigu diegiama laikantis specifikacijos reikalavimų ir projektavimo stadijoje. Pagrindinis sėkmingo saugumo politikos įgyvendinimo etapas yra visų organizacijos darbuotojų supratimas ir laikymasis jos, kuris pasiekiamas per apmokymus. Korektiškai atlikus saugumo politikos diegimo etapus, tolesniam efektyviam jos veikimui reikalingas nuolatinis stebėjimas ir testavimas. Stebint ir testuojant galime:

- pastebėti pasikeitusius verslo poreikius, prioritetus pagal, kuriuos pritaikysime ir apsaugos

politiką;

- pamatyti naujas grėsmes ir pažeidžiamumus, kuriais turėsime pasirūpinti;
- patikrinti ar visi apsaugos procesai efektyvūs ir tinkami, jei ne – juos reikia keisti.

Turėdami rezultatus galime apsaugos politiką pritaikyti prie esamos padėties, kuri toliau padės informacijos sistemai išlikti saugiai.

Nereiktų būti užtikrintiems, kad aš jaučiuosi saugus, tai reiškia aš esu saugus ir saugausi taip kaip man atrodo geriausia. Kiekvienas gali pasižiūrėti ir preliminariai nuspręsti ar saugumo jausmas tikras, o gal vis dėl to yra kur tobulėti. Požymiai, rodantys apie pažeidžiamų vietų buvimą informacijos saugume:

- Nesukurtos informacinės saugos nuostatos arba jų nesilaikoma. Nepaskirtas už informacinę saugą atsakingas asmuo.
- Slaptažodžiai užrašomi ant kompiuterinių terminalų, paliekami viešai prieinamose vietose arba jais keičiamasi su kitais darbuotojais; atvejai, kai jie prieš įvedimą rodomi kompiuterio ekrane.
- Per nuotolį valdomi terminalai ir mikrokompiuteriai paliekami be priežiūros darbo ir nedarbo valandomis, tuo tarpu be priežiūros paliktuose kompiuterių ekranuose rodomi duomenys.
- Neegzistuoja apribojimų prieigai prie informacijos ir jos naudojimui. Visi vartotojai turi priėjimą prie visos informacijos ir gali atlikti visas sistemos funkcijas.
- Nėra naudojami sisteminiai žurnalai ir nesaugoma informacija apie tai, kas ir kam naudoja kompiuterį.
- Pakeitimai ir programos diegiamos be išankstinio vadovybės leidimo.
- Nėra dokumentacijos arba ji neleidžia atlikti tokių veiksmų, kaip: suprasti gaunamas ataskaitas ir formules, pagal kurias gaunami rezultatai, modifikuoti programas, ruošti duomenis įvesčiai, taisyti klaidas, atlikti apsaugos priemonių įvertinimą ir suprasti pačius duomenis - jų šaltinius, saugojimo formatus, jų tarpusavio sąryšius.
- Daromi daugybiniai bandymai įeiti į sistemą, naudojant neteisingus slaptažodžius.
- Netikrinamas įvedamų duomenų korektiškumas ir tikslumas arba jų įvedimo metu daug duomenų atmetama dėl juose esančių klaidų, todėl prireikia daug kartų taisyti duomenis, žurnaluose nedaromi įrašai apie atmestas transakcijas.
- Yra sistemų išėjimo iš rikiuotės atvejų, sukeliančių didelių nuostolių.

- Neatliekama kompiuteriu apdorojamos informacijos analizė, kurios tikslas - jam tinkamo apsaugos lygio nustatymas.
- Skiriama per mažai dėmesio informaciniam saugumui. Nors saugumo politika ir egzistuoja, dauguma žmonių mano, kad ji iš tikrųjų nereikalinga

Saugi informacijos sistema mus įgalina toliau siekti užsibrėžtų verslo planų, nebijant, jog bus pavogti, nuplagijuoti ar sugadinti duomenys reikalingi efektyviam tikslo siekimui

2. INFORMACIJOS SISTEMŲ PAŽEIDŽIAMUMAI

Šiais laikais, kai įvairiausio tipo virusai ir kirminai vagia, naikina ir iškraipo informaciją, ugniasienės ir antivirusinės programos tapo įprastinėmis apsaugos priemonėmis tiek kompiuteriuose namuose, tiek ir darbe. Susikoncentravus ties šitomis problemomis dažnai neįvertinama, o kartais net ir nepastebima tampa kita problema – žmogus, kuris naudojasi kompiuteriu ir informacine sistema.

Kas yra socialinė inžinerija, iš kur ir kodėl ji atsirado? Pirmiausia socialinė inžinerija yra grėsmė į kurią kol kas žiūrime pro pirštus, nesuprasdami jos galimybių ir pasekmių, kol nesusiduriame su ja.

Nuolatinis ir spartus apsaugos sistemų ir technologijų tobulėjimas įsibrovėlius privertė prisitaikyti prie naujos padėties ir ieškoti lengvesnių ir pigesnių kelių į informacijos sistemų vidų. Tuo keliu tapo informacijos sistemų naudotojai.

Socialinės inžinerijos terminas siejamas su informacijos saugumo pažeidimais pasinaudojus žmogiškuoju faktoriumi. Čia pasitelkiamas principas – kam sunkiai dirbti laužtuvu norint išlaužti duris, jei lengviau pasinaudojus žmogumi, kuris žino kur yra raktas, gauti jį ir atsirakinti duris. Šis palyginimas gan tiesmukas, bet atskleidžia pagrindinę socialinės inžinerijos esmę – silpniausia grandis apsaugoje yra žmonės. Žmogus, pirmiausia yra individas, kurio negali užprogramuoti veikti pagal tam tikras taisykles, bet kurioje situacijoje. Jis pasielgs taip, kaip jam atrodo teisingiausia ir priimtiniausia. Taigi socialinių inžinierių taikinys žmogus ir jo silpnybės, kurias jie meistriškai išnaudoja siekdami užsibrėžto tikslo. Nesant įdiegtai ir veikiančiai saugumo politikai socialinis inžinierius lengvai nutrauks silpniausią grandį saugume, ir turėsime pažeistą informacijos sistemos saugumą. Socialiniai inžinieriai tai lyg psichologo ir „hakerio“ mišinys, kuriems kibus į darbą sunkiai atsilaiko dauguma apsaugos sistemų.

Štai kaip skirtingi autoriai pateikia ir skirtingus socialinės inžinerijos apibrėžimus.

„...menas ir mokslas priversti žmones vykdyti tavo norus.“

Harl. People hacking.

„Socialinė inžinerija – informacijos gavimas manipuliuojant žmogumi. Socialiniai inžinieriai norėdami išgauti konfidencialią informaciją, ar priversti žmogų elgtis ne pagal nustatytas darbovietės tvarkas naudojasi telefonu arba internetu. Lengviau pasinaudoti žmogiškosiomis savybėmis, nei ieškoti spragų kompiuterinėje sistemoje.“

Nežinomas autorius. Social engineering. Wikipedia

„ informacinė sistema susideda iš trijų dalių – geležies (hardware), programų (software) ir žmonių (wetware). Milijoninės vertės apsaugos sistemos daro pirmąsias dvi dalis neįveikiamas. Bet pasitelkiant

kantrybė, sumanumą ir žinias socialinis inžinierius pasinaudos paskutine sudėtine dalimi ir sužinos konfidencialią informaciją. Socialinis inžinierius žaisdamas psichologinius žaidimus su auka atskleis pageidaujamą informaciją.

Ross Bearman. A guide to social engineering, Volume one.

Kompanija gali nusipirkti geriausią apsaugos sistemą, išmokyti darbuotojus užrakinti visas paslaptis nakčiai, įstatyti neišlaužiamas duris pasamdyti geriausius apsaugos darbuotojus, instaliuoti apsaugos programas, bet ji vis vien bus pažeidžiama. Sukuriama vis tobulesnių apsaugos sistemų, į kurias įsibrauti technikos pagalba tampa beveik neįmanoma, arba tai užtruks daug laiko ir kainuos daug pinigų. Taigi kenkėjai vis dažniau traukia prie žmogiškojo elemento. Nulaužti žmogiškąją ugniasienę yra pakankamai lengva, nereikalauja didelių investicijų ir apima nedidelę riziką būti sučiuptam.

Socialiniu inžinieriumi galime pavadinti ir įsižeidusį darbuotoją, kuris jaučiasi neįvertintas ar neteisingai atleistas. Keršydamas pakenks įskaudinusiam darbuotojui, taip pat ir organizacijai. Toks pats gali būti ir įskaudintas mylimasis, kuris iš kerštо gali padaryti bet ką. Socialiniu inžinieriumi galime būti bet kuris. Tai lyg vaidmuo, kurį vaidina asmuo siekdamas vienokių ar kitokių tikslų. Kalbėsime apie tuos socialinius inžinierius, kurių tikslai susiję informacijos saugumo pažeidimais, kai suinteresuoti asmenys gauna pelną ar pranašumą kitų atžvilgiu.

Grandinė stipri tiek, kiek stipri jos silpniausia grandis.

2.1. Socialinių inžinierių tikslai

Egzistuoja posakis, kad saugus kompiuterius – išjungtas kompiuteris. Bet įjungti mes jį galime net keliais būdais. Klausimas tik kiek tai užims laiko, kiek reikės kantrybės, tvirto charakterio, pasiryžimo ir atkaklumo. Čia ir pasireiškia apgavystės menas. Įsilaužėlis turi atrasti būdą kaip apgauti vartotoją ir priversti atkleisti slaptą informaciją. Kai darbuotojas apgautas, įtakotas ir manipuliuojamas atskleidžia slaptą informaciją arba sukuria skylę apsaugoje, niekas nebeapsaugos jūsų. Kaip kriptografai randa užuominas tekste ir iššifruoja tekstą, taip socialiniai inžinieriai naudojasi apgavystės menu ir palaužia apsaugos sistemas.

Ko siekia socialiniai inžinieriai savo veikla? Pagrindinis tikslas, kaip ir kiekvieno įsilaužėlio, neteisėta prieiga prie informacijos sistemos ir kitokių informacijos laikmenų. Tolesnis neteisėtos prieigos naudojimas labai platus. Pradedant nuo asmeninių tikslų baigiant pramoniniu šnipinėjimu ar net valstybės paslapčių išgavimu. Galima pažymėti keturis motyvacinius aspektus, kodėl socialiniai inžinieriai puola taikinius:

- **Materialinė nauda –** sieki uždirbti daugiau ir pagerinti savo gyvenimo sąlygas;
- **Savanaudiškumas** – smalsumas; noras save išbandyti; pakeisti duomenis apie save, tarkime nuobaudas darbe panaikinti;
- **Kerštas –** priežastis žinoma tik pačiam žmogui;
- **Išorinis spaudimas, šantažas** – iš draugų; nusikalstomų grupuočių siekiant pelno, keršto ar šiaip susidomėjus.

Toliau galėtume išskirti du socialinių inžinierių tipus: mėgėjai ir profesionalai.

Mėgėjai socialiniai inžinieriai neuždirba pinigų pragyvenimui šnipinėdami, vogdami ar naikindami informaciją. Tai greičiau žmogaus kaukė, kuri užsidedama norint išgauti norimą informaciją. Pvz.: mokinys apsimeta palikęs knygą klasėje ir prašo budinčiojo duoti raktą nuo jos, bet tikrasis tikslas nugvelbti kontrolinio darbo užduotis. Darbuotojas, kuriam labai įdomu kiek uždirba jo kolegos.

Profesionalai socialiniai inžinieriai šnipinėdami, vogdami informaciją, iškraipydami ir naikindami ją uždirba pragyvenimui. Juos samdo įmonės šnipinėdamos konkurentus arba dirba savo asmeniniais tikslais.

Galutinis tikslas kodėl taikomasi į informacijos sistemą gali būti bet kas. Tiek piniginė nauda, kurią pažadėjo informacijos pageidaujantys verslo konkurentai, kuriuos lenkiate rinkoje savo naujomis idėjomis, pavydas, pyktis, godumas, puikybė. Galime sakyti, kad priežasčių yra tiek, kiek ir žmonių. Bet pagrindas yra, buvo ir bus piniginė nauda. Nesvarbu ar tu prarandi dešimt milijonų ar kelis litus, bet tokie procesai vyksta kasdien. Gal netgi dabar tu prarandi pinigus, o gal iš tavęs vagia naujas idėjas, o tu net nežinai.

2.2. Socialinių inžinierių taikiniai

Taikinių kaip ir tikslų gali būti be galo daug. Pradedant nuo paprastų žmonių iki stambių korporacijų ar net vyriausybinių institucijų. Todėl kiekvienas turi neprarasti budrumo ir darbe, ir namie. Jei iš tavęs dar neišviliojo sukčius apsimetęs „Topo Centro“ darbuotoju tūkstančio litų, ir tu galvoji, kad ant tokio kabliuko nepapulsi – pagalvok dar kartą. Socialiniai inžinieriai puikiai išnaudoja visas žmogiškąsias savybes idant pasiektų užsibrėžto tikslo.Gal kažkas nori sužinoti Jūsų telefono numerį, asmens kodą ar mokėjimo kortelės PIN kodą? Dažniausiai į socialinių inžinierių akiratį patenka tokie objektai:

- Telekomunikacijų bendrovės;
- Finansinės ir bankinės institucijos;

- Karinės paskirties organizacijos;
- Didelės korporacijos ir įmonės;
- Vyriausybinės institucijos.

T.y. taikiniai, kurie gali atnešti nemažą pelną suinteresuotiems asmenims. Kokias organizacijas dažniausiai puola socialiniai inžinieriai žinome, iškyla klausimas, o kuriais darbuotojais pasinaudoja atakų metu. Taikinys gali būti bet kuris darbuotojas, nepriklausomai nuo užimamų pareigų, bet padidintos rizikos ir dažniausiai atakuojami yra žemiausio rango darbuotojai. Taikiniais jie pasirenkami todėl, kad galbūt mažiau supranta konfidencialios informacijos reikšmę įmonei. Tokius darbuotojus lengva paveikti autoritetu, draugiškumu, žmogumi, kuris pažysta kitus darbuotojus ir kuriuos pažysta auka, skubiu prašymu, pažadėjimu, kad auka bus pripažinta ar gaus kokią tai paslaugą. Silpna grandis yra nauji darbuotojai, kurie dar nieko nepažysta ir nėra perpratę darbo taisyklių, tuo labiau saugos taisyklių. Reiktų nepamiršti žmonių dirbančių priėmime ar atsiliepiančiu telefonu, kurių pagrindinis darbas bendrauti su klientais. Jie kaip ir žemiausio rango darbuotojai galbūt nevisiškai supranta informacijos saugos esmę. Apsaugos darbuotojai taip pat yra taikiniai. Net ir valytojas, kuris valo patalpas, kai jau senai visi namie gali tapti auka, kuria manipuliuodamas socialinis inžinierius įvykdys suplanuotus juodus darbus. Negalima pamiršti ir tokių darbuotojų, kurie neturi tiesioginio kontakto klientais, tai būtų personalo valdymo skyrius, buhalterija. Reiktų pasirūpinti darbuotojais, kurie turi galimybę naudotis specifiniais resursais ar duomenimis. Pastebėta, kad gobšūs žmonės dažniausiais tampa aukomis, nes jais lengviau manipuliuoti.

Žvelgiant plačiau galima teigi, kad visi darbuotojai gali tapti aukomis. Pradedant nuo valytojų, kurie net nekalba lietuviškai, neturi jokio priėjimo prie kompiuterio ir supratimo kas yra informacijos apsauga. Užtektų pamojuoti padirbtu darbuotojo pažymėjimu ir pagrasinti jei neįleis baigsis jai blogai ir durys atsidarytų akimirksniu. Ne išimtis ir aukštesnio rango vadovai, kuriuos taip pat galima apgauti pasitelkus norą, atkaklumą ir fantaziją. Taigi kuriant saugos politiką negalima pamiršti nei vieno žmogaus.

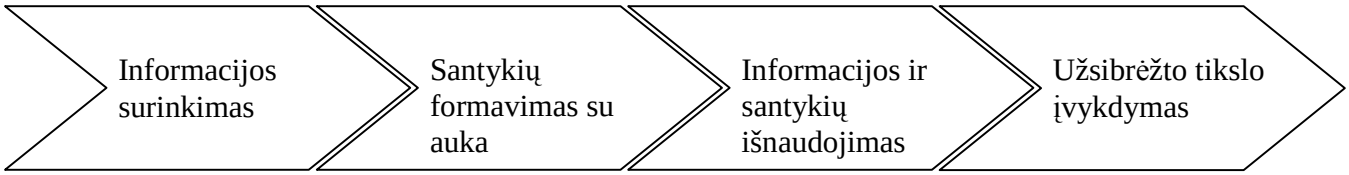
Jei saugumas nebuvo pažeistas, tai neturėtų kilti klausimas ar jis bus pažeistas. Klausimas turi būti – kada jis bus pažeistas?

2.3. Kaip veikia socialiniai inžinieriai

Socialinio inžinieriaus ginklas manipuliacija žmonėmis, priversti juos pasielgti taip, kaip jis nori. Įgauti aukos pasitikėjimą, ja pasinaudoti ir prieiti prie informacijos. Socialiniai inžinieriai atakuoja dviem

lygiais psichologiniu ir fiziniu. Dažniausiai jie sujungiami į vieną norint pasiekti užsibrėžtą tikslą greičiau, efektyviau ir sumažinant riziką iki minimumo, jog būsi pagautas. Todėl sėkmė reikalauja nemažai žinių apie kompiuterines, telekomunikacines sistemas ir gerų psichologo žinių (parasčiau tariant pažinti silpnas žmogiškąsias savybes). Prie fizinės grėsmės priskiriami telefonai, internetas, darbovietė ir net šiukšlių dėžės. Psichologiniai aspektai būtų įkalbinėjimas, apgaudinėjimas kuris gali skambėti kaip prašymas, padėjimas ir net reikalavimas. Nelygu kuom apsimeta ir kokią kaukę užsideda socialinis inžinierius. Kad ir kokiomis priemonėmis veiktų socialinis inžinierius galime pastebėti jo veiksmų ratą, kuris visur yra vienodas. Galbūt kai kuriuose apgavystės modeliuose bus praleista viena ar keleta grandžių, bet esmė išlieka ta pati. Veiksmų ratą sudaro keturios dedamosios, kurios pavaizduotos 1 paveiksle.

1 Paveikslas. Socialinio inžinieriaus veiksmų eiga.



Smulkiau apibūdinsiu fizinius, psichologinius ir kombinuotus būdus naudojamus išgaunant informaciją. Niekada nežinai, kuom gali apsimesti socialinis inžinierius ir kokią taktiką jis naudos. Ataka bus pritaikyta būtent pasirinktam taikiniui, kad kuo geriau išnaudotų jo silpnąsias savybes.

Fizinis kontaktas

Telefonas. Tai labiausiai paplitęs ir mėgstamas būdas tarp socialinių inžinierių. Paplitęs todėl, kad sukelia nedidelę riziką būti pagautam, bei pakankamai pigus metodas. Naudojantis telefonu kartu pasitelkiami ir psichologiniai aspektai, kurių veikiama auka atskleidžia reikiamą informaciją. Pavyzdžiui daugumoje organizacijų telefonai atpažįsta skambinančiojo numerį. Profesionalus socialinis inžinierius, pasitelkęs technines žinias lengvai gali perprogramuoti taip, kad vietoj numerio matysime direktoriaus vardą ir pavardę. Manau, kad bet kuris darbuotojas įvykdys dauguma paliepimų, kuriuos išreiks toks direktorius.

„Vishing“ – telefoninė „phishing“ versija. Metodo schema yra tokia: telefoninis robotas skambina atsitiktiniu telefono numeriu, atsiliepusiam asmeniui praneša apie tam tikrus apribojimus jo mokėjimo kortelei ir prašo nedelsiant paskambinti nurodytu telefono numeriu. Įtaigumo dėlei nurodytas telefono numeris būna nemokamas iš 800 serijos.

Paskambinus šiuo numeriu telefoninis auto atsakovas prašo suvesti mokėjimo kortelės numerį bei kitą konfidencialią informaciją, kuri iškart patenka į sukčių rankas. Pasinaudodami šia informacija jie sugeba “prieiti” prie žmonių sąskaitų bankuose. Ši schema gali būti taikoma ne tik mokėjimo kortelių, bet ir internetinės bankininkystės konfidencialiems kodams išgauti. Ši schema pastaruosius keletą metų plačiai buvo taikoma, naudojant elektroninius laiškus ir internetą.

Kaip apsisaugoti nuo telefoninių atakų? Niekada ir niekam nesakykite savo prisijungimo vardų ir slaptažodžių ar kitokių konfidencialių duomenų telefonu. Jei gaunate paliepimą, kuris jums kelia įtarimų ar yra neįprastas, nueikite ar perskambinkite ir patikrinkite ar jie teisingi.

Šiukšlių dėžės. Didelę dalį dokumentų, sąskaitų, išrašų ar šiaip popierių mes išmetame net nepagalvodami, kad socialinis inžinierius jais gali pasinaudoti. Šis metodas, kai informacijos ieškoma šiukšliadėžėse vadinamas nardymas po šiukšles (dumpster diving), kuris labai populiarus tarp socialinių inžinierių. Šiukšliadėžėje galima rasti vidinius darbuotojų telefonus su vardais ir pavardėm, lapelius su priminimais ar kitokia mažareikšme informacija jos savininkui, kalendorius su užrašais, sistemos žinyną, diskelius, nebenaudojamą kompiuterinė techniką ir netgi prisijungimo vardus su slaptažodžiais. Socialinis inžinierius net ir turėdamas, atrodo iš pirmo žvilgsnio, menkavertę informaciją sugeba sudėlioti ją kaip dėlionę, kuri jam pravers žengiant sekantį žingsnį. Taigi, bet kokia informaciją gali būti paskutinė vinis kruopščiai konstruojamame apgaulės mechanizme. Galbūt socialiniam inžinieriui net nereikės dėlioti informacijos ir mąstyti ką toliau daryti jei jis ras jūsų slaptažodį su prisijungimo vardu užrašytą ant lapelio, kurį išmetėte.

Kaip apsisaugoti nuo konfidencialios informacijos patekimo į išorę? Tai būtų keli paprasti dalykai – smulkinti šiukšles su naikinimo įranga taip, kad jų nebūtų įmanoma perskaityti, užrakinti šiukšliadėžes prie įmonės patalpų. Jei nėra galimybės nusipirkti šiukšlių smulkintuvo galima pasisamdyti įmonę, kuri atlieka darbus tiesiog užsakovo akivaizdoje. Paprasti gyventojai gali tiesiog sudeginti nereikalingus dokumentus.

Darbovietė. Ši socialinių inžinierių ataka apima didelę riziką būti sučiuptam, todėl reikalauja gerų vaidybinių, psichologinių ir techninių žinių ir kruopštaus pasiruošimo. Šiuo atveju tai tiesioginė ataka, kai atakuotojas su auka susiduria akis į akį.

Informacijos rinkimas. Prie tokių atakų būtų galima priskirti socialinio inžinieriaus pasivaikščiojimą po įmonę apsimetant tiekėju, interesantu, nutolusio padalinio darbuotoju ar verslo partneriu. Kaukių socialinis inžinierius gali užsidėti daug. Įvaizdžiui sustiprinti inžinierius net persirengs taip, kad atrodytų įtikinamiau – tiekėjo logotipu pažymėta apranga, verslo partneris avės brangiais batais,

vilkės Armani kostiumą, ant rankos kabės Rado vienetinis laikrodis. Šiuo atveju, jei mes nepažystame žmogaus asmeniškai, arba neturime pranešimo iš darbovietės jog lankosi svečiai ar tiekėjai reiktų žvelgti įtariai. Kad ir kaip atrodytų nepažystamasis nereiktų spręsti apie jį iš jo rūbų ir iš to kas jis sakosi esąs. Socialinis inžinierius patekęs į atakuojamo objekto vidų vaikšto po patalpas ir šniukštinėja, renka informaciją. Surenkama net menkiausia informacija, kuri vėliau sisteminama. Turint pakankamai informacijos planuojami tolesni žingsniai ir siekiama galutinio rezultato. Informacijos surasti galima visoje darbovietėje. Tai gali būti neužrakintas kompiuteris, kurio ekrane matosi konfidenciali informacija, kai jo savininkas išėjęs pietų. Žvilgčiojimas per petį darbuotojui, kai jis suvedinėja savo prisijungimo duomenis. Lapelių studijavimas, kuriais apklijuotas visas kompiuteris. Stalo kalendoriaus peržiūra, kuriuose daugelis mėgsta užsirašyti neviešinamą informaciją. Dokumentų paliktų matomoje vietoje peržiūra.

Instaliuojamos piktybinės programos. Tiesioginiu puolimu galime vadinti piktybinės programinės įrangos instaliavimu. Tai padaryti galima keliai būdais. Prieiname prie laisvo įjungto kompiuterio ir instaliuojame piktybinę programą. Tai gali sukelti įtarimų ir sužlugdyti puolimą, bet jei nėra kitų būdų ir šis suveikia – tikslas pasiektas. Sekantis būdas yra palikti diską ar kitą duomenų laikmeną netoli darbovietės ar pačioje darbovietėje ir laukti kol smalsus darbuotojas jį pasiims. Smalsumas nugali visus. Darbuotojui radusiam duomenų laikmeną įdomu pažiūrėti kas viduje. Socialinis inžinierius ten bus patalpinęs piktybinę programą, kuri atrodys labai nekaltai – nuotrauka, filmukas arba šiaip dokumentas. Aukai belieka atidaryti failą, piktybinis kodas automatiškai aktyvuojamas ir durys į informacinę sistemą sukurtos. Dabar socialiniam inžinieriui visi keliai atviri.

Prie socialinės inžinerijos priskiriami ir tokie informacijos rinkimo būdai kai naudojama technika. Tai gali būti slaptos kameros įmontavimas darbo vietoje, klaviatūros klavišų paspaudimų fiksavimo prietaisas, garso įrašymo mechanizmai ir visa kita technika, kuri padeda atskleisti konfidencialią informaciją.

Apsisaugoti padėtų įdiegta ir veikianti švaraus stalo politika, apribojimai darbuotojams instaliuoti ir keisti programinę įrangą, naudoti išorines duomenų laikmenas, sustiprinti patekimo į patalpas kontrolę, kad svečiai visada turėtų palydovą ir būti tinkamai identifikuojami.

Internetas

Internetas – derlinga aplinka norint išvilioti iš patiklių žmonių prisijungimo vardus ir slaptažodžius. Socialinis inžinierius pasinaudoja tuo, kad daugelis vartotojų naudoja tuos pačius arba panašius prisijungimo vardus ir slaptažodžius prisijungdami prie pašto, internetinio banko puslapio ir net

darbo vietos. Taip pat išnaudojamas vartotojų smalsumas, kai elektroninio pašto dėžutėje randa laišką su pasiūlymu laimėti savaitgalį Nidoje, tereikia paspaudus nuorodą užsiregistruoti. Kai tik į sukčių rankas papuola prisijungimo vardas ir slaptažodis, durys atsidaro ir į daugelį kitų sistemų.

*Elektroninis paštas.*Socialinis inžinierius apsimetęs sistemų administratoriumi atsiųs elektroninį laišką su prašymu užrašyti savo slaptažodį. Įtikinamumo dėlei laiškas atrodys, lyg jį siųstų vidinis abonentas. Pvz.: it.pagalba@rimi.lt

Galime sulaukti laiško, kuriame nebus prašoma įvesti savo duomenų, bet jame mes rasime prikabintą failą, kurį paleidus bus instaliuotas piktybinis kodas sekantis mūsų darbą. Priversti vartotoją paleisti failą nėra sunku. Kai kuriems užteks kad failas turėtų dominantį pavadinimą - „I love you“, „Ana Kurnikova Naked“ ir taip toliau. Tas pats apsimetėlis sistemų administratorius įtikinamumo dėlei gali paskambinti paprašyti vartotoją paleisti prikabintą failą, nes nepaleidus jo, visus tavo duomenis sunaikins virusas. Taip pat galime sulaukti nemokamų programų ar pataisymo kodų, kurie neva turėtų pagreitinti ir pagerinti mūsų darbo kokybę, bet deja čia tik šnipinėjimo programos.

„Phishing“.„Phishing“ (angl. password + fishing) - sukčiavimo forma prieš organizacijas ar privačius asmenis, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar falsifikuotais internetiniais tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius ar kitus konfidencialius duomenis. Pvz. banko sąskaitų numerius, apsaugos slaptažodžius, prisijungimo prie tinklalapių duomenis ir t.t. Vagys gali pasielgti dvejopai - patys imtis pavogtos informacijos realizavimo, slaptos medžiagos gavimo, pinigų plovimo ar panašiai. Arba, jie gali parduoti šią informaciją tretiesiems asmenims. „Phishing“ atakos pagrįstos padirbtu kažkokios firmos tinklalapiu. Tinklapis yra tiksliai nukopijuotas (gali būti ir pavogtas) ir atrodo bei funkcionuoja visiškai kaip reali svetainė. Tokių tinklapių gaminimu bei naudojimu užsiima įsilaužėliai norintys išgauti priėjimą pvz. į banko sistemas. Yra keli būdai „phishing“ atakų, kuriuos galima suskirstyti į aktyvius ir pasyvius. Tarkime Jūs norite apsilankyti tinklapio forume, bet netyčia surenkat ne Critical.lt, o Critical.com, vietoj google.lt parašote gooogle.lt arba hotmail.com parašote hotmale.com. Jums atidaro visiškai taip pat atrodantį tinklalapį, kuris yra tiksli originaliojo kopija. Jūs nukeliaujate į prisijungimo formą, įvedate savo duomenis ir jie nukeliauja tiesiai įsilaužėliams į rankas.Tokius puslapius, kurie gaudo suklydusius vartotojus priskirčiau prie pasyviųjų grupės. Čia aišku tik pavyzdys, bet galima numanyti ir platesnį tokių atakų mastą. Čia apsisaugojimo priemonę sunku sukurti, nes nuo žioplumo vaistų nėra. Taigi patartina atidžiai stebėti kur keliaujame.

Prie aktyviųjų grupės priskirčiau tokias realių puslapių kopijas, kurios pasirodo greitai ir dingsta greitai. Mechanizmas veikia taip pat. Sukuriamas tokio pačio dizaino puslapis kaip ir tikrasis, tik čia nekuriamas vardas, kurį vartotojas suklydęs papuls į netikrą puslapį. Falsifikuoto puslapio nuoroda, kuri atrodo kaip originalas, nusiunčiama klientui elektroniniu laišku, kuriame prašyma suvesti prisijungimo

duomenis, nes vėliau dėl techninių kliūčių paslauga gali būti atjungta ir ją aktyvuoti bus galima tik pas paslaugos teikėją. Auka nenorėdama gaišti laiko, sutaupo jį suvesdama prašomus duomenis fiktyvioje svetainėje, kurie patenka sukčiams į rankas.

2.4. Psichologija socialinėje inžinerijoje

Pagrindiniai psichologiniai aspektai, kuriuos nustatė mokslininkai ir kurių veikiamas žmogus yra linkęs vykdyti prašymus, nurodymus nesvarstydamas ir pažeisdamas taisykles yra šeši. Tai:

- **Valdžia, autoritetas**
- **Reta prekė ar paslauga**
- **Patikimas ir panašumas**
- **Apsikeitimas paslaugomis**
- **Įsipareigojimas ir pastovumas**
- **Socialinis pripažinimas**

Profesionalūs socialiniai inžinieriai pasižymi stipriomis žmogiškosiomis savybėmis – žavūs, mandagūs, gražiakalbiai, paslaugūs, dauguma jais greitai susižavi, charizmatiški. Taigi susidūrus su tokiu žmogumi sunku neapsigauti jo preciziškai sudėliotame žaidime.

Išskirčiau dvi aukos padėtis į kurias socialinis inžinierius siekia įvesti ją. Pirmoji būtų kai auka jaučiasi patogiai, nėra forsuojamas jos darbas ir tokiu būdu užmigdomas atidumas. Auka jaučiasi patogiai - socialiniai inžinieriai įgauna pasitikėjimą, susidraugauja su ja. Antroji padėtis, kai aukai sukeliamas nemalonus pojūtis ir auka nori kuo greičiau išeiti iš šios padėties. Tai gali būti laiko stoka, atitraukimas, stresinė situacija ir t. t. Ir pirmu ir antru atveju žmogus yra atitraukiamas nuo sisteminio mąstymo. Jis pradeda mąstyti euristiniu būdu. Kai žmogus mąsto sistemingai, jis pirma apgalvoja visus galimus variantus ir pasekmes prieš vykdydamas prašymus. Mąstant sistemingai aukai kyla loginiai klausimai, kuriuos uždavus socialiniam inžinieriui galima atskleisti jo tikruosius planus ir ataka bus atremta. Deja jei mąstymas tampa euristiniu, auka veikia skubotai, praleisdama logines jungtis tarp veiksmu ir negalvodama apie pasekmes. Taip mąstydamas žmogus būna mažiau įtarus, neklausia klausimų, nekelia prieštaravimų įsibrovėliui. Pvz. jei paskambinsi į darbovietę penkias minutes prieš darbo pabaigą, tai darbuotojo mintis apie darbo baigimą laiku gali užgožti sistemingą mąstymą.

Valdžia ir autoritetas

Žmonės linkę vykdyti paliepimus ar prašymus, kai juos išreiškia autoritetas ar didesnę valdžią, aukštesnes pareigas užimantis asmuo. Ypač tai pasireiškia karinėse organizacijose, kur aukštesnio rango karininko liepimas yra nediskutuojamas. Paprastoje įmonėje taip pat paklūstame vadovui, nors jo mes nesame matę. Socialinis inžinierius prašydamas paslaugos gali įbauginti žmogų. Įbaugintas žmogus negalvos ir elgsis taip, kaip liepiama. Baimė pasireiškia dėl kelių priežasčių. Jei bus paviešinta, kad darbuotojas suabejojo vadovo kompetencija į jį pradės žiūrėti nepatikliai ir tai gali pakenti jo tolesnei karjerai, greta ir finansinei būklei. Socialiniam inžinieriui belieka tik pasinaudoti šia spraga. Tai jis daro sumaniai. Apsimeta kito departamento vadovu ir skambina paprastam vadybininkui prašydamas išsiųsti atitinkamą medžiagą, prieš tai dar paminėjęs, kad tai labai skubu ir svarbu, nes kitaip valdžia nespės padaryti darbų ir visi nukentės. Norint susilpninti įtarinėjimus socialinis inžinierius visada paminės vardus žmonių, kuriuos pažysta auka. Vienas iš būdų apsimesti svarbiu verslo partneriu, paminėti keletą asmenų, susidraugauti ir paprašyti menkavertės, aukos atžvilgiu, paslaugos. Kartais nereikės net minėti vardų, jei skambinantis asmuo prisistatys Finansinių nusikaltimų tyrimo tarnybos darbuotoju ir paprašys kai kurių duomenų. Informacija nutekėjo, socialinis inžinierius turi dar vieną dalelę, kuri padės suktis apgavystės ratui.

Reta prekė ar paslauga

Žmonės turi polinkį atlikti prašymus jei siekiamas objektas yra retas, arba jį gauti reikia labai greitai. Auka supranta, kad ji nėra vienintelė, kuri bando šį daiktą ar paslaugą gauti, tai paskatina auką negalvojant atlikti prašymus. Prašymų vykdymas dar labiau suaktyvėja, kai auka supranta, jog šį daiktą ar paslaugą ji galės įsigyti tik ribotą laiką ir vėliau to padaryti bus neįmanoma. Pavyzdys galėtų būti iššokantis langas (pop-up) su prašymu suvesti duomenis ir pirmieji tūkstantis užsiregistravę gauna bilietus į filmo premjerą. Aišku niekas bilietų negauna, bet socialinis inžinierius jau turi nemažai duomenų apie aukas, kuriuos jis sumaniai panaudos tolesniame darbe.

Prie tokio tipo socialinės inžinerijos priskiriami ir vadinamieji „saldūs sandoriai“, kurių reklaminiai šaukiniai skamba panašiai - „ pirk vieną, gauk du“, „nuolaidos iki 75%“ ir t.t. Tiesa, ši socialinė inžinerija dar vadinama reklama. Pastudijavus atidžiau pastebime, kad nors perki du už vieno kainą, bet moki kaip už du, o kartais ir brangiau. 75% pigesnės prekės būna su pasibaigusiu galiojimu arba išvis nenaudojamos. Taigi pirmas įspūdis gali būti apgaulingas. Būkime budrūs.

Patikimas ir panašumas

Žmonės lengviau pasiduoda manipuliacijai kai socialinis inžinierius panašus į jį.Turi panašius pomėgius, tikėjimus, požiūrius, gimęs tame pačiame mieste, klausosi panašios muzikos, mėgstą tokį patį maistą ir t. t. Susidūrus su tokiu žmogumi auka linkusi žiūrėti pro pirštus į nustatytas darbo ir saugos taisykles vien todėl, kad jis panašus į ją.

Daug lengviau palaikyti pokalbį su žmogumi, kai jus sieja bendri interesai, pomėgiai. Taip užmigdomas aukos budrumas ir išviliojama informacija.

Prie tokių atakų galime priskirti, kai socialinis inžinierius apsimeta nauju darbuotoju arba nemokša vartotoju, kuriam darbo specifika ir visi procesai tik gūdus miškas. Apsimetęs naujoku socialinis inžinierius prašo pagalbos. Supratingi seni darbuotojai stengiasi padėti, nes jie prisimena, kaip buvo nedrąsu pirmosiomis dienomis ir kaip jiem reikėjo pagalbos. Taip sukuriamas žaidimas, kurio metu iš darbuotojų išgaunama reikiama informacija.

Socialinis inžinierius gali ir pasiūlyti pagalbą. Apsimetėlis paskambina aukai, tarkime naujam darbuotojui, kuris dirba tik gal dvi dienas. Bando su ja susidraugauti, šneka apie pomėgius, visokius kitus mažmožius, kurie visiškai nereikšmingi ir pokalbio pabaigoje draugiškai pasisiūlo padėti jei iškiltų kokių nors problemų, jam tereikia tik paskambinti. Apsimetėlis tyčia sukelia vienokį ar kitokį nepatogumą aukai, kuri netrukus skambina geradariui prašydama pagalbos. Auka visiškoje socialinio inžinieriaus valioje. Panašus metodas taikomas, kai socialinis inžinierius tiesiog palieka savo kontaktus prie aukos darbo vietos su prierašu: „jei kas neveiks skambinkite...“. Tiesa, prieš tai jis pats ir padarė taip, kad kas nors neveiktų.

Socialinis inžinierius linkęs apsimesti darbuotoju draugu, bendradarbiu. Jis kalbėdamas naudoja žargoną, kuris yra įprastas dirbant vienoje ar kitoje sferoje. Aukai sukuriamas įvaizdis, jog skambina senas, valdžios ujamas darbuotojas iš kito departamento, kuriam reikia mažos paslaugos.

Dažnai sukčius parodo save tokioje padėtyje, kad auka yra laiminga sutikus tokį žmogų.

Socialiniai inžinieriai mėgsta apsimesti programinės įrangos tiekėjais, kurie skambina norėdami išsiaiškinti ar viskas veikia tvarkingai, ar nėra sutrikimų. Taip užkalbinėdami jie išvilioja menkavertę mums, bet labai vertingą jiem informaciją.

Atoveikis, atsiliepimas, pasikeitimas

Auka galima lengvai pasinaudoti, jei jai kažką duodi, ar pažadi vertingo. Tai gali būti daiktas ar patarimas. Žmogiškoji savybė yra ta, kad jei žmogus kažką gauna, net jei ir neprašo, tai labai tikėtina, jog

jis suteiks paslaugą kitam žmogui. Lyg principas, kuris veikė vaikystėje, aš tau saldainį – tu man saldainį. Net jei žmogus padėjo vieną kartą, tai atsidėkodamas jam kitas žmogus bus linkęs padėti ne vieną kartą. Schema atakų kaip ir daugelis prieš tai buvusių. Socialinis inžinierius apsimetęs kito departamento vadovu susidraugauja su auka, sako jai komplimentus, pabrėžia, kad ji šauniai atlieka savo darbą. Kalbėdamas lyg netyčia pasako, kad ji labai tiktų greitai atsilaisvinančiose aukštesnėse pareigose pas jį skyriuje ir auka tai išgirdusi tampa labiau suinteresuota padėti apsimetėliui, kad tik pakiltų karjeros laiptais. Įdomu tai, kad daugeliu atveju auka negauna nieko, tik pažadą su daug „jei“. Aukos noras tampa toks stiprus, kad pro pirštus žiūri į visas vidaus darbo taisykles.

Įsipareigojimas ir pastovumas

Žmogus linkęs elgtis taip, kaip prieš tai jis pasižadėjo, pritarė kažkokiems teiginiams. Nesielgdamas kaip pažadėjo jis jaučiasi esąs nesąžiningas, todėl stengiasi elgtis taip, kad jaustųsi gerai. Pvz.: socialinis inžinierius apsimetės IT saugos darbuotoju aiškina apie sistemos apsaugą, kas ir kaip saugoma, kad negalima atskleisti duomenų, skelbti prisijungimo vardo su slaptažodžiu ir slaptažodis turi atitikti saugos politikos reikalavimus. Išklausiusi instrukciją auka pasižada vadovautis jomis. „Instruktorius“ klausinėja aukos, kaip ji įsisavino įgautas žinias ir paprašo jai pasakyti savo slaptažodį, nes tikslas yra patikrinti ar pakankamai jis sudėtingas. Aukai jį pasakius sukčius paprašo sudaryti slaptažodį pagal jo instrukcijas. Taip sudarytą slaptažodį socialinis inžinierius lengvai atspės ir turės priėjimą prie informacinė sistemos.

Socialinis pripažinimas

Žmonės linkę pasiduoti manipuliacijai jei kažkas irgi tą patį daro ir jie daro. Kito žmogaus toks pats veiksmas priimamas kaip socialinis pritarimas, jei taip daro kiti ir aš taip darysiu ir nieko blogo nebus.

Paprasčiausias pavyzdys galėtų būti kai skambina socialinis inžinierius apsimetęs sistemų administratoriumi paprašo darbuotojo, kad šis įrašytų porą simbolių programoje, nes kitaip programa nustos veikusi. Apsimetėlis pavardina kelis aukos pažystamus, kurie jau jam padėjo ir toliau sau sėkmingai dirba. Auka linkusi sutikti su prašymu, nes jis draugų veiksmus priima, kaip įrodymą, kad nieko blogo nebus, jei ir jis padės sistemų administratoriui.

3. SAUGUMO POLITIKA

Kiekviena organizacija susiduria su grėsmėmis, kurios kyla iš daugelio šaltinių ir pasireiškia įvairiausiomis formomis, todėl apsisaugoti nuo jų pakankamai sunku. Į pagalbą ateina saugumo politika. Saugos politika – pagrindiniai taikytini informacijos saugos užtikrinimo ir valdymo principai, pagrindinės taisyklės, į kuriuos atsižvelgiant turi būti derinami informacinės sistemos (ar informacinių sistemų) veiklos ir naudojimo procesai, procedūros ir rengiami juos reglamentuojantys dokumentai. Šis taisyklių rinkinys niekada nėra užbaigiamas, tai „gyvas“ dokumentas, kuris papildomas kaskart iškilus naujiems reikalavimams technologijoms,darbuotojams ir pasikeitus įmonės strategijoms. Saugumo politika apibrėžia ir koordinuoja veiksmus siekiant efektyviai išvengti grėsmių.

3.1. Saugumo politikos prasmė ir principai

Kalbant apie saugumo sistemos prasmę svarbiausiais laikau keturis aspektus. Efektyvumas – apsaugos sistema turi užtikrinti efektyvią informacijos apsaugą. Apsaugos sistema turi nustatyti realią informacijos apsaugos padėtį, nes gavus klaidingus duomenis bus padaryti klaidingos išvados ir sprendimai, ko išvadoje galima stipriai nukentėti. Galimų grėsmių ir jų poveikio išryškinimas taip pat svarbi apsaugos sistemos dalis, kuri padeda susikoncentruoti į svarbiausias grėsmes, kurios gali atnešti daugiausia nuostolio. Identifikavus grėsmes galima efektyviai jų išvengti arba sumažinti poveikį. Paskutinis aspektas yra efektyvus investavimas į saugumo sistemą, t.y. saugumo sistema neturi tapti finansine našta ir jos kaina turi atitikti saugomos informacijos kainą.

Ar tikrai reikalinga apsaugos sistema, kuris saugo nuo internetinių atakų, jei nei vienas kompiuteris neturi interneto prieigos. Gal užteks paprasčiausios virusus ieškančios ir naikinančios programos, kuri skenuos pageidautinus failus. Taip pat reiktų nusistatyti kas mums gresia ir nuo ko saugotis. Nereikia draustis nuo žemės drebėjimų Lietuvoje, geriau apsidrausti nuo vagystės. Nereiktų diegtis brangių apsaugos sistemų, jei neturime ko saugoti, arba apsaugai užtektų paprasto seifo. Reikia pabrėžti jog absoliutaus saugumo, kaip ir saugumo politikos tinkančios visiems nėra. Kiekviena organizacija ar įmonė turi siekti, kad saugumo užtikrinimas taptų valdomu procesu.

Saugumo sistemos principai

- Stebėjimo (reagavimo į aplinką);
- Įgūdžių ugdymo (saugos kultūros);
- Atskaitomybės (accountability) principas. Jis remiasi tuo, kad kiekviena šalis yra atsakinga už saugumą ir suprantą jo reikšmę. Atskaitomybės principas padeda audituoti vykstančius procesus, kai pareigos ir atsakomybė yra aiškiai apibrėžtos;
- Supratimo (awareness) principas pasireiškia tuo, kad darbuotojas suprasdamas saugos sistemos reikšmę, linkęs jos laikytis. Jei darbuotojas nesupranta saugumo sistemos reikšmės, jis linkęs nesivadovauti ja, neva, kaip nereikalinga funkcija. Supratimas ir įsisąmoninimas ženkliai sumažina informacijos saugumo pažeidimus;
- Etikos, moralės principas;
- Atitikimo principas nurodo, kad saugumo sistema turi atitikti saugotinos informacijos reikšmę, kainą;
- Integralumo principas pasireiškia saugumo sistemos integracija į kompanijos politikas ir siekius, idant sukurtų bendrą sistemą, kuri efektyviai apsaugotų informacijos sistemas;
- Savalaikiškumo principas. Saugumo sistema turi suveikti tada kai reikia, laiku;
- Pastovus saugumo sistemos vertinimas (assessment). Besitęsiantis procesas, kurio pagalba saugumo sistema išlieka efektyvi;
- Teisingumo ir nešališkumo principas (equity). Nepažeisti vartotojų ir savininkų teisių, bei orumo.

Taigi geras saugumas yra:

- įsidiegta saugumo politiką;
- saugotinu resursų klasifikavimas;
- grėsmių žinojimas;
- grėsmių valdymas;
- tinkamas reagavimas įvykus incidentui;
- ataskaitų kūrimas;
- adaptyvus elgesys.

Susikoncentravę ties žmogiškuoju faktoriumi informacijos sistemų saugoje ir sugretinę su anksčiau minėtais metodais, kaip pažeidžiamas saugumas pasinaudojant juo, galime sukurti saugos politiką. Tikslingiau ją būtų galima vadinti tik dalimi visos saugos politikos, kuri koncentruojasi tik į siaurą dalį ir tikrai nėra ta pagalba kuri tiks visiems, nes kiekvienos kompanijos saugos politika priklauso nuo jos subrendimo lygio, veiklos procesų ir daugelio kitų aspektų.

3.2. Saugumo kūrimas

Suprasdami kokia informacijos sistema yra saugi, bei žinodami saugumo politikos prasmes ir principus galime kurti savo saugumo politiką, kuri bus pritaikytą mūsų poreikiams. T.y. kiek galima sumažinti žmogiškojo veiksnio įtaką informacijos sistemai. Kuriant saugumo politiką ir jos laikantis negalima pamiršti, jog tau tęstinis procesas, kuris reikalauja pastovios analizės ir tobulinimo. Saugos politikos kūrimas preciziškas procesas, kuriame negalima praleisti nei vienos smulkmenos, nes ji gali tapti ta vieta, dėl kurios bus pažeistas saugumas. Saugomo politika nėra vaistas visiems nuo visų ligų, kiekviena organizacija turi susikurti savo saugumo politiką pagal savo poreikius ir galimybes. Galime prisiminti lietuvių liaudies patarlę – „Pagal Jurgį ir kepurė“.

Organizacijos vadovams reikia suprasti, kad investavimas į apsaugos sistemas neatneš realaus pelno, o tik sumažins nuostolio tikimybę.

Kaip ir bet kuris projektas, saugumo kūrimas apima:

- Esamos saugumo būklės nustatymas;
- Plano sudarymas;
- Rizikos valdymas:
    - Rizikos vertinimas:
        - Rizikos analizė;
        - Rizikos įvertinimas;
    - Rizikos tvarkymas;
    - Rizikos priėmimas;
    - Informavimas apie riziką

- Priemonių diegimas;
- Sistemos stebėjimas.

3.3. Saugumo reikalavimų nustatymas ir rizikos valdymas

Kompanijos norėdamos susikurti saugumo politiką (IT saugos politiką, saugos architektūrą ir t.t.), naudojasi daugiausia tarptautiniais standartais (pvz., ISO 17799), kurių pagalba įdiegiamas saugumas. Be abejo kompanija turi subręsti vienokiems ar kitokiems standartams arba diegti tik kai kuriuos reikalavimus. Nebrandžiai kompanijai diegiamas jos lygio neatitinkančio saugumo, gali sukelti didesnes problemas ir atnešti nuostolį, kaip ir per maži saugumo reikalavimai brandžiai kompanijai neduos laukiamų rezultatų.

Saugumo reikalavimai identifikuojami metodiškai įvertinant saugumo riziką. Priežiūros išlaidas reikia sugretinti su komercinės veiklos nuostoliais, kaip saugumo nesėkmės rezultatu. Rizikos įvertinimo metodai gali būti taikomi visai organizacijai arba tik jos dalims, taip pat atskiroms informacijos sistemoms, ypatingiems sistemos komponentams arba paslaugoms, kai tai praktiška, realu ir naudinga.

Rizikos įvertinimas yra metodiškas apsvarstymas:

- veiklos nuostolių, kaip saugumo nesėkmės rezultato, įvertinant galimus informacijos konfidencialumo, vientisumo arba prieinamumo netekties padarinius;
- tokios nesėkmės, kuri kiltų atsižvelgiant į vyraujančias grėsmes ir silpnąsias vietas bei jau įdiegtus priežiūros metodus, realių tikimybių.

Šio įvertinimo rezultatai padėtų nuspręsti ir apibrėžti tinkamus valdymo veiksmus ir prioritetus, skirtus valdyti informacijos saugumo riziką ir įgyvendinti parenkamus apsaugos nuo šios rizikos metodus. Kad būtų įvertintos visos organizacijos dalys arba atskiros informacijos sistemos, gali prireikti daug kartų kartoti rizikos įvertinimo procedūras ir parinkinėti priežiūros metodus.

Svarbu periodiškai peržiūrėti saugumo riziką ir įdiegtus priežiūros metodus, siekiant:

- atsižvelgti į veiklos reikalavimų ir prioritetų pokyčius;
- aptarti naujas grėsmes ir pavojus;
- patvirtinti, kad esami priežiūros metodai vis dar veiksmingi ir tinkami.

Atsižvelgiant į ankstesnius įvertinimus ir keičiamus rizikos lygius, kuriuos vadovybė pasirengusi priimti, peržiūrėjimai turėtų būti atliekami įvairaus nuodugnumo lygiais. Dažnai pirmasis rizikos

įvertinimas atliekamas aukštu lygiu, suteikiant prioritetą didelės rizikos zonoms, o po to mažesniu lygiu, kreipiant dėmesį į ypatingas rizikas.

Rizikos valdymas yra organizacijos strateginio valdymo pagrindinė dalis. Tai toks procesas, kai yra nusprendžiama kiek rizikos galima prisiimti siekiant konkretaus tikslo, kad gauti rezultatai atneštų naudą ir kuo mažesnį nuostolį. Ji surikiuoja veiksnius pagal priimtinumą, kurie yra tiek teigiami, tiek neigiami. Be to, tinkamas rizikos valdymas padidina sėkmės galimybę ir sumažina nesėkmės poveikį organizacijai. Rezultatyvus rizikos valdymas susideda iš rizikos identifikavimo ir jos traktavimo. Reiktų pabrėžti, kad rizikos valdymas tai viena iš paskutinių stadijų kalbant apie jas. Prieš pradedant valdyti riziką tenka nueiti ilgą kelią. Pradžioje apsibrėžkime kas yra rizika. Štai kokį apibrėžimą pateikia „Rizikos valdymo vadovas“ išleistas 2005 Lietuvos Respublikos Vidaus reikalų ministerijos : „rizika tai – įvykio tikimybė ar jos pasekmių darinys“.

Reiktų paminėti, kad rizikos valdymas yra nepertraukiamas ir besivystantis procesas, kaip ir pati saugumo politika. Jis apima visą organizaciją, įsiskverbia į jos kultūrą per rizikos politiką ir programą, kurią kuruoja atsakingas asmuo. Rizikos valdymas strategiją paverčia į taktinius ir vykdomuosius tikslus, už kuriuos atsakingi rizikos valdymo specialistai.

Tinkama rizikos valdymo strategija yra raktas į rizikos ir galimybių santykio vertinimą. Bendrovėms, kurios patiria reikšmingų pokyčių, susijusių su įėjimu į elektroninio verslo aplinką, reikia struktūros ir metodologijos, kaip valdyti riziką. Ši struktūra padeda joms:

- prisiimti riziką, kurios veda į galimą adekvatų atlygį;
- sušvelninti neišvengiama riziką;
- išvengti nebūtinos rizikos;
- tinkamai paskirstyti rizikos valdymo išteklius.

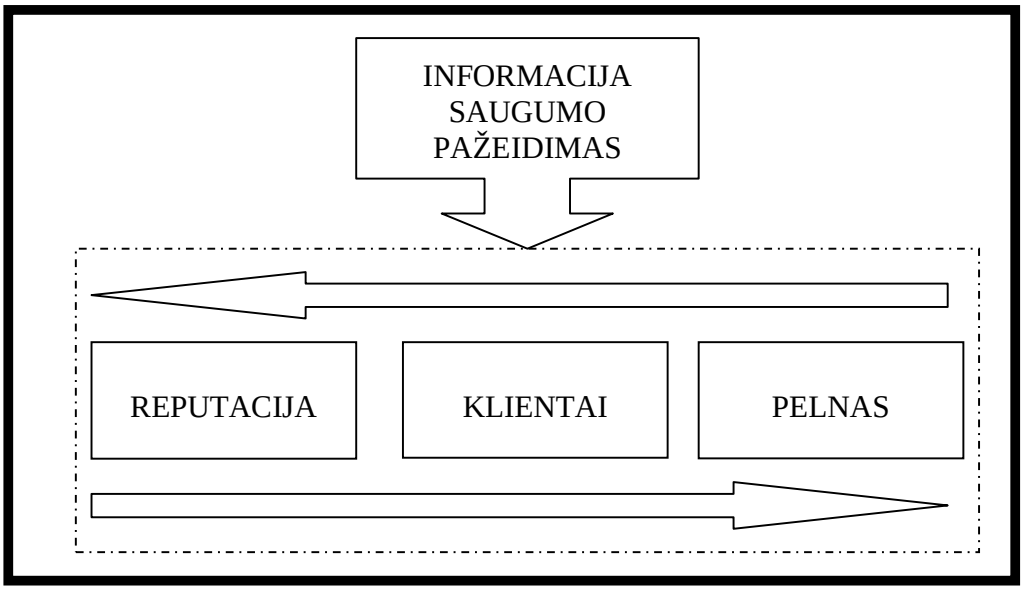
Norėdami tinkamai valdyti riziką, bendrovės vadovai ir darbuotojai privalo dirbti naudodami vienodą terminologiją, vienodus būdus ir vienodą bendrovės tikslų bei uždavinių supratimą. Kad būtų galima tinkamai paskirstyti išteklius, rizikos valdymas reikalauja sisteminio požiūrio, kuris leistų riziką laiku atpažinti ir įvertinti. Bendrovės strateginių uždavinių kontekste, kiekviena konkreti rizika gali būti charakterizuota kaip pavojus, netikrumas arba galimybė. Išanalizavusi konkrečios rizikos priimtinumą, apimtį ir atlygį, įmonė pasirenka atitinkamą rizikos valdymo variantą. Įmonė gali riziką priimti, sušvelninti arba perkelti. Priėmusi atitinkamą sprendimą, įmonės vadovybė vėliau nuolatos seka minėtą riziką bei užtikrina, kad į apie riziką turimą informaciją bus nuolat atsižvelgiama derinant bendrovės strateginius uždavinius.

Taigi svarbiausia ką mes norime apsaugoti, yra informacijos sistemoje esantys konfidencialūs duomenys, kuriais naudojasi organizacijos darbuotojai. Tai gali būti verslo planai, naujų paslaugų ar produktų aprašymai, klientų duomenys ir t.t. Netekus konfidencialių duomenų didėja rizika prarasti

- reputaciją;
- klientus;
- pelną.

Visi išvardinti galimi praradimai glaudžiai susiję (2 paveikslas). Mažai esama dalykų, kurie būtų taip lengvai pažeidžiami ar tokie sunkiai apčiuopiami, kaip bendrovės reputacija. Praradus reputaciją, didėja tikimybė prarasti klientus, esamus ir būsimus, ko išdavoje negausime pelno. Praradus klientus, gali sumažėti reputaciją ir be abejo pelnas. Visi veiksniai tiek į vieną pusę, tiek į kitą gali iššaukti ir bankrotą.

2 paveikslas. Informacijos saugumo pažeidimų sąsajos su įmonės veikla



Informacijos sistemų saugumo, kalbant apie žmogiškąjį veiksnį, siekiančios kompanijoms būtina atsižvelgti ir analizuoti šiuos rizikos šaltinius, kurias čia ir išvardinsiu:

- Konkurentai;
- Būsimi, esami ir buvę darbuotojai;
- Klientai;
- Kiti asmenys ar nusikalstamos grupuotės;
- Aptarnaujantis personalas (tiekėjai).

Išvardinti rizikos šaltiniai tarpusavyje gali glaudžiai sietis, tarkime konkurentai apsimeta klientais arba įsidarbina pas jus, kad sužinotų verslo planus. Galimybių be galo daug, todėl negalima praleisti nei vieno aspekto.

Riziką pagal tikimybę galėtume suskirstyti į keturias grupes:

- rizika yra mažai tikėtina ir savo realizavimosi atveju bendrovei darys nežymų poveikį;
- rizika yra labai tikėtina, tačiau mažo poveikio;
- rizika yra mažai tikėtina, tačiau savo realizavimosi atveju bendrovę paveiktų stipriai;
- rizika yra labai tikėtina ir turėtų stiprų poveikį bendrovės veiklai.

Rizika susijusi su žmogiškojo veiksniu informacijos sistemų apsaugai reiktų priskirti prie pačių pavojingiausių, t.y rizika yra labai tikėtina ir turėtų stiprų poveikį bendrovės veiklai. Žmogus ne mašina, negalima jo užprogramuoti siųstis atnaujintų saugumo standartų ir reikalavimų, jis kiekvieną kartą gali pasielgti skirtingai, dėl išorinių, vidinių ir tik jam vienam žinomų priežasčių. Saugumo politikos, orientuotos į žmogiškąjį veiksnį, paskirtis nustatyti atsakomybes, taisykles ir procedūras atitinkamose situacijose taip, kad nebūtų pažeistas informacijos sistemos saugumas.

Dauguma informacijos sistemos pažeidimų įvykdo vidaus darbuotojai, todėl svarbu techninėmis priemonėmis riboti informacijos prieinamumą. Pradžioje reiktų suklasifikuoti darbuotojus ir jų teises į informaciją. Kurie darbuotojai gali žiūrėti, modifikuoti informaciją, o kuriems nereikia suteikti priėjimo prie duomenų, jei jie nereikalingi darbuotojo darbui. Taip pat techninės priemonės turėtų sekti kas naudojasi, kada ir kiek laiko naudojosi, bei ar darė pakeitimus ir kokius informacijai, kad įvykus incidentui būtų galima identifikuoti vartotoją. Techninėmis priemonėmis reiktų riboti ir išorinių duomenų laikmenų naudojimąsi, jei darbas to nereikalauja. Tai būtų cd-rom įrenginio užrakinimas, atminties raktų nepripažinimas kompiuteryje ir t.t. Kalbant apie elektroninį paštą, sistema turi riboti išeinančios už organizacijos ribų informacijos turinį. Apibrėžti, kas gali siųsti laiškus su priedais. Darbuotojui naudojantis nešiojamu darbiniu kompiuteriu, reiktų jį apsaugoti slaptažodžiais ir informaciją jame koduoti, kad netekus kompiuterio, niekas negalėtų pasinaudoti informacija esančia jo viduje.

Techninės priemonės nepanaikina žmogiškojo veiksnio įtakos informacijos sistemų saugumui, o tik sumažina riziką. Jei projekto ar produkto vadovas, kuriam be abejo leidžiama naudotis informacija apie sukurtą naują paslaugą ar produktą, perduoda informaciją konkurentams, tai jokie techniniai apribojimai nepadės. Padėti gali būsimų darbuotojų atranka, domintis jų praeitimi – kur dirbo, ką veikė ir pan. Esami darbuotojai turėtų pasirašyti sutartį dėl konfidencialios informacijos neatskleidimo dirbant įmonėje, bei

nutraukus darbo santykius su ja, kurioje numatomos šalių pareigos ir atsakomybės. Panašias sutartis reiktų pasirašyti su tiekėjais ir įmonėmis, kurioms perkelti su įmonės veikla nesusiję darbai („outsourcing“), prieš tai atidžiai išsinagrinėjus jų patikimumą. Informacijos neatskleidimo sutartis gali ir nepadėti, jei darbuotoju pasinaudos sumanus socialinis inžinierius ir įvykdys savo juodus darbus. Šiuo atveju į pagalba ateina procedūros ir darbo tvarkos, susijusios su duomenų apsauga.

Procedūros ir darbo tvarkos, vadovaujantis saugumo politikos prasme, turi apibrėžti, kurie darbuotojai už kokią informaciją atsakingi, kas gali naudotis ir kaip naudotis informacija. T.y. įvykus incidentui ir esant neapibrėžtai atskaitomybei, negalėsime identifikuoti, kas buvo atsakingas už informacijos saugumą. Procedūros darbuotojui privalo nurodyti, kaip elgtis tam tikrose situacijose. Jei žmogus ne iš organizacijos prašo vidinės įmonės informacijos pas darbuotoją, procedūros turi nurodyti kaip reiktų veikti ir ką informuoti esant tokiai situacijai. Būtina saugos taisykles ir procedūras sukurti kiek galima trumpesnes ir aiškesnes, kad darbuotojui nesukeltų didesnių sunkumų jas skaitant.

Saugumo politika turi būti sukurta taip, kad nestabdytų efektyvaus darbuotojo darbo ir netaptų našta, kurios bus bandoma išvengti. Taigi apsauga ir darbas turi būti subalansuoti, kad nei vienas iš jų nenukentėtų. Saugumas turi tapti ne papildomu darbu, bet pačio darbo dalimi ir kartu įmonės strategija.

Saugumo politikos supratimas aukščiausiame įmonės lygmenyje vienas iš kertinių akmenų efektyviam jos įgyvendinimui. Palaikant vadovams yra lengviau išaiškinti ir įtikinti žemesnes pareigas užimančius darbuotojus, kad saugumo politika ir procedūros yra būtinos ir neatsiejamos nuo atliekamo darbo. Geriau suprasti ir laikytis saugumo padės motyvavimo sistema. Neretai pasitaiko, kad sukūrus saugos politiką, bei procedūras darbuotojams liepiama jomis vadovautis, pamiršus išaiškinti jos prasmę. Darbuotojas, nesupratęs kodėl reikalingi atitinkami veiksmai, juos tiesiog ignoruoja arba laikosi tik iš dalies. Taigi saugumo politika sukurta, pinigai išleisti, bet niekas jos nesilaiko – galime teigti, kad saugumas šiuo atveju fiktyvus. Grįžtant prie teigiamo rezultato, kai saugos politika įsisąmoninta visos organizacijos lygmenyje, sekantis žingsnis būtų vadovautis saugumo politika darbe. Laikymasis saugumo, kaip ir supratimo prasideda nuo aukščiausių vadovų, jie turi rodyti pavyzdį kitiems įmonės darbuotojams. Darbuotojai matydami vadovų palaikymą ir elgesį, elgsis adekvačiai.

Kalbant apie socialinių inžinierių atakas ir saugumo politikos sugretinimą, kuri turi sumažinti riziką tokių atakų iki priimtino lygio, politikos supratimas ir laikymasis įgyvendinamas per apmokymus ir dar kartą apmokymus, nepraleidžiant nei vieno darbuotojo.

Mokymus kaip ir procedūras privalu diferencijuoti, atsižvelgiant į darbuotojo pareigas, atliekamas funkcijas ir priėjimą prie informacijos. Svarbi detalė yra tai, kad nėra įmonėje darbuotojo, kuriam nereiktų mokymų apie informacijos svarbą ir saugą. Ypatingas dėmesys kreiptinas ir plačiausi apmokymai reikalingi darbuotojams, kurie tiesiogiai susiję su klientų aptarnavimu ir bendravimu su jais. Dažniausiai

tokie darbuotojai užima žemesnes pareigas ir mažiau supranta informacijos svarbą įmonei. Negalime pamiršti ir tų, kurie nebendrauja su klientais, t.y. vadinamų „back office“ darbuotojų, bet turi priėjimą prie informacijos. Jiems reikalingi siauresni, galbūt į vieną ar kelias informacijos saugumo sritis orientuoti apmokymai. Reikalingi apmokymai ir tiems darbuotojams, kurie nesinaudoja informacijos sistemomis. Nauji darbuotojai pirmiausia yra apmokomi ir tik tada gali gauti priėjimą prie informacijos sistemos, kuris yra limituotas ir tik praėjus atitinkamam laiko tarpui ir išklausius nuodugnesnius apmokymus, suteikiamos platesnės teisės į informaciją.

Stambioje įmonėje galima įkurti pagalbos centrą, kuris rinktų informaciją apie įtartiną veiklą. Šio centro numerį kiekvienas darbuotojas turėtų šalia ir kilus įtarimams galėtų paskambinti.

Įdiegta ir veikianti saugumo politika reikalauja pastovios priežiūros ir tobulinimo. Jei atsirado naujos darbuotojų pareigos ar pasikeitė informacijos sistemos struktūra būtina peržiūrėti saugumo politiką iš naujo, įsivertinti galimas grėsmes, riziką ir patobulinti taip, kad atitiktų saugios informacijos sistemos reikalavimus. Saugumo sistemą privalu testuoti ir rezultatus analizuoti įžvelgiant privalumus ir trūkumus, kuriuos būtina ištaisyti. Testavimas galimas pasiunčiant netikrą socialinį inžinierių į darbovietę, skambinant telefonu ir daug kitų būdų, kuriuos galime susikurti pasitelkę fantaziją.

Visą socialinio inžinieriaus klastą galima labai lengvai sužlugdyti keliais paprastais žingsniais:

- patikrinti asmens tapatybę, ar jis tikrai tas, kas sakosi esąs;
- ar asmuo turi teisę žinoti prašomos informacijos;
- ar asmuo turi teisę teikti užklausas dėl norimos informacijos.

3.4. Priežiūros metodų parinkimas

Kai saugumo reikalavimai yra identifikuoti, turėtų būti parenkami ir įdiegiami priežiūros metodai, kad būtų užtikrintas rizikos sumažinimas iki priimtino lygio. Priežiūros metodus galima parinkti arba naudojantis ISO 17799/ BS 7799, arba kitais metodais, arba, jei tai yra reikalinga, galima sukurti ir naujus metodus, kurie atitiktų ypatingus įmonės poreikius.

Parenkami priežiūros metodai turėtų būti grindžiami įdiegimo kainos ir rizikos mažėjimo santykiu bei galimomis netektimis saugumo nesilaikymo atveju. Taip pat reikia įvertinti ne tik piniginius faktorius, bet ir reputacijos netektį. Taip pat saugumas neturėtų stabdyti darbo našumo.

Priežiūros metodai apibrėžti įstatymiškai:

- asmens duomenų apsauga;

- organizacijos dokumentų apsauga;
- intelektualinės nuosavybės apsauga.

Įprasti priežiūros metodai informacijos saugumui:

- saugumo politikos sukūrimas;
- bendrų ir specifinių saugos reikalavimų paskirstymas personalui;
- informacinio saugumo mokymas ir tobulinimas;
- pranešimai apie saugumo pažeidimus;
- verslo tęstinumo valdymas.

3.5. Kaip apsisaugoti

Kas sustabdys socialinį inžinierių? Ugniasienė? Galinga autorizacijos priemonė? Įsibrovimo aptikimo sistema? Koduojama informacija? Limituotas priėjimas prie telefono numerių? Koduotas serverio pavadinimas, kuriame saugoma svarbi informacija, kad pašalietis negalėtų atsekti kur kas yra? Tiesa yra tokia, kad nėra technologijos kuris galėtų apsaugoti nuo socialinio inžinieriaus.

Taigi tikslas sukurti tokią apsaugos politiką, kuri kiek būtų galima sumažintų įsibrovimo galimybę. Kaip jau buvo minėta anksčiau kiekviena darbuotojo užimama pozicija reikalauja skirtingos apsaugos sistemos. Vienas apsaugos būdas tikrai netiks visiems. Galime prisiminti patarlę – kas tinka viskam, tas netinka niekam. Taigi identifikuojame visas pažeidžiamas vietas. Nustatome, kokie pažeidimai čia galimi. Vadovaudamiesi gautais rezultatais kuriama saugos politiką. Pirmiausia tokios politikos reikalingumu reikia įtikinti aukščiausius įmonės vadovus, nes be jų palaikymo tai bus tik popierius, kuriame užrašyti daug visokių taisyklių, kurių niekas nesilaiko. Apsaugos politika neturi trukdyti dirbti, ji turi padėti. Ne taip lengva apjungti gerą saugumą ir darbuotojų produktyvumą. Darbuotojas turi ne tik žinoti, kad apsaugos politika egzistuoja ir ji padeda išvengti nuostolių, bet ir suprasti kokia ji svarbi. Apsaugos politika turėtų tapti ne papildomu darbu šalia einamųjų darbų, o kasdieniu darbu, kuris atliekas įprastai. Kiekviena įmonė privalo turėti apsaugos politikas ir procedūras, kurios padėtų darbuotojams reaguoti į žmones, kurie prašo kažką padaryti su kompiuteriu ar kitokia sistema kuri yra kompiuterizuota ar susijusi su kompiuteriais.

Technologijos gali pasunkinti kelią įsibrovėliams. Bet vienintelė efektyvi priemonė sušvelninti grėsmę yra sujungti apsaugos techniką su apsaugos politika, kurios apibrėžtų taisykles darbuotojų elgesiui, tinkamam išsilavinimui ir mokymui. Tik vienu būdu galime apsisaugoti, turėdami išmokytą, sąmoningą ir sąžiningą darbo jėgą. Tai apimtų mokymus politikų ir darbo tvarkų ir svarbiausią – supratimą, kad visa tai ko mokomės yra svarbu, o ne tik tai kad tą reikia daryti. Pirmas žingsnis – kiekvienas darbuotojas žinotų, jog yra nesąžiningų žmonių, kurie pasinaudos apgaule ir galės psichologiškai paveikti, manipuliuoti žmonėmis. Darbuotojai turi suprasti ir žinoti kaip informacija turi būti apsaugota ir kaip tai padaryti. Kai darbuotojai žino, supranta, kaip veikia socialiniai inžinieriai ir kaip jie gali manipuliuoti, darbuotojai gali suprasti, atsekti kada jais bandoma pasinaudoti, arba jau naudojasi. Apsaugos įsisąmoninimas taip pat reiškia mokymą darbuotojų įmonės apsaugos politikos ir darbo tvarkos. Politikos svarbios tuo, kad tai lyg taisyklės, kurios apibrėžia darbuotojų elgseną norint apsaugoti įmonės informacines sistemas ir svarbią informaciją.

Darbuotojus reikia išmokyti naudotis apsaugos politikos nuostatomis. Dar daugiau, turime užtikrinti, kad kiekvienas darbuotojas suprastų apsaugos reikšmę, kad nesugalvotų praleisti ją savo patogumui. Darbuotojas turi suprasti kam apsauga skirta. Kitaip nežinojimas, neišprusimas bus darbuotojo pasiteisinimas, ir aiškus pažeidžiamumas, kuriuo socialinis inžinierius tikrai pasinaudos. Pagrindinis apsaugos sąmoningumo programos tikslas paveikti taip žmones, kad jie pakeistų savo elgesį ir nuostatas, motyvuojant kiekvieną darbuotoją, kad jis norėtų būti dalimi organizuojant įmonės informacinių išteklių apsaugą. Reikia išaiškinti kaip tai padės įmonei pasiekti didesnio pelno, ir ne tik įmonei, bet ir pačiam darbuotojui. Įmonė turi tam tikrą informaciją apie kiekvieną darbuotoją, taigi kol darbuotojas saugo įmonės informaciją taip pat jis saugos ir informaciją apie save.

Apsaugos mokymo programa reikalauja svaraus, didelio palaikymo. Mokymo pastangos turi pasiekti kiekvieną darbuotoją, kuris turi prieigą prie svarbios informacijos, kompiuterių ir jų sistemų. Mokymai turi būti tęstiniai ir reguliariai peržiūrimi ir tobulinami atsižvelgiant į atsiradusias grėsmes ir pažeidžiamumus. Aukščiausi vadovai turi pilnai palaikyti politika, nes kitaip darbuotojai ja netikės. Ir tai turi būti tikras tikėjimas. Programa privalo turėti papildomų lėšų plėtojimui, testavimui ir jos rezultatų įvertinimui.

Mokymų programą reikia sukurti taip, kad visi darbuotojai suprastų jog įmonė gali būti užpulta bet kada. Turi suprasti, kad kiekvienas darbuotojas užima tam tikrą poziciją apsisaugant nuo bet kokio mėginimo įsibrauti į sistemą ir pavogti svarbią informaciją. Apsaugos mokymas turi siekti didesnio tikslo nei paprastų taisyklių perdavimas ar išmokimas. Darbuotojai dirbdami įtemptai, stengdamiesi kuo geriau atlikti užduotis gali pražiūrėti pro pirštus arba nepaisyti saugumo taisyklių. Žinojimas kaip veikia socialiniai inžinieriai ir kaip nuo jų apsisaugoti yra vertingos žinios, kuriomis darbuotojas gali ir

nepasinaudoti. Reikia motyvuoti darbuotojus, kad jie naudotųsi įgautomis žiniomis, o ne tik žinotu. Informacijos apsauga yra ne papildomas darbas, o viso darbo dalis, kurią reikia dirbti. Darbuotojai turi suprasti, kad apgaulės grėsmė yra reali. Taigi svarbios informacijos praradimas gali paveikti pačią įmonę įskaitant ir darbuotojus. Taigi rūpintis sauga įmonėje reiktų taip pat, kaip ir savo mokėjimo kortelės PIN kodo saugojimu.

Kuriant apsaugomos mokymo ir sąmoningumo saugos programas reiktų nepamiršti, kad vienas modelis netiks visiems. Programoje reiktų išskirti darbuotojų grupes, kurioms dirbant skirtingose pozicijose gresia skirtingi pavojai. Programa vadovams, IT personalui, kompiuterių vartotojams, vadovų asistentams, priimamojo darbuotojams, apsauginiankams, net ir tiems kas neprisiliečia prie kompiuterio. Mokymai turi sudominti ir įtraukti vartotoją, tokiu būdu žinios bus suprantamesnės ir greičiau įsisavinamos. Tikslas programą paversti patrauklia, interaktyvia patirtimi, kur teorija sugretinama su praktika. To pasiekti galime žinias perduodami žaidimo forma įtraukdami visus klausytojus ir panašiai.

Būtų galima pacituoti Bruce Schneier „ apsauga nėra produktas, tai procesas“. Taigi belieka tik tobulintis, tobulintis ir dar kartą tobulintis.

4. PRAKTINĖ DALIS

Siekdamas išsiaiškinti kaip žmonės suvokia ir laikosi informacijos saugumo principų, praktinį tyrimą atlikau finansines paslaugas teikiančioje įmonėje. Pasirinkau finansinę organizaciją, nes duomenų apsaugai čia turi būti skiriamas ypatingas dėmesys. Pažeidus informacijos sistemos konfidencialumo, prieinamumo ir vientisumo principus pasekmės tiesiogiai atsilieps pelnui. Be to duomenų apsauga yra griežtai prižiūrima ir jos tvarkymą reglamentuoja Lietuvos Respublikos įstatymai. Bet koks informacijos sistemos pažeidimas turės poveikį finansinei būklei.

Tyrimo eiga ir vykdymas ilgai derintas su įmonės informacinių technologijų ir operacinės rizikos departamentais, siekiant nepažeisti duomenų saugumo ir neįžeisti respondentų žmogiškųjų savybių. Suderinus bendras sąlygas, kaip įsipareigojimas darbe neminėti įmonės pavadinimo ir priešus sąlygą, jog nebus minimas organizacijos vardas, leista jį atlikti.

Tyrimas susideda iš dviejų dalių:

- Darbuotojų apklausa;
- Suvaidinti situacija.

4.1. Darbuotojų apklausa

Tyrimui susidedant iš dviejų dalių, pirmiausia buvo atlikta apklausa, siekiant išsiaiškinti kaip darbuotojai supranta ir laikosi informacijos saugumo.

Darbuotojų apklausa vykdžiau sudaręs anketą (priedas nr.1). Anketos tikslas išsiaiškinti, kaip darbuotojai supranta duomenų apsaugą, kaip jos laikosi namie ir darbe. Būtina atsižvelgti į tai, kad darbuotojas, pildydamas anketą stengsis pasirodyti kuo geriau, t.y iš visų atsakymų rinksis teisingiausią, bet nebūtinai, tą, kuris tinka jam. Norint įsitikinti ar tikrai, tai ką anketoje teigia darbuotojas yra teisybė, padės antroji tyrimo dalis – suvaidinti situacija.

Anketa, kurios klausimai su darbuotojų atsakymais išreikštais skaitine ir procentine forma pateikiama lentelėje nr.1.

1 lentelė. Darbuotojų atsakymai išreikšti skaitine ir procentine reikšme

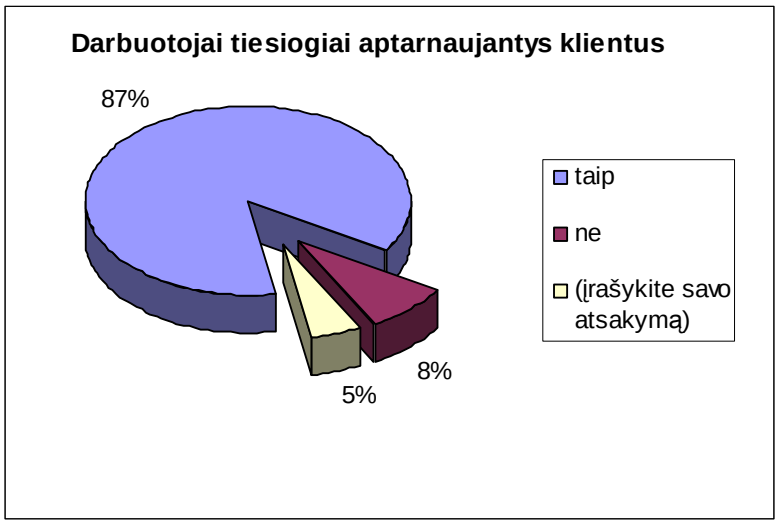
1. Kiek laiko dirbate su finansais susijusiose įmonėse?	iki 1 metų	28	47%
	2-3 metus	9	15%
	virš 3 metų	23	38%
2. Ar atidarinėjate elektroniniuose laiškuose esančias nuorodas ar prikabintus failus, kuriuos gavote į darbinę pašto dėžutę iš nepažystamų adresatų?	taip	6	10%
	ne	44	73%
	kartais	10	17%
3. Kur dedate mažai reikšmės turinčius popierinius dokumentus susijusius su darbu, kai jie nebereikalingi?	į šiukšliadėžę	10	17%
	sunaikinate krokodilu	43	72%
	(įrašykite savo atsakymą)	7	12%
4. Paaiškinkite terminą phishing:		21	35%
5. Ar Jūsų darbas susijęs su tiesioginiu klientų aptarnavimu?	taip	52	87%
	ne	5	8%
	(įrašykite savo atsakymą)	3	5%
6. Ar patikrinate (t.y. telefonu paskambinate ir paklausiate) paliepimus atlikti vienokius ar kitokius veiksmus iš aukštesnes pareigas užimančio žmogaus, kuriuos gaunate žodžiu per trečiuosius asmenis (ne darbuotojus):	taip	34	57%
	ne	10	17%
	(įrašykite savo atsakymą)	16	27%
7. Ar pasakysite telefonu paskambinusiam žmogui, jo sąskaitos numerį?	taip	1	2%
	ne	29	48%
	taip, kai jį identifikuosiu	30	50%
8. Ar pasitraukdami iš darbo vietos „užrakinate“ kompiuterį?	taip	27	45%
	ne	11	18%
	kartais	11	18%
	naudoju automatinį užrakinimą	11	18%
9. Kelių bendradarbių žinote slaptažodžius, kuriais jie prisijungia prie kompiuterio ar informacinės sistemos (specialios programos)?	vieno	8	13%
	dviejų	1	2%
	daugiau nei dviejų	1	2%
	(įrašykite savo atsakymą)	50	83%
10. Slaptažodžius ar prisijungimo vardus naudojamus darbe prisijungiant prie informacinių sistemų, specializuotų internetinių puslapių ir kompiuterio esate užsirašę ant lapuko ir laikote darbe, kad nepamirštumėte?	taip	1	2%
	ne, visus prisimenu mintinai	47	78%
	užrašyti, bet ne visi	8	13%
	(įrašykite savo atsakymą)	4	7%
11. Ar persiuntinėjate kitiems elektroninio pašto adresatams gautus	taip	4	7%

laiškus apie naujus virusus, kurie sugadina kompiuterio kietąjį diską; nelaimingus vaikus, kuriem kaupiasi pinigai sąskaitoje nuo kiekvieno išsiųsto laiško ir panašius?	ne	41	68%
	kartais	15	25%
12. Ar atidarinėjate elektroniniuose laiškuose esančias nuorodas ar prikabintus failus, kuriuos gavote į asmeninę pašto dėžutę iš nepažystamų adresatų?	taip	3	5%
	ne	50	83%
	kartais	7	12%
13. Jūsų slaptažodis naudojamas elektroninio pašto prieigai susideda iš:	Raidžių (abcdefgh)	27	45%
	Raidžių ir skaičių (abcde123)	24	40%
	Didžiųjų ir mažųjų raidžių, skaičių ir kitų simbolių (Abcd12!@)	9	15%
	(įrašykite savo atsakymą)	0	0%
14. Kaip dažnai kečiate slaptažodžius ?	Nekeičiu	9	15%
	Karta į mėnesį	13	22%
	Kartą į pusmetį	11	18%
	Kartą per metus	4	7%
	(įrašykite savo atsakymą)	23	38%
15. Ar naudojate ugniasienes ir/arba antivirusines programas asmeniniame kompiuteryje namie?	taip	53	88%
	ne	1	2%
	nežinau	6	10%
16. Ar esate kada suvedę savo asmeninius duomenis t.y. asmens kodą, asmens dokumento duomenis internetiniame puslapyje, svetainėje forume?	taip	3	5%
	ne	53	88%
	(įrašykite savo atsakymą)	4	7%
17. Keliomis paslaugomis (internetinė bankininkystė; elektroninis paštas; prisijungimas prie darbo ar asmeninio kompiuterio; specializuoti internetiniai puslapiai ir t.t.) naudojatės, kuriose Jūsų identifikavimui reikalingas slaptažodis?	viena	1	2%
	dvi	4	7%
	trys	11	18%
	daugiau nei keturios	44	73%
18. Jeigu Jūs naudojatės daugiau nei viena paslauga, kuri reikalauja prisijungimui slaptažodžio, Jūs:	Visoms paslaugoms turite viena slaptažodį, kad lengviau prisiminti	5	8%
	Turite kelis (2-3) slaptažodžius, kuriuos naudojate	40	67%
	Kiekvienai paslaugai skirtingas slaptažodis	15	25%

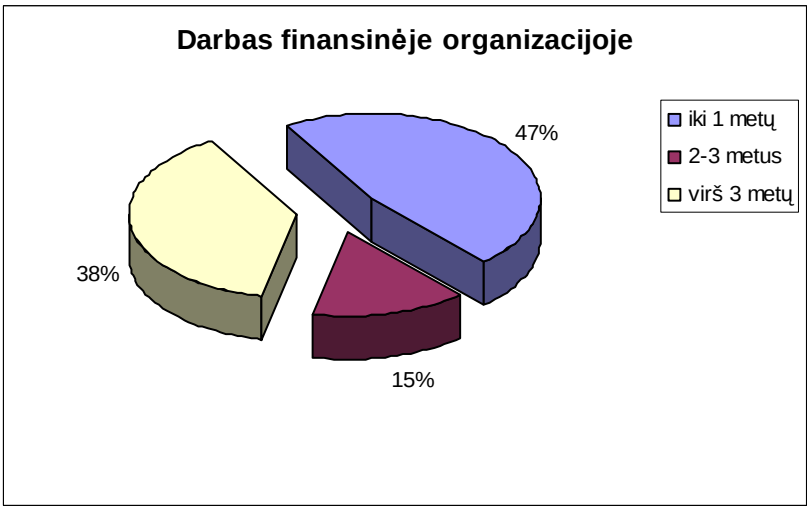
Anketa buvo išsiųsta elektroniniu paštu 158 darbuotojams, iš kurių 38%, t.y. 60 darbuotojų atsakė į anketoje pateiktus klausimus. 87% apklaustųjų darbas yra tiesioginis klientų aptarnavimas ir 5% - iš dalies (3 paveikslas). Taigi 92% apklaustų darbuotojų priklauso padidintos rizikos darbuotojų grupei,

kuriai informacijos sistemos ir joje esančių duomenų apsauga ypatingai svarbus klausimas. 47% respondentų finansinėje įstaigoje dirba iki vienų metų (4 paveikslas) ir jų funkcijos yra tiesioginis klientų aptarnavimas ir bendravimai su jais. Šiems darbuotojams reikia skirti ypatingą dėmesį, kadangi jiems finansinės operacijos dar visiškai naujos ir duomenų apsauga jie mažiausiai gali rūpėti, adaptuojantis įmonėje.

3 Paveikslas. Darbuotojai tiesiogiai aptarnaujantys klientus



4 paveikslas. Darbas finansinėje organizacijoje.



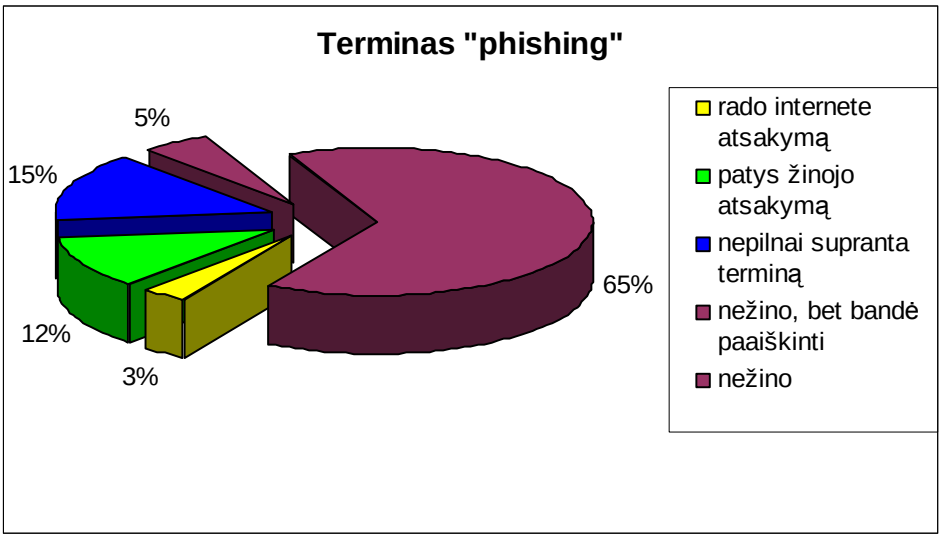
Optimistiškai nuteikia faktas, kad net 73% atsakiusiųjų neatidarinėja prikabintų failų ir nuorodų, kurias gavo į darbinė pašto dėžutę elektroniniu laišku iš nepažystamo adresato. Asmeninėje elektroninio pašto dėžutėje tokių laiškų neskaito 83% respondentų. Rezultatai rodo, kad darbuotojas namie savo

informacijos saugumu rūpinasi labiau nei darbe. Pakeisti rodiklius į darbovietės naudą galėtų mokymai, kurių pagalba darbuotojas suprastų, kad duomenų saugumas darbe toks pat svarbus kaip namie ir net svarbesnis. Akstinas darbuotojui labiau saugoti duomenų konfidencialumą yra supratimas, jog nuo to, ar duomenys išliks saugūs priklauso jo karjera, alga ir net darbo vietos išsaugojimas.

Nagrinėjant atakas, kurių šaltinis yra internetas, matyti, kad darbuotojai nėra linkę tapti įrankiu „spam“ atakoms, kai laiškuose prašoma persiųsti laišką kuo daugiau adresatų, siekiant sulėtinti arba nutraukti elektroninio pašto serverio veiklą. 68% respondentų nepersiuntinėja „spam“ tipo laiškų ir 25% persiuntinėja retai.

Paprašius darbuotojų paaiškinti terminą „Phishing“, 65% respondentų atsakė, jog nežino šio termino. Vienas darbuotojas atsakė, jog tingi aiškinti, ką būtų galima prilyginti ir nežinojimui. Likę 35%, t.y. 21 darbuotojas bandė paaiškinti, kurių atsakymus galima suskirstyti į kelias grupes, kurios pavaizduotos paveiksle nr. 5.

5 Paveikslas. Terminas „Phishing“



3% darbuotojų termino „phishing“ prasmės nežinojo, bet žinos dabar, nes jį rado internete. Įkėlus jų atsakymus į paieškos sistemą www.google.lt jie atitiko keliose svetainėse patalpintus „phishing“ apibrėžimus. Nepilnai suprantančių terminą „phishing“ yra 15%. Vieni darbuotojai žino, jog tai duomenų (internetinio banko slaptažodžiai, kodai) vagystė, kiti, jog tai internetinis sukčiavimo būdas arba patiklių vartotojų paieška. Nežinantys, bet bandę paaiškinti, teigia, jog čia anglų kalbos žargonas ir atitikmuo žodžiui „fishing“. Labiausiai suintrigavo atsakymas, kurį norėčiau pacituoti: „sukčiavimo būdas, kai apsimetėliai internete sukurę analogišką svetainę "sužvejoja" asmens duomenis apgaulės būdu ir jais pasinaudoja - persiveda pinigus iš el. pašto ir pan.“

Darbuotojams būtini apmokymai pavyzdžiais, kurie parodytų ir išryškintų galimus atakų būdus. Atpažinus, internetines ir ne tik, atakas darbuotojui reikalingos instrukcijos, kaip elgtis tokiose situacijose ir kam pranešti.

Svarbus faktas, jog 72% apklaustųjų mažareikšmius popierinius dokumentus darbe sunaikina „krokodilu“ ir 12% išmeta į tam skirtas dokumentų kaupimo dėžes, kurias surenka ir dokumentus sunaikina samdoma firma. Anketoje ne be reikalo paminėtas žodis „mažareikšmius“, siekiant išsiaiškinti ar darbuotojas supranta, kad bet kokie darbo dokumentai yra svarbūs ir kad juos reikia sunaikinti, norint išvengti informacijos saugos pažeidimų.

Sugretinus aukščiau minėtus rezultatus, galime teigti, kad nuo pasyvios socialinių inžinierių atakos darbuotojai atsilaikytų. Taigi nesant konkretiems informacijos saugos mokymams, darbuotojai patys yra sąmoningi ir minimaliai supranta duomenų apsaugos prasmę. Nereikėtų džiaugtis rezultatais, tai tik ženklas, kad saugumo supratimo ir laikymosi kartelę privalu pakelti į aukštesnį lygį.

Kaip minėjau anksčiau, neišvengta to, kad darbuotojai stengdamiesi pasirodyti geriau, stengsis pasirinkti „teisingiausius“ atsakymus. Pasitaikė anketų, kuriose darbuotojai teigia, kad naudodamiesi daugiau nei keturiomis elektroninėmis paslaugomis, kurių prieigai reikalingi slaptažodžiai, pastaruosius keičia kas mėnesį arba kai pareikalauja programa ir kiekvienai paslaugai turi atskirą slaptažodį.

Darbuotojams atsilaikius prieš internetines atakas, socialiniai inžinieriai „puola“ kitomis priemonėmis – skambina telefonu ar net patys atvyksta į įmonę. 2% apklaustųjų pasakytų skambinančiajam jo sąskaitos numerį, 48% - nesakytų ir net 50% pasakytų, kai tik identifikuotų skambinantįjį. Deja nėra bendros tvarkos kaip identifikuoti asmenį, kuris skambina telefonu, todėl telefonu teikiama tik bendra informacija apie paslaugas. Socialiniam inžinieriui nesukeltų didelių problemų sužinoti, kad ir ne visą norimą, bet dalį informacijos, kurią susisteminus gautų visus geidžiamus duomenis.

Socialiniam inžinieriui pasirodžius darbovietėje informacijos jis galėtų prisirinkti iš 18% respondentų kompiuterio ekranų, kurie neužrakinami paliekant darbo vietą. Reikia pridurti, kad įmonė naudoja automatinį ekrano užrakinimą, kuris suveikia tik po pakankamai ilgo laiko tarpo, kurio užtektų įsibrovėliui. Tiek pat , 18% kompiuterių ekranus užrakina tik kartais. 2% apklaustųjų slaptažodžius skirtus prisijungti prie specializuotų interneto svetainių ar informacijos sistemų yra užsirašę ant lapuko ir turi juos darbe. 13% taip pat turi tokius lapelius, bet juo užrašyti ne visi slaptažodžiai – kitus jie prisimena mintinai. Peržvelgus anketas atidžiau matyti:

- kad lapelius su slaptažodžiais turi tik tie darbuotojai, kurie nerakina kompiuterio ekrano, arba rakina tik kartais;

- darbuotojai turintys užrašytus slaptažodžius, juo sugalvoja nesudėtingus, t.y. susidedančius iš raidžių;
- dauguma darbuotojų, kurie turi užrašytus slaptažodžius, prieigai prie specializuotų internetinių puslapių ir informacijos sistemų turi du arba tris slaptažodžius, kuriuos naudoja.

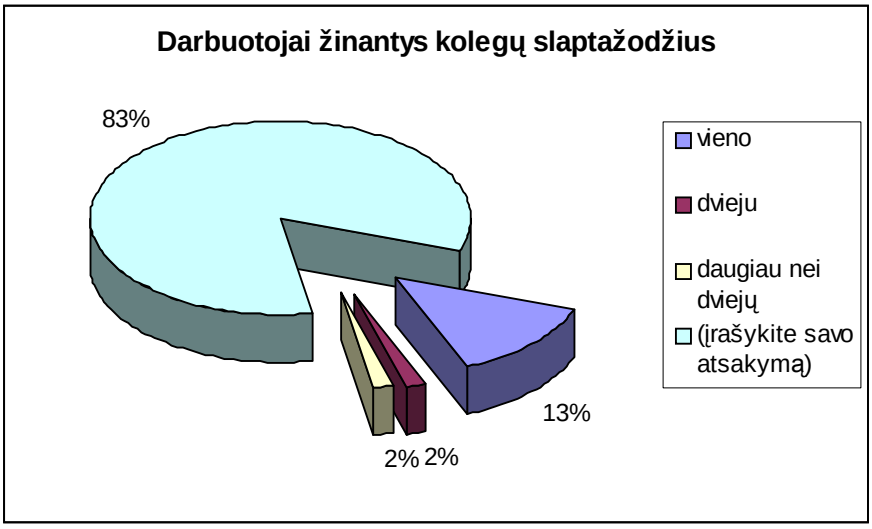
Tokie darbuotojai gali tapti lengvomis aukomis piktavaliams organizuojant juodus darbus. Siekiant turėti saugią informacijos sistemą, reiktų, įdiegti švaraus stalo politiką, bei techninėmis priemonėmis sugriežtinti slaptažodžių naudojimo tvarką prisijungiant prie kompiuterių ir specializuotų programų:

- reikalauti sudėtingesnių slaptažodžių;
- dažniau prašyti pasikeisti slaptažodžius;
- neleisti vesti tų pačių slaptažodžių (pvz. negali būti panašūs paskutiniai penki slaptažodžiai).

Ne įmonės darbuotojui, gal net socialiniam inžinieriui, priėjus prie darbuotojo ir paminėjus aukštesnes pareigas užimančių darbuotojų pavardes ir paprašius atlikti vienokius ar kitokius veiksmus, šiuos reikalavimus patikrintų 57% respondentų, tuo tarpu net 17% nesuabejotų ir įvykdytų paliepimus. Privalu įgyvendinti tvarką, kurioje griežtai apibrėžiama, kas gali ir kokio pobūdžio užklausas teikti ir kokios informacijos prašyti, bei kaip elgtis jei informacijos prašo tie, kurie neturi tokių teisių.

Prisimenant teiginį, jog didžioji dalis informacijos saugumo pažeidimų įvykdo darbuotojai, sveikintinas rezultatas yra tai, kad 83% apklaustųjų nežino kolegų slaptažodžių naudojamų prisijungiant prie kompiuterio ar informacinės sistemos. Anketoje šis pasirinkimas nebuvo pateiktas, norint išgauti tikrąjį atsakymą, taigi darbuotojai patys įrašė atsakymą, jog nežino kitų darbuotojų slaptažodžių. Nors nežinojimas gali virsti žinojimu, jei apsilankytumėme prie darbuotojų kompiuterių, kurie turi užsirašę slaptažodžius ir laiko juos darbe. Vis dėlto 17% apklaustųjų žino kolegų slaptažodžius, kas sudaro prielaidą apsimetus kitu vartotoju pažeisti informacijos sistemos saugumą (6 Paveikslas).

6 Paveikslas. Darbuotojai žinantys kolegų slaptažodžius.



4.2. Suvaidinta situacija

Antroji tyrimo dalis pradėta vykdyti praėjus savaitei po pirmosios dalies, t.y. anketos. Toks principas pasirinktas todėl, kad darbuotojai grįžo į įprastinį darbo ritmą, bei pamiršo anketą ir jos klausimus. Tikėtasi, jog darbuotojai grįžo į rutiną, susikoncentravo į darbą ir galbūt prarado budrumą.

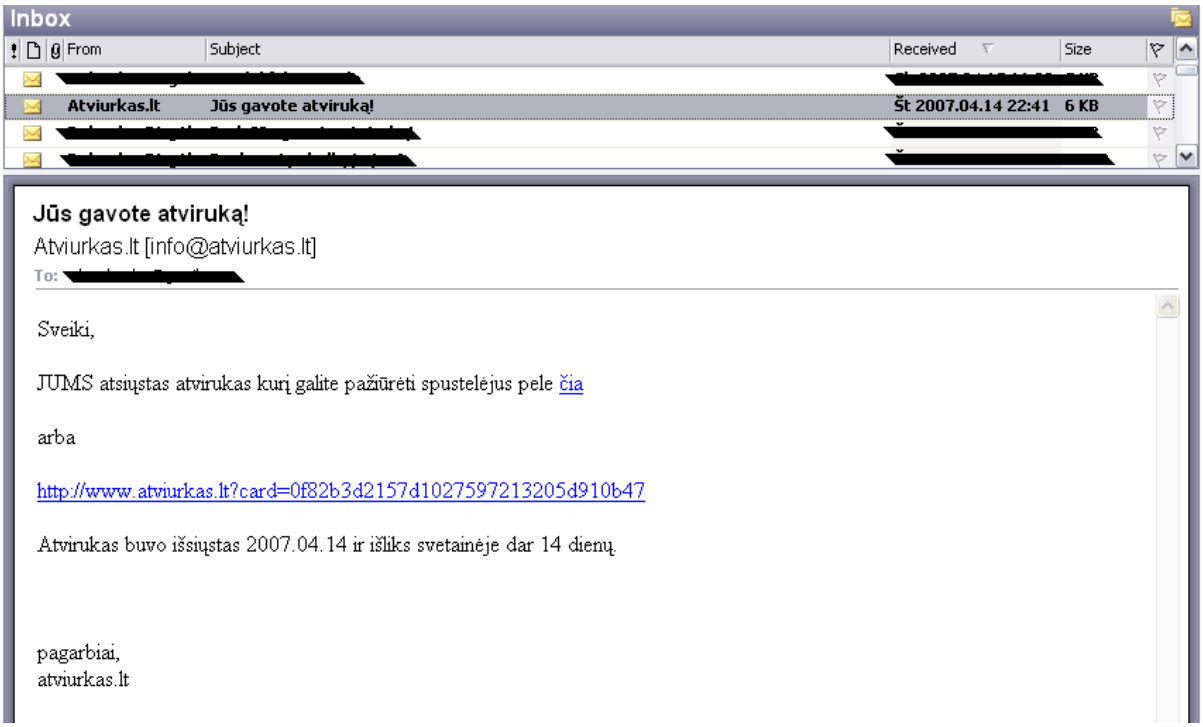
Suvaidintos situacijos esmė tokia:

- ar tikrai darbuotojai, kaip jie teigia, neatidarinėja nuorodų elektroniniuose laiškuose, kurie atsiųsti nežinomų siuntėjų;
- sužinoti ar darbuotojai linkę atskleisti konfidencialią informaciją, šiuos atveju savo slaptažodžius;
- ar darbuotojai atpažins ataką ir apie ją praneš.

Darbuotojams (tie patys, kurie elektroniniu paštu gavo anketą) buvo siunčiamas elektroninis laiškas iš nepažystamo adresato su prašymu įvesti slaptažodį. Siuntėjas yra fiktyvi svetainė www.atviurkas.ten.lt su elektroniniu adresu info@atviurkas.lt. Taigi darbuotojas gauna elektroninį laišką, iš siuntėjo Atviurkas.lt (7 Paveikslas). Klaida įvelta neatsitiktinai, o dėl kelių priežasčių:

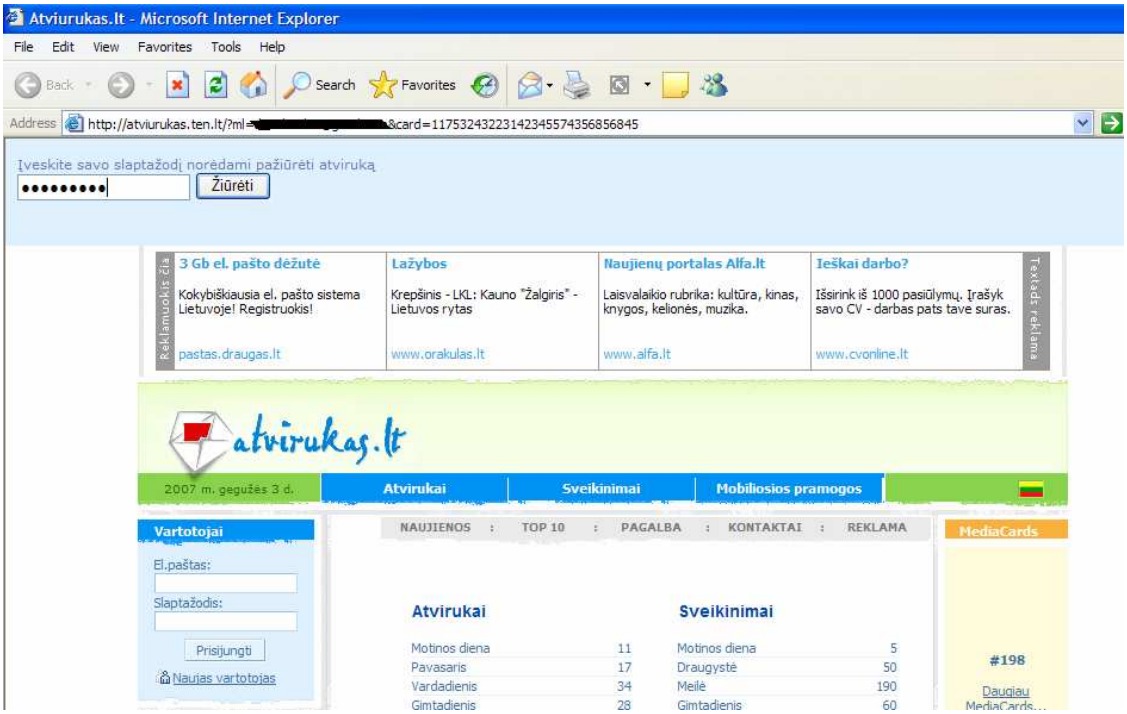
- Atvirukas.lt yra registruotas ženklas, siekiant išvengti konflikto jo naudoti negalima;
- Patikrinti darbuotojų budrumą.

7 Paveikslas. Elektroninis laiškas



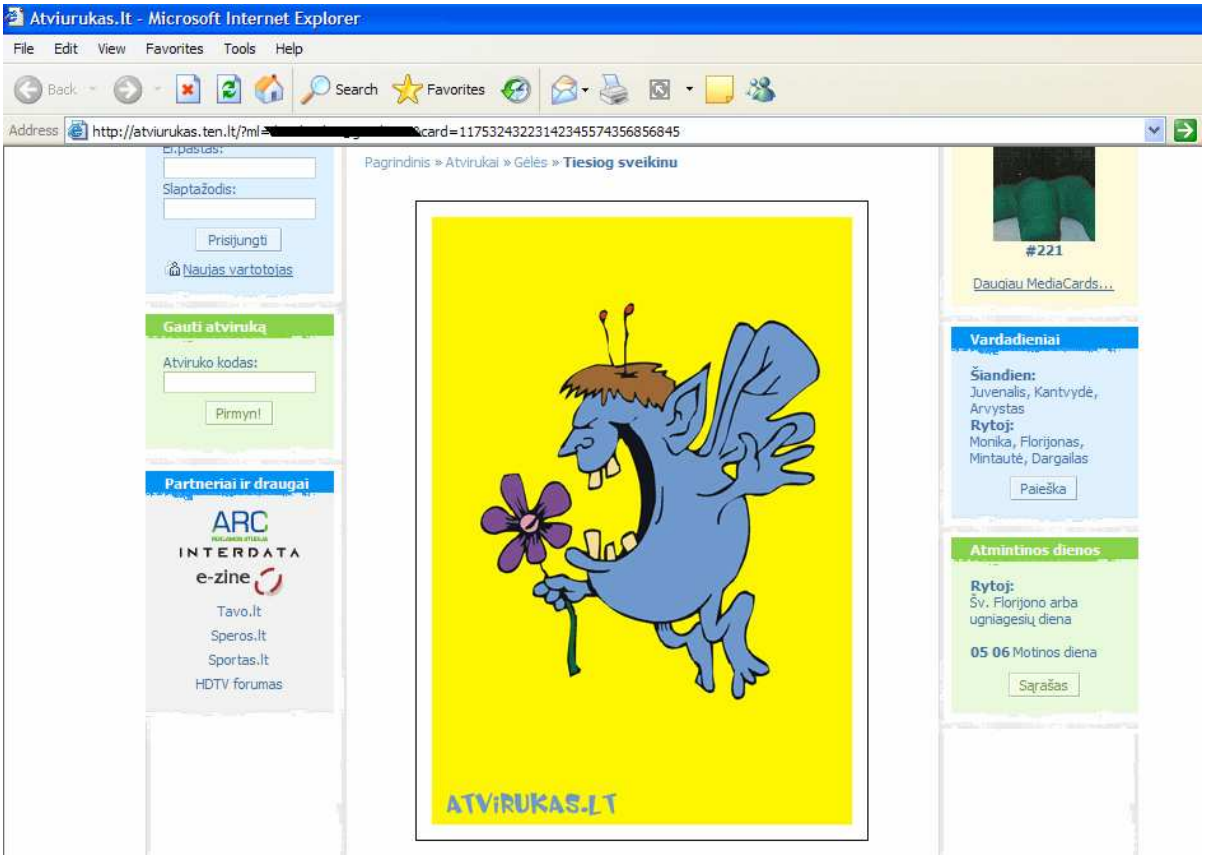
Laiške nurodoma, kad adresatui atsiųstas atvirukas, kurį peržiūrėti galima paspaudus nuorodą. Darbuotojui paspaudus ją, atsidaro naujas langas kuriame prašoma suvesti slaptažodį (8 Paveikslas).

8 Paveikslas. www.atviurkas.lt



Prašyme nenurodoma kokio reikia slaptažodžio, tiesiog norima pažiūrėti ar darbuotojas linkęs atskleisti informaciją vedamas smalsumo ir dirbdamas rutinoje, kurioje slaptažodžių naudojimas įprastas dalykas. Suvesti galima bet kokius simbolius ir tik suvedus yra parodomas atvirukas (9 Paveikslas) . Kita šio tyrimo pusė yra pažiūrėti ar darbuotojas supras, kad tai gali būti ataka, bei praneš vadovams.

9 Paveikslas. Ilgai lauktas atvirukas.



Kiekvienas darbuotojo apsilankymas puslapyje paspaudus nuorodą užrašomi specialiame faile, kuriame matyti, kuris elektroninio pašto adresatas paspaudė ir kada paspaudė nuorodą. Darbuotojui suvedus simbolius į prašomo slaptažodžio lauką, suvesti duomenys, elektroninio pašto adresas ir laikas kada buvo suvesti simboliai saugomi kitame faile. Taigi užfiksuota kiek darbuotojų paspaudė nuorodą, kada paspaudė, bei ką suvedė.

Vykdydamas tyrimą susidūriau su problemomis, kurias galėčiau išskirti į dvi grupes:

- Techninės problemos;
- Reguliacinės problemos, siekiant nepažeisti suinteresuotų grupių teisių.

Techninių problemų identifikavimas ir pašalinimas nesukėlė didesnių sunkumų, deja jų nepašalinus tyrimo eiga būtų sudėtingesnė. Pirmiausia teko tikrąsias internetinių puslapių nuorodas slėpti,

kad darbuotojas nepastebėtų, jog keliauja į puslapį kitu vardu. Akylesnis darbuotojas atsistojęs pelės kursoriumi ant nuorodos lengvai pamatytų tikrąjį svetainės adresą. Programinis kodas, kuris siunčia laiškus ir renka duomenis, kuris darbuotojas atidarė laišką ir ką suvedė buvo patalpintas išoriniame serveryje. Išsiuntus bandomąjį laišką, paaiškėjo, kad finansinės institucijos pašto programa pakeičia laiško formatą į tekstinį. Tekstiniame laiško formate parodomos tikrosios nuorodos, kurios dabar yra neaktyvios, t.y. paspaudus pelyte ant jų, neatidaromas internetinis puslapis. Vienintelis būdas pažiūrėti atviruką yra nukopijuoti nuorodą ir įkelti į interneto naršyklę. Be viso ko, taip išdarkytas laiškas nukeliamas į nepageidautinų laiškų aplanką, taip sumažinama galimybė, kad darbuotojas jį pastebės. Pastebėjus laišką nepageidautinų laiškų aplanke retas, kuris skaitytų jį, o tuo labiau spaustų nuorodas esančias jame. Ši problema išsisprendė išsprendus reguliacines problemas, kurias išvardinsiu sekančioje pastraipoje.

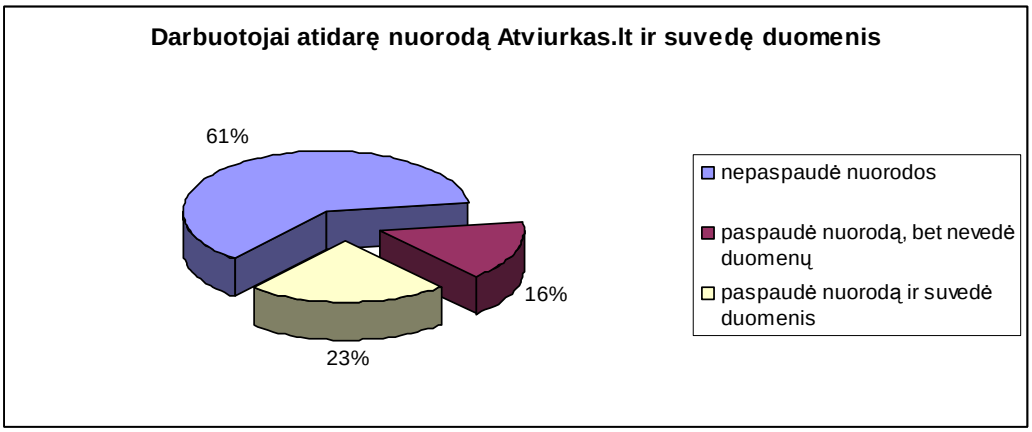
Reguliacines problemas įvardinčiau tas, kurios iškilo ir yra susijusios su finansine įmone, jos pageidavimais ir apribojimais. Tyrimo eigą derinant su Informacinių technologijų departamentu ir operacinės rizikos skyriumi buvo iškelta problema dėl darbuotojų identifikavimo pagal elektroninį paštą ir jų suvestų duomenų saugojimą ir saugumą išoriniame serveryje patalpintuose failuose. Įvertinus riziką, kad duomenų konfidencialumas gali būti pažeistas iškelti keli pasiūlymai:

- Nesaugoti elektroninio pašo adresų;
- Riboti suvedamų duomenų ilgį saugomame faile.

Nesaugant elektroninio pašto adresų būtų sunku atlikti tyrimo analizę, kurios būdu siekčiau išsiaiškinti ryšius tarp anketos atsakymų ir „phishing“ atakos. Derybų metu prieitas vieningas sprendimas – programinį kodą patalpinti vidiniame įmonės serveryje, kuriame duomenys būtų saugesni. Tai įvykdžius išsisprendė problema dėl laiško konvertavimo į tekstinį formatą ir perkėlimo į nepageidaujamų laiškų aplanką. Prašymas riboti įvedamų duomenų ilgį buvo įvykdytas. Darbuotojai puslapyje suvesti galėjo kiek nori simbolių, bet į failą, laikantis saugumo reikalavimų, buvo saugoma tik pirmi keturi simboliai.

Išsiuntus laiškus 158 įmonės darbuotojams, 61 darbuotojas t.y. 39% visų gavusių laišką paspaudė nuorodą pateiktą (8 Paveikslas). Panašus aktyvumas buvo ir atsakinėjant į anketos klausimus.

8 Paveikslas. Darbuotojai atidarę nuorodą Atviurkas.lt it suvedę duomenis

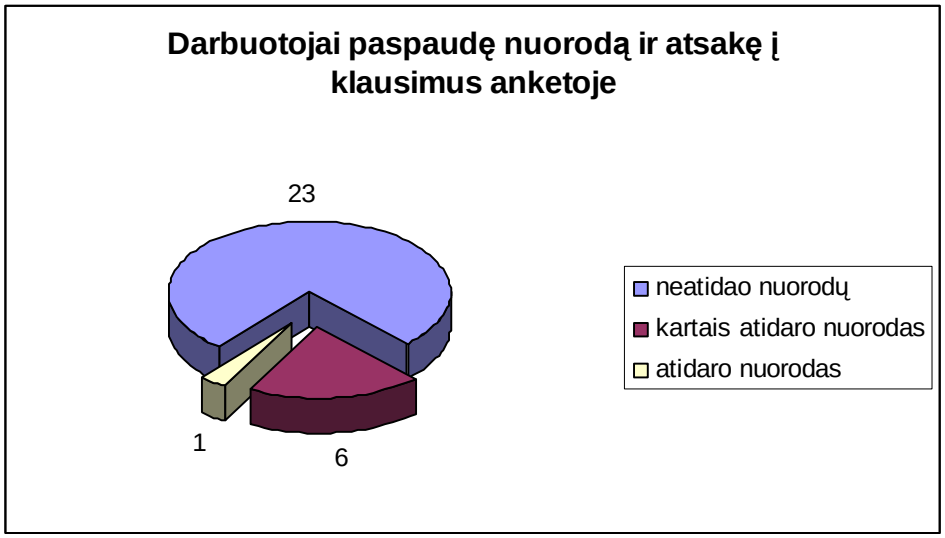


Atrodo nieko tokio nenutiko, jog darbuotojai atidarė nuorodą, pateiktą elektroniniame laiške. Labiau verčia sunerimti faktas, kad 36, t.y. dagiau nei pusė iš 61 atidariusių nuorodą, suvedė simbolių sekas, tariamus slaptažodžius. Tiesa, patikrinti ar suvesti simboliai tikrai yra slaptažodžiai neįmanoma, nes turime tik pirmus keturis simbolius, bet daryti prielaidas galime. Dauguma atidariusių nuorodą neskubėjo vesti slaptažodžio, bandė atnaujinti atidarytą puslapį, išjungdavo ir vėl jį įjungdavo. Smalsiausieji atidarę puslapį ketvirtą ar penktą kartą neatlaikydavo ir suvesdavo tariamą slaptažodį. Iš 36 suvestų simbolių eilučių, tik 2 įrašai panašūs ir padrikus kompiuterio klavišų paspaudimus. 34 simbolių eilutės, kurio susideda iš keturių simbolių panašios į galimus slaptažodžių pradžias. Vienas respondentas suvedė pirminio slaptažodžio simbolius, kuris naudojamas pirmą kartą prisijungiant prie įmonės informacijos sistemos ir iškart turi būti pakeistas į savo sugalvotą slaptažodį. Vienam iš suvedusiųjų slaptažodį taip patiko atvirukas, kad jis jį peržiūrėjo net penkis kartus, visus kartus suvesdamas tuos pačius simbolius. Socialiniam inžinieriui surinkti slaptažodžiai tikrai pagelbėtų vykdant tolesnius sumanymus.

Sugretinus anketos duomenis su atliktos „phishing“ atakos duomenimis matyti, kad 30 apklaustųjų atsakė į anketos klausimas, bei atidarė nuorodą atsiųstame laiške. Dar kartą pasitvirtino tai, kad respondentai stengiasi pasirodyti kuo geriau, atsakinėdami į anketos klausimus, bet realioje situacijoje elgiasi kitaip.

Paveiksle numeris 9 matyti, kad 23 respondentai anketoje teigia, jog neatidarinėja nuorodų ar prisegtų failų pateiktų elektroniniuose laiškuose, kuriuos gavo iš nepažystamų adresatų, nors nuorodą paspaudė. Tik vienas respondentas pasakė teisybė, jog atidarinėja nuorodas gautas iš nepažystamų elektroninio pašto adresatų.

9 Paveikslas. Darbuotojai paspaudę nuorodą ir atsakę į klausimus anketoje



Dar daugiau respondentų, net 27 neveda asmeninių duomenų internetinėse svetainėse, 2 asmenys tik kartais. Prisimenat faktą, jog labai mažai respondentų yra suvedę asmeninius duomenis internetiniame puslapyje, vis dėl to 19 respondentų suvedė simbolių eilutes, nors anketoje visi vieningai teigia, jog neveda. Taigi apklausa ne visada parodo tikrąsias žinias apie saugumą, bei ar laikomasi jo. Tuo tarpu suvaidinta situacija arba testavimas parodo tikrąsias žinias ir supratimą. Darbuotojai supranta, kad atskleisti duomenų nevalia, bet elgiasi priešingai.

Konfidencialių duomenų atskleidimu, matyt, respondentai laiko situaciją, kuri nėra įprastą jų gyvenime, išsiskiria iš rutinos. Pvz. kai prieina nepažystamas žmogus ir paprašo pasakyti mokėjimo kortelės PIN kodą. Tikrai nei vienas nepasakytų. Prašymą suvesti slaptažodį, jei nori pamatyti atviruką, respondentai priėmė, kaip normą, rutinos dalį neišsiskiriančia nieko iš kitų veiksmų, nes visur prisijungiant – darbovietės IS, specializuoti internetiniai puslapiai, elektroninis paštas ir pan.jų prašo slaptažodžio. Taigi nejausdami ir nesuprasdami grėsmės darbuotojai pasielgė, jų manymu įprastai.

Laukiami rezultatai buvo pamatyti ar darbuotojai yra susirūpinę tik savo duomenų saugumu ir nepasiduos provokacijai suvesti slaptažodį, bet pasirūpins ir kolegų, bei visos įmonės gerove ir reputacija. Sveikintinas rezultatas yra tai, kad 61% respondentų visai neatidarė nuorodos, o 16% atidarė, bet nepasidavė provokacijai ir neatskleidė galimai konfidencialių duomenų. Karti teisybė tokia, kad užtenka vienam iš tūkstančio darbuotojų suklupti ir atakuotojas susikurs kelią prie norimų duomenų informacijos sistemoje, nors likę devyni šimtai devyniasdešimt devyni nepriekaištingai laikysis saugumo politikos.Užkirsti kelią tyrimui lengvai galėjo, bet kuris darbuotojas, kuris atidarė nuorodą ir pamatė, jog

jo prašoma slaptažodžio. Tokie slaptažodžių prašinėjimai ar panašūs būdai, kuriais bandoma išvilioti konfidencialią informaciją turėtų sukelti darbuotojams įtarimus. Šiuo atveju darbuotojas, įtaręs klastą ar galimą ataką turėtų skambinti atsakingam asmeniui ir pranešti susidariusią situaciją. Laiku informavus atsakingus asmenis didėja tikimybė, jog toks šnipinėjimas ir slaptažodžių rinkimas bus operatyviai sustabdytas, ko išdavoje informacijos sistemų saugumas nebus pažeistas. Deja nei vienas darbuotojas nepranešė apie įtartiną veiklą ir slaptažodžių rinkimą.

Apibendrinant atlikto tyrimo rezultatus galiu teigti jog esama padėtis informacijos sistemų apsaugos procesuose yra gera ir nuteikia optimistiškai. Respondentai žino pagrindinius duomenų apsaugos principus, bei supranta informacijos svarbą ne tik namuose, bet ir darbo vietoje. Dauguma apklaustųjų, kaip parodė tyrimo antroji dalis, laikosi duomenų saugumo principų, kuris labiau paremtas ankstesniu patyrimu ir reagavimu į apklinką, o ne vidiniais apmokymais. Aukščiausiai įmonės valdžiai suprantant saugumo politikos svarbą ir palaikant jos įgyvendinimą, atsakingo personalo tikslas siekti gilesnio darbuotojų saugumo supratimo ir jo laikymosi. Pagirtina yra tai, kad techninėmis priemonėmis sugriežtinta slaptažodžių naudojimo politika. Siekti veiksmingesnio saugumo padės darbuotojų apmokymai, testavimas, rezultatų apžvalga ir vėl apmokymai, testavimas...

5. Esama situacija ir prognozės

Tyrimą atlikus finansinėje įmonėje, kurioje duomenų apsaugai turi būti skiriamas ypatingas dėmesys, galime spręsti apie duomenų saugumą kitose Lietuvoje veikiančiose įmonėse. Visas įmones, pagal duomenų apsaugos lygį, lyginant su nagrinėta finansine organizacija galiu suskirstyti į tris grupes:

- Aukštesnis ir panašus;
- Žemesnis;
- Nesantis

Tikėtina, kad aukštesnis ar panašus duomenų saugumo supratimas yra ir kitose finansinėse įmonėse; stambiose organizacijose, kuriose duomenų perdavimo, gavimo ir kaupimo procesai yra pilnai kompiuterizuoti ir naudojamos informacinės sistemos; organizacijose, kurias valdo užsienio vadovai ir investuotas užsienio kapitalas. Tai įmonės, kuriose saugumo politika, veiksmai ir uždaviniai siejasi su įmonės uždaviniais ir atitinką vidinę jos kultūrą, bei jaučiama vadovų parama.

Prie žemesnio lygio priskirčiau vidutinio dydžio įmones, kuriose vadovai tik pradeda suprasti saugumo politikos svarbą, bet dar nelinkę investuoti pinigų į ją. Tokiose įmonėse sukurta saugumo politika pakankamai primityvi.

Įmones, kuriuose saugumo nerasi nė su žiburiu, būtų mažos ir vidutinės. Šių įmonių vadovai nesirūpina informacijos apsauga, o visą veiklą sukoncentravę į didesnio pelno siekimą.

Esant tokiai situacijai, saugumo politikos supratimo ir kūrimo atžvilgiu, negalime trypčioti vietoje, džiaugdamiesi esamais laimėjimais. Nūdienos aplinkoje vis sparčiau plinta ir tobulėja informacinių technologijų bazėje sukurti darbo įrankiai. Darbui su moderniomis IT priemonėmis pasirengusi vis didesnė visuomenės dalis. Puikiai matyti, kad socialinės inžinerijos apraiškos, kurios aktyviai veikė ir davė vaisius prieš keletą metų užsienyje pagaliau atėjo ir į Lietuvą. Deja ne visi sugebėjo pasimokyti iš kitų klaidų. Dabar, laiko tarpas per kurį socialinės inžinerijos metodai pritaikomi ir Lietuvoje darosi vis trumpesnis, ir vis dažniau žengia koja kojon. Lieka tik nesustoti, o veržtis į priekį, sekti vykstančius įvykius pasaulyje ir namie, bei reaguoti į juos. Taip visuomet turėsime sąmoningus darbuotojus ir saugias informacijos sistemas.

Išvados

Surinkta ir apibendrinta informacija apie socialinės inžinerijos atakas, leidžia suprasti jos veikimo principus ir būdus. Tik žinodami, kaip veikia socialiniai inžinieriai suprantame jos mastus ir galimybes. Identifikavę resursus, duomenis, kuriuos norime apsaugoti, ir supratę apsaugos politikos prasmes bei principus galime siekti efektyvaus duomenų saugumo.

Informacijos sistemų apibrėžimų įvairovė rodo, kad ji apima įvairius pasaulio ir kasdieninės būties reiškinius. Ji labai plati, pasižymi įvairiomis savybėmis. Šiandieninis informacijos supratimas siejamas su informacinės veiklos kompiuterizavimu, naujomis technikos rūšimis, informacijos apdorojimo, saugojimo ir perdavimo technologijomis.

Uolūs technikai kruopščiai kūrė apsaugos sistemas, kurių nebūtų galima apeiti ir informacija išliktų konfidenciali, nepažeista ir prieinama. Deja jie pamiršo vieną grandį – žmogų. Nepaisant žmogiškojo intelekto mes keliama didelę grėsmę informacijos sistemų saugumui. Neužtenka turėti geros techninės ir programinės apsaugos sistemos, kartu su ja turi dirbti sąmoningas, informacijos saugos prasme, darbuotojas. Žmogiškasis faktorius yra ypač svarbus veiksnys tiek namų ūkyje, tiek įmonės informacinių technologijų sektoriuje. Dėl vartotojo aplaidumo, neatidumo ar lengvabūdiškumo galimi duomenų praradimai, finansiniai nuostoliai ir pan. Žmogiškas faktorius yra ne antrinis, o bene vienas svarbiausių kompleksinių veiksnių, kalbant apie informacijos sistemų bei žinių visuomenės saugumą.

Informacinių technologijų plėtra suteikia ne tik naujas galimybes, bet ir atveria papildomas grėsmes. Saugumo politika turi būti orientuota į gaisro vengimo taktiką, t.y. prevencines priemones, kaip išvengti grėsmių, o ne į kovojimą jau su kilusiu gaisru. Tiesa, pamiršti saugumo politikoje, kaip kovoti ir pašalinti pasekmes jei saugumas buvo pažeistas nedera. Saugumo politika yra tęstinis procesas.

Apsaugos produktų paskirtis kompanijose apsaugoti nuo „žalių“ hakerių, kurie sukeliu tik mažus trukdžius. Didžiuosius praradimus sukelia profesionalai, kurie žino ką daro ir taip užsidirba pragyvenimui. Kol jaunimas taikosi į kiekybę, profesionalai koncentruojasi į kokybę. Įsilaužėliai stengiasi apeiti galimas apsaugos sistemas ir dažnai puola žmones, kurie naudojasi tomis apsaugomis sistemomis. Apsauga per dažnai yra tik iliuzija, o iliuzija yra labai pavojinga kai šalia atsiranda patiklumas ir nemokšiškumas. Albertas Einšteinas pasakė – „tik du dalykai yra begaliniai, visata ir žmogaus kvailumas, bet dėl pirmojo aš nesu visiškai užtikrintas“. Socialinio inžinieriaus atakos gali pasiekti tikslą kai žmonės yra kvaili, bet dažniausiai nesivadovauja gera apsaugos praktika (o gal net nežino apie tokią). IT profesionalai tiki, kad sistema saugi, nes instaliuota naujausia ir brangiausia ugniasienė, įsibrovimo aptikimo sistema, tobulesnė

atpažinimo technologija. Anksčiai ar vėliau socialiniam inžinieriui susidomėjus organizacija saugumas bus pažeistas pasinaudojus apgaule, kuriuos nesuseks jokia technika.

Kiekviena darbovietės pozicija turi savo specifinius pažeidžiamumus, kuriuos reikia identifikuoti ir stengtis, kad šie nebūtų išnaudoti. Pasiekto efektyvaus saugumo, kalbant apie žmogiškąjį faktorių, padės personalo ugdymas, esamos saugumo politikos peržiūrėjimas, tobulinimas ir vėl apmokymai.

Apibendrinus tyrimo duomenis galime teigti, jog informacijos sistemų apsauga, kuri orientuota į žmogiškąjį faktorių, Lietuvoje rūpinasi nedaugelis įmonių. Tokia situacija susiklostė todėl, kad dauguma už apsaugą atsakingų asmenų, įmonėse orientuojasi į technologijomis paremtą prevenciją ir kovą su duomenų saugumo pažeidimais ir pamiršo žmogų, kuris naudojasi šiomis apsaugos ir informacijos sistemomis. Integruojantis į pasaulines rinkas, nykstant bendravimo barjerams mes iš pasaulio gauname ne tik gera, bet ir bloga. Teisingas kelias į efektyvų saugumą – rūpintis visomis apsaugos sistemos grandimis. Turėdami gerą saugumą galėsime drąsiai jaustis informacinių technologijų globalizacijos visumoje.

Apibendrinant žinias gautas nagrinėjant teoriją su atliktu tyrimu, galime teigti jog, turėdami pačią brangiausią ir geriausią apsaugos sistemą, negalime būti 100% saugūs, kol neturime sąmoningo ir apmokyto personalo. Personalo, kuriam saugumo laikymasis yra darbo dalis, tokia pat svarbi kaip ir tiesiogiai atliekamos funkcijos, o ne veiksmas trukdantis efektyviai dirbti. Kiekvienas kompiuteris turi žmogų, kuris juo naudojasi, taigi jei tu valdai žmogų – valdai ir kompiuterį. Apsauga turi laimėti visada, įsibrovėliui pakanka laimėti tik vieną kartą.

Bibliografinių nuorodų sąrašas

1. BISHOP, Matt. *Computer security: art and science*. Addison Wesley, 2002. 1136 p. ISBN 0-201-44099-7.

2. Gonzalez J.J., Sawicka A. *A framework for human factors in information security*. WSEAS conference on information security, Rio De Janeiro 2002.

3. Information technology – Code of practice for information security management. International Standard ISO/IEC 17799:2000 (E). First edition 2000.12.01

4. Krause M., Tipton H.F. *Handbook of information security management*. CRC press LLC, 1998. ISBN 0849399475

5. Mitnick K.D., Simon W.L. *The art of deception: Controlling the human element of security*. Indianapolis: Wiley Publishing, Inc., 2002. 368 p. ISBN 978-0-471-23712-9.

6. Mitnick K.D. Simon W.L. The *art of intrusion: The real stories behind the exploits of hackers, intruders and deceivers*. Indianapolis: Wiley Publishing, Inc., 2005. 261 p. ISBN 0-7645-6959-7.

7. Rizikos analizės vadovas. *Administracinių ir techninių gebėjimų stiprinimas užtikrinant duomenų informacinių technologijų ir jomis perduodamų duomenų apsaugą.* Lietuvos Respublikos Vidaus Reikalų Ministerija. Vilnius: Vaga, 2005. 161 p. ISBN 54150118271.

8. ALLEN, Malcolm. *Social engineering. A means to violate a computer system* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 16 d.]. Prieiga per internetą: <http://www.sans.org/reading_room/whitepapers/engineering/529.php?portal=ac26c73224f9a30ead6b39754ca9e75d>.

9. ANUCHA, Zach. *The human factor in information security* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 21 d.]. Prieiga per internetą: <http://www.bcs.org/server.php?show=ConWebDoc.2790>.

10. DANCHEV, Dancho. *Reducing "Human factor" mistakes* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 14 d.]. Prieiga per internetą: <http://www.windowsecurity.com/articles/Reducing_Human_Factor_Mistakes.html>.

11. DOLAN, Aaron. *Social engineering*. [Interanktyvus]. [Žiūrėta 2007 m. balandžio 24 d.]. Prieiga per internetą: <http://www.sans.org/reading_room/whitepapers/engineering/1365.php?portal=317663e0daf83ed8568e9340b60fd691>.

12. EDGAN, Mark. *Information security and the human factor* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 14 d.]. Prieiga per internetą: <http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=25111&TEMPLATE=/ContentManagement/ContentDisplay.cfm>.

13. Egger F.N., Abrazhevich D. *Security and trust: taking care of the human factor* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 16 d.]. Prieiga per internetą: <http://www.telono.com/research/publications/epso.htm>.

14. GRAGG, David. *A multilevel defence against social engeneering* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 14 d.]. Prieiga per internetą: <http://www.sans.org/reading_room/whitepapers/engineering/920.php?portal=844c86f58416af1edf621832c1d02c5b>.

15. GRANGER, Sarah. *Social engineering fundamentals, part 1: hacker tactics* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 14 d.]. Prieiga per internetą: <http://www.securityfocus.com/infocus/1527>.

16. GRANGER, Sarah. *Social engineering fundamentals, part 2: Combat strategies* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 26 d.]. Prieiga per internetą: <http://www.securityfocus.com/infocus/1533 >.

17. GULATI, Radha.*The treat of social engineering and your defence against it* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 25 d.]. Prieiga per internetą: <http://www.sans.org/reading_room/whitepapers/engineering/1232.php?portal=1dafad06e727d332832bbd1874c292f3>.

18. HINSON, Gary. *Human factors in information security* [Interanktyvus]. [Žiūrėta 2007 m. kovo 18 d.]. Prieiga per internetą: <http://www.infosecwriters.com/text_resources/pdf/human_factors.pdf>.

19. Information systems control journal. *Social engineering: a tip of the iceberg* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 24 d.]. Prieiga per internetą: <http://www.isaca.org/Template.cfm?Section=Article_Index1&CONTENTID=17032&TEMPLATE=/ContentManagement/ContentDisplay.cfm#f5>.

20. JAQUES, Robert. *Human factor essential for IT security*. [Interanktyvus]. [Žiūrėta 2007 m. kovo 20 d.]. Prieiga per internetą: <http://www.vnunet.com/vnunet/news/2167357/human-factor-essential-security>.

21. KRATT, Heather. *The inside story: a disgruntled employee gets his revenge* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 25 d.]. Prieiga per internetą: <http://www.sans.org/reading_room/whitepapers/engineering/1548.php?portal=273639268dd867c9d74d01d498e470c7>.

22. MCDEMOTT, Jeff. *Social engineering – the weakest link in information security* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 25 d.]. Prieiga per internetą: <http://www.windowsecurity.com/whitepaper/Social-Engineering-The-Weakest-Link.html>.

23. PATRICK, Andrew. *Human factors of security systems: A brief review* [Interanktyvus]. [Žiūrėta 2007 m. kovo 18 d.]. Prieiga per internetą: <http://www.andrewpatrick.ca/passwords/passwords.pdf>.

24. PRATT, Mary K. *Security‘s human factor* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 17 d.]. Prieiga per internetą: <http://www.microsoft.com/business/momentum/content/article.aspx?contentId=1297>.

25. RUSCH, Jonathan J. *The social engineering of internet fraud* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 14 d.]. Prieiga per internetą: <http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm>.

26. SCHWARTZ, Mathew. *Organization neglect human factors in Security* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 16 d.]. Prieiga per internetą: <http://www.itcinstitute.com/display.aspx?id=363>.

27. SOPRANOV, Konstantin. *The human factor and information security* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 15 d.]. Prieiga per internetą: <http://www.viruslist.com/en/analysis?pubid=176195190>.

28. THOMPSON, Kerry. *Human factor in managing IT security systems* [Interanktyvus]. [Žiūrėta 2007 m. vasario 4 d.]. Prieiga per internetą: <http://www.windowsecurity.com/whitepapers/Human-Factors-Managing-IT-Security-Systems.html>.

29. TRECK, Denis. *Security models: refocusing on the human factor* [Interanktyvus]. [Žiūrėta 2007 m. balandžio 26 d.]. Prieiga per internetą: <http://www.computer.org/portal/site/computer/menuitem.5d61c1d591162e4b0ef1bd108bcd45f3/index.jsp?&pName=computer_level1_article&TheCat=1001&path=computer/homepage/1106&file=itsystems.xml&xsl=article.xsl&>.

The impact of human factor on IS security

Rolandas Dirgėla

Summary

The main object of work is the impact of human factor on IS security. The main purpose of this work is to show that human factor is very important part of successful information system security policy in organization. Main tasks are in final thesis: define information system, define secure information system, analyze methods of vulnerability information system seizing IS users, define security policy conception, signification and principles, development and implementation security policy pointed to human factor, forecast position of other organization in Lithuania.

Carefully developed and implemented security policy which include all organization layers can protect effectively all organization including IS and data stored in it. The result, which I got from analyzing literature, shows that human factor takes wrong place in security policy because of his unique structure which involves a lot of problems in security policy development and implementation. Most of organizations take only technical measures to ensure IS security and often forget train users for security awareness. IT globalization melts the borders between countries and cultures for this reason attacks on IS will increase rapidly in Lithuania. Research made in financial institution shows real situation of security system in organization and let us prognosticate situation in another Lithuania companies.

Final thesis may be useful companies to improve existing security policies and for people who gain more information on IS security.

Priedai

1 Priedas. Anketų rezultatai pavieniui.

1		X	X					X	X			X			X	X				X		X	X	X				X		X
							X						X	X			X		X											
	X			X	X	X				X	X							X			X				X	X	X		X	
2																										X				
	X	X	X	X	X	X	X	X	X	X	X		X	X	X		X	X	X			X		X	X		X		X	X
												X				X				X	X		X					X		
3												X					X	X	X					X	X					
		X	X	X	X	X	X	X	X	X	X		X		X	X				X	X	X	X			X	X		X	X
	X													X														X		
4		X	X		X	X				X	X	X	X						X			X	X					X		
5	X	X	X	X	X	X	X	X	X	X	X	X	X			X	X	X	X	X	X	X	X		X			X		X
														X	X									X						
																													X	
6	X	X										X	X	X	X	X	X	X		X	X	X	X	X		X	X	X		X
			X				X	X											X											
				X	X	X			X	X	X														X				X	
7																														
			X	X			X	X					X	X	X			X				X	X			X	X		X	
	X	X			X	X			X	X	X	X				X	X			X	X			X	X			X		X
8			X			X	X	X	X	X			X		X	X	X		X	X		X		X	X	X	X	X		
					X						X	X									X								X	
	X	X												X									X							X
				X														X												
9												X			X							X					X	X		
	X	X	X	X	X	X	X	X	X	X	X		X	X		X	X	X	X	X	X		X	X	X	X			X	X
10								X																						
	X	X	X	X		X	X		X	X		X	X		X	X	X	X	X	X	X	X		X	X	X	X			X
					X						X			X														X		
																						X							X	

11						X																							X	
	X	X	X	X	X		X		X	X		X			X	X	X	X	X	X		X		X	X			X		X
											X		X	X							X		X			X	X			
12																										X				
	X	X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X		X	X	X	X			X	X		X
												X								X					X				X	
13	X		X		X		X	X			X			X			X	X						X	X			X		
				X		X			X	X		X			X	X			X	X		X	X			X			X	
		X											X								X						X			X
14		X		X																								X		
			X				X	X		X					X											X			X	
													X						X	X	X						X			X
																X														
	X				X	X			X		X	X		X			X	X				X	X	X	X					
15	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	
							X											X												X
16						X													X					X						
	X	X	X	X	X		X	X		X	X		X	X	X	X	X	X		X	X	X	X		X	X	X	X	X	X
									X			X																		
17																					X									
											X																			
					X		X											X									X	X		
	X	X	X	X		X		X	X	X		X	X	X	X	X	X		X	X		X	X	X	X	X			X	
18																					X									
	X	X		X		X	X	X	X		X		X	X	X		X	X	X	X		X	X		X		X			
			X		X					X		X				X								X		X		X	X	X

1	X				X	X		X			X	X			X		X	X	X				X	X		X	X			X
			X	X			X																						X	
		X							X	X			X	X		X				X	X	X			X			X		
2	X										X		X			X					X									
			X		X	X	X	X	X	X		X			X		X		X	X		X	X	X	X	X	X	X	X	X
		X		X										X				X												
3									X									X		X	X									
	X	X	X	X	X	X	X			X	X	X	X	X		X	X		X			X	X	X	X	X		X	X	
								X							X												X			X
4				X				X				X	X								X					X	X	X		X
5	X			X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			X		X																									
		X																												
6			X	X	X		X		X	X			X	X		X	X	X				X		X		X	X		X	
											X				X				X		X		X					X		
	X	X				X		X				X								X					X					X
7				X																										
	X	X	X		X	X		X							X		X		X	X		X	X		X	X		X	X	
							X		X	X	X	X	X	X		X		X			X			X			X			X
8	X			X			X			X	X						X	X			X				X				X	
		X							X					X		X				X										X
			X		X							X										X	X	X						
						X		X					X		X				X							X	X	X		
9		X				X															X									
																							X							
				X																										
	X		X		X		X	X	X	X	X	X	X	X	X	X	X	X	X	X		X		X	X	X	X	X	X	X
10																														
	X	X	X	X	X	X	X		X	X	X		X		X	X	X		X			X	X	X	X	X	X	X	X	X
												X		X						X	X									
								X										X												

11													X																	
	X	X	X	X	X	X		X			X				X	X		X	X	X	X	X	X	X			X	X	X	X
							X		X	X		X		X			X								X	X				
12														X								X								
	X		X		X	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X		X	X	X	X		X	X	X
		X		X																							X			
13	X				X			X	X	X		X			X			X			X		X	X		X		X		X
		X				X	X						X	X		X			X			X			X					
				X							X																X		X	
			X														X			X										
14				X					X	X					X	X		X												
					X	X	X						X								X				X					
			X								X									X			X				X			
																	X									X				
	X	X						X				X		X					X			X		X				X	X	X
15	X		X	X	X	X	X	X	X	X		X	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X	X
															X															
		X									X					X														
16																														
	X	X		X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
			X						X																					
17																														
																X								X		X				
		X				X				X												X							X	X
	X		X	X	X		X	X	X		X	X	X	X	X		X	X	X	X	X		X		X		X	X		
18	X						X																	X		X				
			X	X	X	X		X	X		X	X	X		X	X	X	X	X		X	X	X		X			X	X	X
		X								X				X						X							X			

2 Priedas. „Phishing“ termino darbuotojų paaiškinimai (paaiškinimai netaisyti)

Paieškos sistemose rasti atsakymai.

- duomenų vagystė. Tai sukčiavimo forma prieš organizacijas ar privačius asmenis, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar falsifikuotais internetiniais tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius ar kitus konfidencialius duomenis.
- sukčiavimo forma, kai pasinaudojant elektroninio pašto žinutėmis siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius ar kitus konfidencialius duomenis.

Terminas paaiškintas savais žodžiais teisingai

- sukčiavimo būdas, kai el.pašte gaunama klaidinga žinutė apie problemas banko duomenų bazėje, raginama prisijungti prie internetinės bankininkystės netikrame puslapyje.
- interneto svetaines kopijos (identiškos tikrajai) sukūrimas ir slaptažodžių, bei kitų asmens duomenų pavogimas iš asmenų kurie ja pasinaudoja.
- "padirbti" puslapiai,dažniausiai atrodantys taip pat,kaip ir originalūs.Naudojami norint iš žmonių išgauti reikalingą informaciją.
- yra puslapiu kur reikia ivesti asmeninius duomenis klonavimas.
- negeros internetinės svetainės, fiktyvios.
- kompiuterinių įsilaužėlių asmeninių duomenų nuskaitymo būdas, siekiant jais pasinaudoti nusikalstamais veiskmais.

Terminas paaiškintas savais žodžiais ir beveik teisingai

- kai norima išgauti kortelės ar internetinio banko slaptažodis.
- bandymas sužinoti elektroninio prisijungimo duomenis.
- gal cia kai sukciai siuntinėja e-mailus kad surinkiti informacija apie gaveja.
- duomenų vagystė.
- informacijos vogimas.
- duomenų vagystė, plintanti pvz. e-laiškais.
- duomenų vagystės naudojant IT.

- Patiklių vartotojų paieška.
- internetinis sukčiavimo būdas.
- sukčiavimo būdas, kai apsimetėliai internete sukurę analogišką svetainę "sužvejoja" asmens duomenis apgaulės būdu ir jais pasinaudoja - persiveda pinigus iš el. pašto ir pan.

Terminas paaiškintas neteisingai

- darbuotojų paieška svetimose kompanijose.
- "Žvejyba" žargonu iš anglu klb.
- Fishing.