

Informacinių sistemų ir kompiuterinių tinklų technologinio pažeidžiamumo įvertinimas

UAB „Informacijos saugos sprendimai“

www.isec.lt



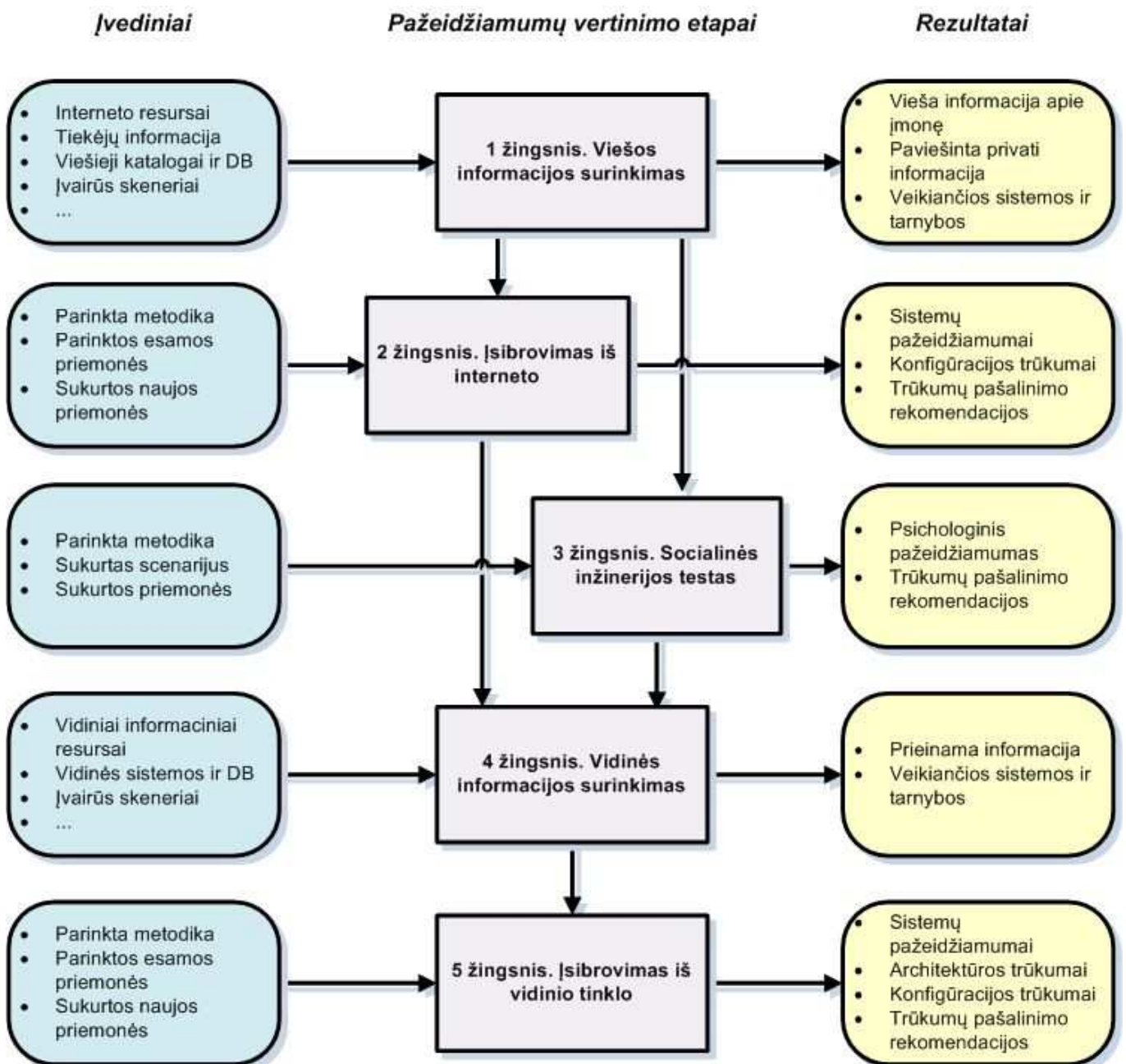
Turinys

1. Pažeidžiamumų įvertinimas	3
2. Viešos informacijos surinkimas	4
3. Įsibrovimas iš interneto	4
4. Socialinės inžinerijos testas	4
5. Vidinės informacijos surinkimas	4
6. Įsibrovimas iš vidinio tinklo	5
7. Rezultatai	5
8. Informacija apie įmonę	5
9. Kontaktai	6

1. Pažeidžiamumų įvertinimas

Pažeidžiamumų įvertinimas vykdomas siekiant nustatyti technologinius organizacijos informacijos apsaugos pažeidžiamumus, iš jų kylančią riziką normaliai organizacijos veiklai ir galimas apsaugojimo priemonės. Paslaugos vykdymo metu analizuojama kompiuterių tinklo architektūra, patikrinamos organizacijos tinklo tarnybos, tinklinės įrangos, ugniasienių, darbo stočių ir asmeninių kompiuterių konfigūracija, administravimo aplinka, atliekamas socialinės inžinerijos testas (manipuliavimas žmonių pasitikėjimu), slaptažodžių, duomenų bazių ir kiti audita. Visi šie darbai atliekami turint vieną tikslą – nustatyti, ar įmanoma įsilaužti į Jūsų įmonės informacines sistemas ir kokią žalą galima padaryti įsilaužus. Kaip rezultatas pateikiama ataskaita, kurioje nurodyti surasti apsaugos trūkumai ir pateikiamos rekomendacijos, kaip juos pašalinti. Taip pat ataskaitoje dažniausiai pateikiamas scenarijus, kuriuo vadovaujantis galima pačiam išbandyti esamus pažeidžiamumus ir įsitikinti jų rezultatais.

Pagrindiniai pažeidžiamumų įvertinimo etapai:



Toliau pateikiama informacija apie kiekvieną iš etapų.

2. Viešos informacijos surinkimas

Viešos informacijos surinkimo metu įvertinama ir dokumentuojama kokią viešą informaciją galima surinkti apie organizaciją, kokią privačią organizacijos informaciją galima gauti *neįsibrovus* į organizacijos tinklą, kokios sistemos ir tarnybos yra prieinamos visiems interneto vartotojams. T.y. surenkama kuo daugiau informacijos, kurią gali gauti bet kuris interneto vartotojas. Nuo šio etapo dažniausiai pradedamas bet koks įsilaužimas.

Informacija renkama naudojantis įvairiomis paieškos sistemomis, programine įranga, interneto resursais, katalogais, viešomis duomenų bazėmis. Surinkta informacija koreliuojama, taip gaunant naujus ir iš pirmo žvilgsnio nepastebimus rezultatus. Visas informacijos surinkimas atliekamas naudojant patikrintą ir efektyvią metodiką, kuri leidžia lengvai atnaujinti analizės rezultatus kitais metais. Kaip rezultatas, parengiama ataskaita, kurioje pateikiami įvairūs surinktos informacijos šaltiniai ir duomenys, perteklinės informacijos pašalinimo rekomendacijos.

3. Įsibrovimas iš interneto

Šio etapo metu nustatomi iš išorės pasiekiamų informacinių sistemų ir technologijų pažeidžiamumai bei konfigūracijos trūkumai, taip pat parengiamos trūkumų pašalinimo rekomendacijos. Šiame etape auditas atliekamas „juodosios dėžės“ principu, kai naudojama tik pirmojo etapo metu surinkta informacija ir nieko nežinoma apie vidines sistemas. Surinktą informaciją bandoma panaudoti įsibrovimui į vidinį organizacijos tinklą, svarbių duomenų išvogimui ir pan. Atliekama išsami sistemų technologinių pažeidžiamumų analizė, slaptazodžių auditas, panaudojant programinę įrangą, sistemas ir metodus, analogiškus įsilaužėlių (hakerių) naudojamiems metodams. Taip pat, priklausomai nuo esamos situacijos, gali būti sukurta specialiai Jūsų įmonės auditui pritaikyta programinė įranga. Kaip rezultatas pateikiami nustatyti sistemų pažeidžiamumai ir konfigūracijos trūkumai bei jų pašalinimo rekomendacijos. Analizės metu surinkta informacija yra dokumentuojama. Dokumentavimo forma leidžia patogiai atlikti pakartotinius išorinius pažeidžiamumų įvertinimus ateityje ir palyginti gautus rezultatus.

4. Socialinės inžinerijos testas

Šio etapo metu, panaudojant pirmame etape surinktą informaciją ir išnagrinėjus organizacijos struktūrą, joje dirbančių darbuotojų pareigas, rengiami psichologiniai spąstai jos darbuotojams. Pagal esamą situaciją sudaromas informacijos išviliojimo scenarijus, paruošiamos reikalingos priemonės ir bandoma tą informaciją išvilioti iš organizacijos darbuotojų pasirinktais metodais. Analogiškais metodais įsilaužėliai bando išvilioti svarbią informaciją pasinaudodami psichologija, o ne techninėmis priemonėmis.

5. Vidinės informacijos surinkimas

Šis etapas yra paskesnis įsilaužėlio žingsnis po to, kai jis įsibrauna į vidinį organizacijos tinklą. Taip pat analogiškais metodais naudojasi ir nesąžiningi organizacijos darbuotojai, norintys pakenkti organizacijai ar tiesiog išgauti informaciją, kurios jie neturėtų matyti.

Vidinės informacijos surinkimo metu įvertinama ir dokumentuojama prie kokios informacijos galima prieiti, ar darbuotojas, neturėdamas specifinių žinių, gali ją pasiekti kolegų kompiuteryje, serveryje ar duomenų bazėje. Šio etapo metu nustatomos veikiančios tarnybos ir sistemos, tikrinamos darbuotojų teisės į įvairius IT resursus ir pan. T.y. surenkama kuo daugiau informacijos, kurią gali gauti

bet kuris darbuotojas ar į vidinį tinklą jau patekęs įsilaužėlis. Nuo šio etapo dažniausiai tęsimas įsilaužimas iš išorės.

6. Įsibrovimas iš vidinio tinklo

Šio etapo metu nustatomi vidiniame tinkle pasiekiamų informacinių sistemų ir technologijų pažeidžiamumai, tinklo įrenginių, serverių bei kitų sistemų konfigūracijos trūkumai, analizuojama tinklo architektūra, taip pat parengiamos trūkumų pašalinimo rekomendacijos. Šiame etape auditas atliekamas „skaidriosios dėžės“ principu, kai įsilaužėlis pakankamai gerai žino kas yra toje „dėžėje“, t.y. vidinio tinklo struktūrą, vidiniame tinkle naudojamas tarnybas, žino kokiame serveryje kas saugoma ir pan. Tokią informaciją paprastai turi nesąžiningi esami arba buvę organizacijos darbuotojai. Šio etapo metu taip pat naudojama ketvirtojo etapo metu surinkta informacija, atliekama išsami tinklo, serverių, darbo vietų kompiuterių, naudojamų apsaugos sistemų technologinių pažeidžiamumų analizė, tikrinama techninės ir programinės įrangos konfigūracija, atliekamas slaptažodžių auditas ir kiti darbai. Auditui naudojama programinė įranga, sistemos ir metodai, analogiškai įsilaužėlių (hakerių) naudojamiems metodams. Taip pat, priklausomai nuo esamos situacijos, gali būti sukurta specialiai Jūsų įmonės IT auditui pritaikyta programinė įranga. Šio tikrinimo metu taip pat atliekama vidinio tinklo srauto analizė. Esant poreikiui, šiame etape taip pat gali būti atliktas socialinės inžinerijos testas.

7. Rezultatai

Kaip rezultatas, pateikiami nustatyti pažeidžiamumai ir įvairūs trūkumai bei jų pašalinimo rekomendacijos, bendrosios išvados. Rezultatų pateikimo forma leidžia patogiai iš karto identifikuoti labiausiai pažeidžiamas sistemas ir didžiausius trūkumus, o atlikus pakartotinius pažeidžiamumų įvertinimus ateityje, palyginti gautus rezultatus ir įvertinti pokyčius.

Pažeidžiamumų įvertinimo rezultatai paprastai pristatomi IT skyriaus darbuotojams nevengiant techninių terminų, o esant poreikiui ir įmonės vadovams ar suinteresuotiems asmenims. Pastaruoju atveju pristatymo metu yra vengiama IT techninės kalbos. IT skyriaus darbuotojai, matydami IT audito rezultatus ir vadovaudamiesi pateiktomis rekomendacijomis, galės pašalinti trūkumus ar sustiprinti silpnesnes informacines sistemas.

8. Informacija apie įmonę

UAB "Informacijos saugos sprendimai" - 2006 metais įkurta kompanija, kurios pagrindinė veikla informacijos apsaugos sprendimai visuose saugumo proceso etapuose. Kompanija yra nepriklausoma ir neatstovauja nei vienam programinės ar techninės įrangos gamintojui, todėl visuomet išlieka nešališka. Įmonėje dirba ne vienerių metų patirtį informacinio saugumo srityje sukaupę specialistai. Įvairias informacijos apsaugos paslaugas (saugumo auditavimo, rizikų vertinimo ir valdymo, veiklos tęstinumo planavimo, techninių ir organizacinių saugumo priemonių rengimo ir įgyvendinimo, švietimo ir mokymo programos) esame suteikę įvairioms Lietuvos įmonėms, tokioms kaip: UAB Bitė Lietuva, AB Rytų skirstomieji tinklai, Vidaus reikalų ministerija, AB Lietuvos geležinkeliai ir kitose. Kompanijos darbuotojai ne tik gerai išmano šiandien aktualius informacijos apsaugos standartus, hakerių metodus, bet turi patirties ruošiant su informacijos apsauga ir informacinių technologijų nusikaltimais susijusius įstatymus, kuriant incidentų valdymo tarnybą.

- Kompanija laikosi savo etikos politikos - suteikti klientui tik aukščiausio lygio paslaugas.
- Įmonė laikosi konfidencialumo principų net jei raštiškai nėra įsipareigojusi to daryti.
- Kompanijai svarbu sukurti vertę, todėl ji savo darbą vertina pagal klientui suteiktą naudą.

9. Kontaktai

Marius Celskis

Mob. tel.: +370 685 52330

Tel.: (8 5) 2030 828

El. paštas: marius@isec.lt

<http://www.isec.lt>

Audrius Lučiūnas

Mob. tel.: +370 615 20288

Tel.: (8 5) 2030 828

El. paštas: audrius@isec.lt

<http://www.isec.lt>