INFORMACINĖS SAUGOS AUDITO VYKDYMAS REMIANTIS ISO/IEC 27000 ŠEIMOS STANDARTŲ REIKALAVIMAIS

Andrius Januta, Leonardas Marozas, Nikolaj Goranin
Vilniaus Gedimino technikos universitetas

Įvadas

Šiuolaikinė visuomenė nebeatsiejama nuo modernių informacijos apdorojimo, kaupimo ir perdavimo priemonių. Todėl auga reikalavimai duomenų, kurių pagrindą sudaro konfidencialumas, vientisumas ir prieinamumas, saugumui užtikrinti.

Deja, kad ir kaip naujausios technologijos leistų palengvinti esamų problemų sprendimą, techninės saugos priemonės savaime nėra galutinis tikslas. Tačiau, nepaisant to, saugumas yra „greitai gendanti prekė“, kuri turi būti nuolat atnaujinama [4].

Informacinės saugos užtikrinimo procesą galimą būtų išskaidyti į kelias dalis [1] [2]:

- Objektų, galinčių sulaukti pavojaus, nustatymas.
- Esančių ir galimų pavojų išaiškinimas.
- Galimų pavojaus šaltinių nustatymas.
- Rizikos analizė.
- Neigiamo poveikio šaltinio suradimo metodai ir priemonės.
- Apsaugos nuo žinomų pavojų metodai ir priemonės.
- Reagavimo į incidentus metodai ir priemonės.

Pagrindinis šio straipsnio ***tikslas*** – parodyti, kad specializuoti atviro kodo įrankiai gali būti taikomi, vykdant organizacijos auditą pagal ISO/IEC 27000 šeimos standartų reikalavimus. Atsižvelgianti į suformuluotą tikslą, sprendžiami šie ***uždaviniai***: pateikiama ISO/IEC 27000 šeimos standartų apžvalga, pagrindžiamas Informacinės saugos valdymo sistemos diegimo tikslingumas, parenkami atviro kodo auditavimo įrankiai, atliekamas technologinis saugos auditas pasirinktoje organizacijoje, pateikiami jo rezultatai bei analizė.

Informacinės saugos valdymo sistema

Informacinės saugos valdymo sistema (ISVS) gali būti suprantama kaip atitinkamų politikų rinkinys, kuris yra susietas su informacijos saugumo valdymu (priemonių). Sąvokos atsiradimas siejamas su ISO/IEC 27001 standartu. Pagrindinis šios sistemos principas yra tai, jog organizacija turi sukurti, įgyvendinti ir palaikyti nuoseklius procesus ir sistemas, kurios būtų skirtos informacinio turto rizikai valdyti, tokiu būdu užtikrinant priimtiną organizacijoje informacijos saugumo lygį, apimant konfidencialumą, vientisumą ir prieinamumą.

Be ISO/IEC 27000 šeimos standartų, egzistuoja ir kitų ISVS modelių, aprašomų ISF (Informacijos saugumo forumo) organizacijos „Standard of Good Practice (SOGP)” standarte, kituose paplitusiuose standartuose – COBIT ir ITIL.

Diegdamos ISVS, organizacijos dažnai didžiąją dalį finansinių lėšų linkusios išleisti tokiems įrenginiams kaip ugniasienės, tarpiniai serveriai, antivirusinės programos, įsibrovimo aptikimo sistemos ir pan., tikint, jog vienokiu ar kitokiu būdu įmanoma užtikrinti informacijos saugumą. Tai galima būtų traktuoti kaip neteisingą požiūrį į informacijos saugos valdymą. Kuriant ISVS, derėtų atkreipti dėmesį ne vien į naujos technikos panaudojimo galimybes, bet ir į tokius faktorius: organizacijos darbuotojai, politika, procedūros, procesai bei atitinkami standartai [12]. Galiausiai ISVS diegimo investicijos atsirems į rizikos faktorius, pažeidžiamumų tipus, kurie susiję su atitinkama organizacijos veikla, dydžiu ir t. t. Be to, ISVS diegimo kaštai neturi viršyti informacinio turto vertės, kuris bus saugomas.

ISO/IEC 27000 serijos standartai

ISO/IEC 27000 serijos standartai dar kitaip vadinami Informacijos Saugumo valdymo sistemų (ISVS) šeimos standartais. Pastarieji apibrėžia rekomendacijas, kurios sudarytos remiantis geriausiomis ISVS praktikomis. Serijos standartai ganėtinai plačios apimties. Jie gali būti taikomi įvairių dydžių ir formų organizacijoms. Visos organizacijos yra skatinamos vertinti savo informacijos saugos riziką ir įgyvendinti atitinkamą informacijos saugos kontrolę pagal savo poreikius, naudojant gaires ir pasiūlymus, jei reikia. Atsižvelgiant į dinamišką informacinio saugumo pobūdį, ISVS sąvoka apima nuolatinį grįžtamąjį ryšį ir veiklos tobulinimą, kuris remiasi W. Edvardo Demingo ciklu [8].

1 pav. W. Edvardo Demingo ciklas

Remiantis šiuo modeliu, siekiama išspręsti pokyčių grėsmę, pažeidžiamumą ir poveikį informacijos saugumo incidentams.

- *Planavimas* – ką reikia padaryti, kada tai reikia padaryti, kas turi tai padaryti ir kokiomis priemonėmis.
- *Vykdymas* – suplanuotų darbų atlikimas.
- *Patikrinimas* – įvertinamas darbų atlikimas ir nustatoma, ar pasiekti laukiami rezultatai.
- *Veiksmas* – koreguojami planai, įvertinant patikrinimo etape gautą informaciją.

Šiuo metu ISO/IEC 27000 seriją sudaro šeši viešai publikuojami standartai, taip pat egzistuoja keletas kitų standartų, kurie dar tik kuriami ir viešai neprieinami. Publikuojami standartai:

- ISO/IEC 27000 – ISVS apžvalga ir žodynas.
- ISO/IEC 27001 – ISVS reikalavimai.
- ISO/IEC 27002 – Informacijos saugos valdymo praktikų rinkinys.
- ISO/IEC 27003 – ISVS įgyvendinimo gairės.
- ISO/IEC 27004 – Informacijos saugos valdymo priemonės.
- ISO/IEC 27005 – Informacijos saugos incidentų valdymas.
- ISO/IEC 27006 – Reikalavimai organizacijoms, atliekančioms auditą bei sertifikuojančioms informacijos saugos valdymo sistemas.

Iš ISVS šeimos standartų svarbu atkreipti dėmesį į ISO/IEC 27005 standartą, taip pat ISO/IEC 27001 ir ISO/IEC 27002 standartus. Tai būtina, nes pastarieji tarpusavyje susiję ir reikalauja suprasti tiek vieną, tiek kitą standartą.

ISO/IEC 27002 turi tiesioginius lygiaverčius standartus daugumoje šalių. Lietuva – ne išimtis (LST ISO/IEC 17799:2005). Standartas iš esmės yra dviejų dalių: ISO/IEC 17799:2005 ir ISO/IEC 27001:2005 (buvę BS7799 ir BS7799-2) [28, 29].

ISO/IEC 27001:2005 – apibrėžia Informacijos saugos valdymo sistemos (ISVS) nurodymus. ISVS – tai priemonė, kurios pagalba aukštesnioji administracija tikrina ir valdo savo saugumą, minimizuodama likutinę verslo riziką ir užtikrina, kad saugumas ir toliau vykdys korporacijos, kliento ir teisinius reikalavimus. Jis sudaro organizacijos vidinės kontrolės sistemos dalį [7, 27].

ISO/IEC 17799:2005 apibrėžia standartinius veiklos principus, kurie yra laikomi išsamiu gerų saugumo praktikų žinynu [7]. Kitaip tariant, ISO/IEC 27001:2005 aprašo reikiamus nurodymus, kaip galima taikyti ISO/IEC 17799. O taip pat sukurti, valdyti, išlaikyti bei gerinti ISVS.

Pagrindinius ISVS komponentus galima būtų pavaizduoti pasinaudojus prieš tai minėto W. Edvardo Demingo ciklu, iš kurio išplauktų schema, pavaizduota 2 paveiksle, bei perrašyti standartines ciklo būsenas taip:

2 pav. W. Edvardo Demingo ciklas, pritaikytas ISVS

Planavimas. Tai turėtų būti pirmasis žingsnis, kuris nustatytų ISVS apimtį. Sistema gali apimti tiek visą organizaciją, tiek tam tikrą dalį, taip pat gali apimti tik tam tikrą paslaugą, pavyzdžiui, internetinę bankininkystę. Į šią būseną turėtų pakliūti ir tokie žingsniai: ISVS politikos apibrėžimas, rizikos įvertinimas, rizikos valdymo planas, tinkamumo patvirtinimas.

Veiksmas. Ši ciklo dalis reikalauja, kad būtų diegiami reikiami priežiūros metodai, t. y. procedūros, kurios užtikrina greitą incidentų aptikimą ir reagavimą į juos. Taip pat reikės užtikrinti, kad visi darbuotojai įgytų supratimą apie informacijos saugą bei būtų tinkamai apmokomi ir kompetentingi savo atitinkamoms saugumo užduotims įgyvendinti. Kad visa tai būtų įgyvendinta, organizacijoje būtina rasti tam reikalingų resursų.

Patikrinimas. Šio ciklo paskirtis yra užtikrinti, kad kontrolės metodai pasiektų išsikeltus tikslus. Egzistuoja įvairių galimų tikrinimo veiksmų, tačiau tik vidiniai ISVS ir vadovybės patikrinimai yra pirminės svarbos. Šalia pastarųjų papildomai gali būti parenkami šie reikalavimai – įsibrovimo nustatymas, incidentų valdymas, einamieji patikrinimai, savikon-

trolės procedūros, mokymasis iš kitų organizacijų (pvz., CERT), valdymo patikrinimas.

Vykdymas. Šio ciklo įgyvendinimas priklauso nuo pastarojo ciklo (Patikrinimas) veiklos rezultatų. Atsižvelgiant į rezultatus, galimi trijų rūšių veiksmai: koregavimo veiksmai, prevenciniai veiksmai, tobulinimo veiksmai.

Verta pastebėti, jog visos *planuok – veik – tikrink – vykdyk* ciklo būsenos gali veikti nesinchroniškai bei skirtingais laiko momentais. ISO/IEC 27002 (17799:2005) standarte yra nustatyti 133 saugumo valdymo svertai, sudaryti iš 12 pagrindinių kategorijų [9, 13]:

1) rizikos vertinimas;
2) saugumo politika;
3) organizacinės saugos priemonės;
4) turto klasifikavimas ir priežiūra;
5) personalo sauga;
6) fizinė apsauga;
7) ryšiai ir operacijų valdymas;
8) priėjimo kontrolė;
9) sistemos sukūrimas ir priežiūra;
10) informacinės saugos incidentų valdymas;
11) komercinės veiklos nepertraukiamumo valdymas;
12) atitiktis.

Kiekviena iš šių kategorijų turi papildomus saugumo kontrolės mechanizmus bei tikslus. Nepaisant to, išvardinti visų kontrolės mechanizmų, kurie būtų pritaikomi bendrojoje praktikoje, neįmanoma. Standarte taip pat pateikiamos valdymo svertų įgyvendinimo gairės, tačiau kiekviena organizacija privalo įvykdyti struktūrinį informacinės saugos rizikos vertinimo procesą, kuris leistų nustatyti konkrečius reikalavimus, prieš pasirenkant kontrolės mechanizmus, bei atitiktų jų tam tikras iškylančias situacijas.

Informacinės saugos audito įrankiai

Atliekant informacinės saugos auditą, buvo atsisakyta komercinių produktų ir pasirinkta naudoti vien tik atviro kodo įrankius. Stebint, kaip kompiuterių industrijoje vis didėja bei auga susidomėjimas pastarosios saugumu, atsiranda didesnė atviro kodo įrankių bei jų patobulinimų, atnaujinimų įvairovė. Viena iš pagrindinių ir svarbiausių priežasčių, kodėl buvo pasirinkti atviro kodo įrankiai – pastebimai žemos naudojimo išlaidos. Dauguma įrankių yra visiškai nemokami arba, palyginus su panašiais komerciniais įrankiais, kainuoja labai nedaug. Tai leidžia juos taikyti informacijos saugos priemonėms įgyvendinti organizacijose, turinčiose ribotą biudžetą.

Kitas atviro kodo įrankių privalumas – visi išeities kodai gali būti laisvai prieinami. Tai leidžia kiekvienam norinčiam modifikuoti atitinkamas kodo vietas bei pritaikyti pasirinktą įrankio funkcionalumą pagal savo reikmes.

Vieni iš pagrindinių atviro kodo įrankių, kurie buvo naudoti atliekant IT saugos auditą:

Nessus [14, 16] – plačiai naudojamas bei žinomas pažeidžiamumų skeneris, turintis kasdien atnaujinamą pažeidžiamumų duomenų bazę bei dideles galimybes.

Metasploit [15] – įsiskverbtiems testavimo sistema bei kartu platforma, skirta apsaugos priemonėms ir pažeidžiamumų išnaudojimo kodams kurti. Šią sistemą visame pasaulyje naudoja daugelis *tinklo saugumo specialistų*, atlikdami įsibrovimo testus, *sistemų administratorių*, tikrindami, ar teisingai įdiegti sisteminiai atnaujinimai, *programinės įrangos pardavėjų*, atlikdami regresijos ir saugumo testus, bei *tyrėjai*. Sistema sukurta naudojant „Ruby“ programavimo kalbą, o įeinantys komponentai – įvairiomis kitomis kalbomis, pvz.: C, perl, assembler ir pan.

Nmap [17] – įrankis, skirtas tinklo analizei atlikti. Dažniausiai naudojamas tinkle esančių prieigos taškams nustatyti, tinklo įrenginių inventorizacijai, tinklo tipologijos analizei, tinklo įrenginių priežiūros vykdymui bei valdymui. Įrankis turi daugybę skenavimo metodų.

Wireshark [18] – paketų analizatorius, naudojamas tinklo trikčių analizėje, programinės įrangos ir ryšio protokolų plėtros srityse. Šis įrankis geba „suprasti“ daugybę skirtingų protokolų, taip pat yra galimybė realiu laiku analizuoti / redaguoti tinklų (Ethernet, IEEE 802.11, PPP ir kt.) srautus.

BackTrack4 [19, 20] – aukščiausius įvertinimus ir pripažinimą pelniusi Linux pagrindu veikiantis paketas. Kitaip tariant, tai operacinė sistema, kurioje įkomponuota daugybė įvairių įrankių, naudojamų informacinės saugos auditui atlikti, ir kitų įrankių. Pakete visi įrankiai suskirstyti į 11 kategorijų: informacijos rinkimo, tinklo išdėstymo, pažeidžiamumų paieškos, internetinių aplikacijų analizės, bevielio tinklo analizės (802.11, Bluetooth, RFID), skverbties (pažeidžiamumus išnaudojantys kodai, socialinės inžinerijos įrankių komplektas, privilegijų pasikėlimas, prieigos palaikymo kontrolė, skaitmeninių duomenų analizė, apgūžos inžinerija, IP telefonija).

Audito vykdymas

Vykdant informacinės saugos auditą, remtasi [22, 23, 24] ISO/IEC 27000 šeimos standartais.

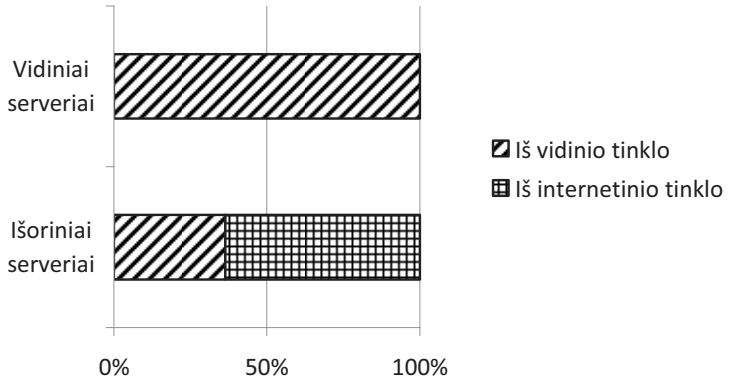
Buvo audituojama valstybinė biudžetinė organizacija, struktūriškai esanti ministerijos sudėtyje. Dėl suprantamų priežasčių (konfidencialios informacijos neatskleidimas, įsipareigojimų audituotai organizacijai, potencialiai pavojingos informacijos patekimas į kibernetinių nusikaltėlių rankas) organizacijos pavadinimas neatskleidžiamas. Siekiant suteikti tam tikros informacijos apie organizacijos tipą

bei siūlomo metodo pritaikomumą kitoms organizacijoms, galima paminėti tokius audituotos organizacijos bruožus:

- Vidutinio dydžio organizacija, kurios pagrindinė veiklos sritis nėra informacinės technologijos, t. y. informacinės sistemos yra naudojamos tik pagrindinei veiklai vykdyti.
- Organizacija pati tvarko (diegia, prižiūri) savo IT ūkį, tačiau ištekliai riboti (1–2 sistemų administratoriai).
- Organizacija neturi atskiro biudžeto informacijos saugos užtikrinimui.
- Sprendimus dėl techninių priemonių diegimo priima žmogus, atliekantis sistemos administratoriaus funkcijas, t. y. nėra atskiro dedikuoto žmogaus (pvz., informacijos saugos įgaliotinio).
- Pagrindinis ir IT personalas neturi pakankamai žinių informacijos saugos srityje.

Tačiau patys standartai tiksliai nenurodo, kaip ir kokiomis priemonėmis turi būti vykdomas audito procesas, kadangi kol kas dar nėra universalaus auditavimo metodo, kuris galėtų būti taikomas skirtingoms organizacijoms. Atliekamas informacinės saugos audito procesas buvo padalytas į dvi dalis – iš tinklo išorės ir iš vidaus [25]. Pateikta informacija skirta veiksmams ir procedūroms, atliktiems vykdant auditą demonstruoti. Kad būtų apsaugota organizacija, visi duomenys, kurie vienaip ar kitaip galėtų atskleisti jos tapatumą, yra iškraipyti. Verta pastebėti tai, jog organizacija iki šiol nebuvo atlikusi jokio IT saugos audito, todėl šio audito rezultatai pasitarnaus kaip pradinis taškas, nuo kurio galima bus vertinti būsimų auditų rezultatus. Norint pasiekti efektyvių rezultatų, būtina nepamiršti, jog IT saugos auditas – tai ne vienkartinis testas, o nuolatos atliekamas bei tobulinimas procesas.

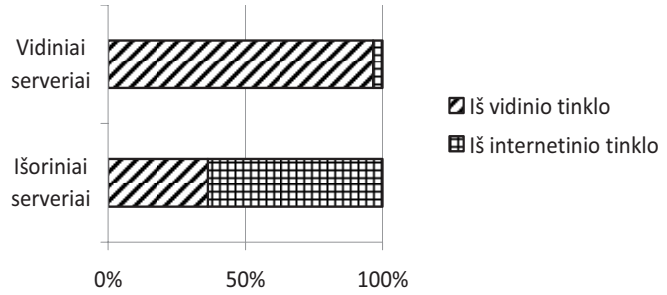
Vienas pirmųjų žingsnių, atliekant auditą, yra tinklo adresų ruožo bei prieigos taškų nustatymas Nmap įrankiu. Prieš atliekant tinklo skanavimą Nmap įrankiu, buvo imituojami kibernetinio nusikaltėlio, norinčio atspėti atakuojamojo tinklo topologiją veiksmai. Šiam uždaviniui įvykdyti buvo taikomi BackTrack4 Linux distribucijos įrankiai.



3 pav. Tarnybinių stočių atvirų prieigos taškų kiekis, išreikštas procentais

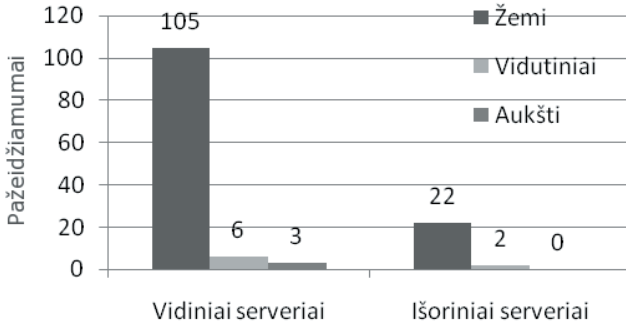
Rezultatai parodė, jog organizacijoje yra daugybė atvirų prieigos taškų, kurie įsilaužėliui suteikia nemenką galimybę rasti įvairių atakos vektorių krypčių. Tinklo srauto analizė, atlikta Wireshark įrankiu, nenustatė rimtų pažeidžiamumų (pvz., slaptažodžių perdavimas atviru tekstu tinkle, nesaugių protokolų – FTP, Telnet – naudojimas), todėl detaliau nėra aptariamas.

Sėkmingai atlikus pirmojo žingsnio veiksmus, tęsiama pažeidžiamumų paieška. Šio etapo tikslas- – surasti visus įmanomus aktyvius tinklo įrenginius ir patikrinti, kokioms atakoms jie yra pažeidžiami. Paieška vykdyta Nessus (automatizuota paieška) ir Metasploit (sudėtingesnė rankinė paieška) įrankiais.



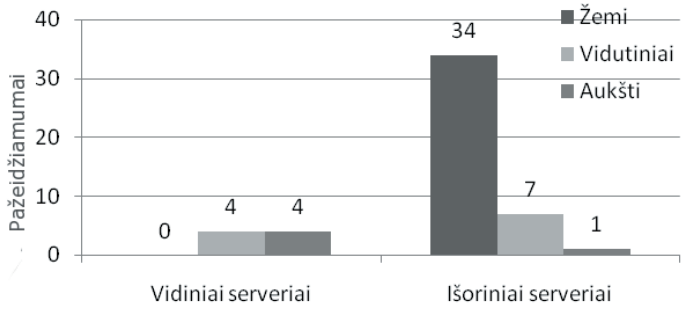
4 pav. Tarnybinių stočių pažeidžiamumai, išreikšti procentais

Paieškos rezultatai yra klasifikuojami į žemo, vidutinio ir aukšto pažeidžiamumo lygius [26]. Tyrimo duomenys dar kartą patvirtina tai, jog organizacija gali būti smarkiai pažeidžiama per išorinius serverius. Norint išsiaiškinti detaliau, kokiu lygiu organizacija yra pažeidžiama, reikia atlikti prieš tai minėtų pažeidžiamumų klasifikaciją, kuri pateikiama 5 bei 6 pav.



5 pav. Vidiniame tinkle rasti pažeidžiamumai pagal pavojingumo lygį

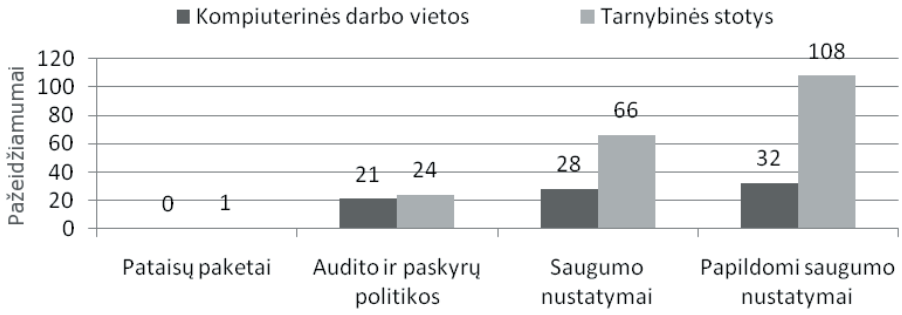
Iš atliktos pažeidžiamumų analizės galima matyti, jog organizacijoje egzistuoja rimtos saugumo spragos, kurias rodo rasti aukšto lygio pažeidžiamumai. Pastarieji pažeidžiamumai gali padidinti sėkmingo įsilaužimo tikimybę. Aukšto lygio pažeidžiamumai gali būti apibrėžiami kaip saugumo spragos, kurios išnaudojamos vykdant specialiai sukurtą pažeidžiamumą išnaudojantį kodą [26]. Tai leidžia nedidelėmis pastangomis pasiekti norimą rezultatą bei planuoti tolimesnes atakos kryptis.



6 pav. Pažeidžiamumai pagal pavojingumo lygį, rasti tikrinant iš internetinio tinklo

Nors pateikti rezultatai atspindi gan prastą organizacijos IT saugą, nereiktų pamiršti tai, jog užtikrinti 100 % saugą vargiai įmanoma. Saugumo lygis visada balansuoja tarp informacijos saugos, jos prieinamumo bei patogumo [25]. Be tinklo įrangos (maršrutizatoriai, spausdintuvai, ugniasienės), serverių ir pan., dažnai praleidžiamas kitas svarbus punktas – fizinė apsauga. Fizinė sauga apibrėžia tokius punktus, kaip: priėjimo kontrolė, nenaudojami tinklo lizdai, stebėjimo sistemos ir t. t. Audituojamoje organizacijoje fizinė sauga nebuvo pamiršta, tačiau audito rezultatai atskleidė, jog organizacijoje egzistuoja keletas fizinės struktūros saugos spragų: galimas laisvas fizinis priėjimas prie organizacijoje esančių serverių, nebuvimas apsaugos nuo vandens užliejimo svarbiausiuose organizacijos taškuose (pvz., serverinė), į organizaciją įeinantys lankytojai neregistruojami.

Kitas žingsnis audito procese – organizacijoje naudojamų politikų bei konfigūracijų įvertinimas. Patikrinimas buvo atliekamas rankiniu būdu lyginant nustatytas politikas su atitinkančių „The Center for Internet Security“ kietinimo gairėmis. Šio etapo metu buvo tikrinami aktyvaus katalogo grupinių politikų (AD group property) saugumo nustatymai. Tikrinami rezultatai parodė, jog organizacija neturi tinkamai paruoštų politikų, tokių kaip: paskyrų, paskyrų blokavimo, slaptažodžių, autentikavimo, lokalios, audito, vartotojo teisių, saugumo operacijų. Pastarosiose politikose arba buvo rasti tik keletas nustatymų, atitinkančių „The Center for Internet Security“ kietinimo gaires, arba jų visai nebuvo. Be politikų patikros, buvo atsižvelgta ir į tai, kaip sukonfigūruotos tarnybinės stotys bei kompiuterinės darbo vietos (7 pav.).



7 pav. Neteisingų nustatymų kiekis tarnybinėse stotyse ir kompiuterinėse darbo vietose

Iš 7 pav. galima daryti prielaidą, jog blogai sukonfigūruotos tarnybinės stotys turi tiesioginę priklausomybę dideliam rastų pažeidžiamumų skaičiui. Toks didelis blogų nustatymų kiekis, kaip buvo minėta prieš tai, palieka įsilaužėliams neribotą terpę savo veiksmams realizuoti.

Paskutinis audito etapas buvo skirtas organizacijai patikrinti ne iš techninės pusės, t. y. atlikti socialinės inžinerijos testą. Tai testas, kurio metu stengiamasi manipuliuoti žmonėmis, priverčiant juos atlikti įvairius veiksmus, ne visuomet jiems apie tai nutuokiant, pvz., pasakyti tam tikrą slaptažodį ar persiųsti slaptą dokumentą. Pasirinkta testo komunikacijos forma – telefoninis skambutis. Teste dalyvavo biuro administratorė, vyr. specialistė ir vyr. specialistas. Socialinės inžinerijos testu buvo mėginama išgauti vienos iš organizacijos sistemų slaptažodį. Pastarojo bandymo rezultatai atskleidė, jog organizacijos darbuotojai gerai išmano savo pareigybines instrukcijas bei geba greitai komunikuoti su kitais darbuotojais dėl tuo metu iškilusių klausimų, vengia atskleisti konfidencialią informaciją. Tačiau testo metu buvo nustatyta, kad darbuotojai ne visuomet yra tikri, kas yra konfidenciali informacija ir kam jie ją gali teikti. Apibendrinant atlikto bandymo rezultatus, galima teigti, jog socialinės inžinerijos testas nepavyko.

Taigi, audituota įmonė kartoja daugelio kitų analogiškų organizacijų taikomą priėjimą ir informacijos saugai užtikrinti naudoja tik technines priemones, neįvertindama organizacinių ir fizinių priemonių svarbos. Bendras įdiegtų technologinių sprendimų lygis yra palyginti žemas, pasižymintis paliktomis saugumo spragomis, dauguma kurių (pvz., neįdiegti operacinių sistemų atnaujinimai), gali būti išspręsti tik organizacinėmis priemonėmis. Atsižvelgiant į nustatytus pažeidimus bei pačios organizacijos suprantamą poreikį kelti saugos lygį, galėtų būti pasiūlytas toks veiklos planas:

- Rizikos analizės atlikimas, įvertinant organizacijai kylančias grėsmes bei reikiamą saugumo lygį.
- Informacijos saugos politikos bei procedūrų kūrimas, atsižvelgiant į rizikos analizės rezultatus.
- Informacijos saugos valdymo sistemos diegimas bei technologinių sprendimų adaptavimas pagal politikos reikalavimus bei ištaisant audito metu nustatytas spragas.
- Pakartotinis auditas organizacijos saugos lygio nepriklausomam progreso įvertinimui.
- Organizacijos sertifikacija pagal ISO/IEC 27001 standartą.

Išvados

1. Atliktas IT saugos auditas atskleidė organizacijos informacinės saugos spragas.
2. Tokio tipo informacinės saugos auditas organizacijoje buvo atliktas pirmą kartą. Audito rezultatai taps pradiniu tašku, nuo kurio galima bus vertinti būsimų auditų rezultatus, kurie taip pat gali būti traktuojami kaip vienas iš atliktų reikalavimų (preliminarus auditas), norint sertifikuotis informacijos saugumo valdymo sistemos standartui ISO/IEC 27001.
3. Pasirinkta informacinės saugos audito metodika – vartoti vien tik atviro kodo programinę įrangą – pasiteisino. Buvo aptikta įvairaus tipo ir lygio pažeidžiamumų.

Literatūra

1. Saugus darbas internete. <http://www.esaugumas.lt/index.php?-229839978>.
2. Šiuolaikiniai įsilaužėliai. <http://www.esecurity.lt/article/1353.html>.
3. Informacijos saugumo, vientisumo ir patikimumo užtikrinimas. <http://emilis.info/straipsniai/ktt_ref/>.
4. Informacijos apsaugos sprendimai. <http://www.smn.lt/index.php?fuseaction=free.browse&mid=34&cid=31>.
5. Leading Voices Think Technology Trumps Content? Well, You're Wrong. <http://paidcontent.org/article/419-think-technology-trumps-content-well-youre-wrong/>.
6. 2009 m. CERT-LT incidentų statistika. <https://www.cert.lt/doc/2009.pdf>.

7. Standartai 7799. <http://www.esecurity.lt/article/1567.html>.
8. The Deming Approach. <http://www.qualitran.com/Seminars/The_Deming_Approach_to_Total_Q/the_deming_approach_to_total_q.html>.
9. ISO/IEC 27002. <http://en.wikipedia.org/wiki/ISO/IEC_27002>.
10. Informacijos apsaugos standartai – 27000 serija. <http://isec.lt/pdf/ISO_standartai.pdf>.
11. ISO vadybos sistemos diegimo ir sertifikavimo procesas – paprastai. <http://www.bureauveritas.lt/wps/wcm/connect/bv_lt/local/home/about-us/our-business/certification/diegimo_ir_sert_procesas>.
12. Dey M., 2007, Information security management – a practical approach. P. 1–6., *AFRICON2007*. Digital Object Identifier: 10.1109/AFRICON.2007.4401528.
13. Liu H., Zhu Y., 2009, Measuring Effectiveness of Information Security Management., Computer Network and Multimedia Technology. P. 1–4. *CNMT 2009. International Symposium* Digital Object Identifier: 10.1109/CNMT.2009.5374634.
14. Lawton G., 2002, Open source security: opportunity or oxymoron? *Computer.* Vol. 35, 3. P. 18–21.
15. Metasploit - Penetration Testing Resources. <http://www.metasploit.com/framework/>.
16. Nessus. <http://nessus.org/nessus/>.
17. Nmap. <http://nmap.org/>.
18. Wireshark. <http://www.wireshark.org/>.
19. BackTrack. <http://en.wikipedia.org/wiki/BackTrack>.
20. BackTrack. <http://www.backtrack-linux.org/>.
21. Introduction To ISO 27002 (ISO27002). <http://www.27000.org/iso-27002.htm>.
22. Sahibudin S., Sharifi M., Ayat M., 2008, Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations Modeling & Simulation. P. 749–753. *AICMS 08. Second Asia International Conference*. Digital Object Identifier: 10.1109/AMS.2008.145.
23. ISO 27001, Information technology-Security techniques-Information Security management systems-Requirements. *International Organization for Standardization*, 2007.
24. ISO 27002, Information technology-Security techniques-Code of practice for information security management. *International Organization for Standardization*, 2007.
25. Lo E. C., Marchand M., 2004, Security audit: a case study [information systems]. *Electrical and Computer Engineering.* Vol. 1. P. 193–196.
26. Krsul I. V., 1998, Software vulnerability anglysis. *Doctor thesis*. Purdue University.
27. Wang C., Tsai D., 2009, Integrated installing ISO 9000 and ISO 27000 management systems on an organization. P. 265–267. 43rd Annual 2009 International Carnahan, Conference. Digital Object Identifier: 10.1109/CCST.2009.5335527.
28. BS7799-2: 1999, Information Security Management – Part 2: Specification for Information Security Management Systems. BSi (British Standards Institution).
29. BS7799-2: 2002, Information Security Management Systems – Specification with guidance for use. Bsi.

INFORMATION SECURITY AUDIT OF FULFILMENT OF ISO/ IEC 27000 FAMILY STANDARD REQUIREMENTS

Andrius Januta, Leonardas Marozas, Nikolaj Goranin

Summary

Information security is one of the critical elements in modern information society. Main problems that organizations can encounter, especially when working with sensitive information, are confidentiality and integrity of information. One of the methods to reduce the risk of the aforementioned problems is information security management system. It is not the solution to the problem by itself: the system is common recommendations and standards following which one can form policy of organizational security.

One of the main aims of this article is to present the ISO / IEC 27000 family of standards and their application in the organization of information security certification process. The article presents the ISO / IEC 27000 family of standards, information security management system, risk analysis process and tools used in penetration testing (for the system auditing in this article Metasploit, Nmap, WireShark, Backtrack4 were used). Furthermore, justification of benefits for using open-source software to perform penetration test, is provided. Lastly, analysis of results of the conducted penetration testing is presented.

Keywords: security, auditing, risk analysis, ISO27007, ISO17799, ISO / IEC 27000 standard, BS7799.

INFORMACINĖS SAUGOS AUDITO VYKDYMAS REMIANTIS ISO/IEC 27000 ŠEIMOS STANDARTŲ REIKALAVIMAIS

Andrius Januta, Leonardas Marozas, Nikolaj Goranin

Santrauka

Informacijos sauga yra vienas kritinių elementų dabartinėje informacinėje visuomenėje. Pagrindinės problemos, su kuriomis gali susidurti įstaigos ir organizacijos, ypač dirbančios su jautria informacija, yra informacijos konfidencialumo ir vientisumo išsaugojimas. Informacinės saugos valdymo sistema yra vienas būdų anksčiau minėtų problemų keliamiems pavojams sumažinti. Savaime tai nėra problemos sprendimas – tai bendrinės rekomendacijos, standartai, kuriais remiantis turi būti formuojama organizacijos saugos politika ir jos laikomasi.

Straipsnio tikslas – pristatyti ISO/IEC 27000 standartus, esančius informacinės saugos valdymo sistemos standartų šeimoje. Taip pat išnagrinėti jų taikymo galimybes organizacijos informacinės saugos sertifikavimo proceso metu. Straipsnyje supažindinama su informacinio saugumo valdymo sistema, jos komponentais, rizikos analizės procesu ir audito metu galimais naudoti įrankiais (šiame straipsnyje atliktam auditavimui pasirinkti Nessus, Metasploit, Nmap, WireShark, Backtrack4 ir kt.). Straipsnyje akcentuojamas atviro kodo programinės įrangos auditui vykdyti tikslingumas. Pateikiami pasirinktos organizacijos, kurioje auditas buvo atliekamas pirmą kartą, informacinės saugos audito procesas, jo rezultatai ir jų analizė.

Prasminiai žodžiai: saugumas, auditas, rizikos analizė, ISO27007, ISO17799, ISO 27000 standartai, BS7799.

Įteikta 2011-05-25