Informacinės sistemos rizikos vertinimas

Turinys

Informacinės sistemos rizikos vertinimas

Darbo struktūra

- Turinys
- Įvadas:
  - Tikslas
  - Rizikos vertinimo ribos.
  - Rizikos vertinimo būdas.
    - riziką vertinančios grupės sudėtis;
    - informacijos surinkimo metodai;
    - pasirinktos rizikos vertinimo skalės aprašymas.
- Sistemos charakteristikos.
- Pažeidžiamumų sąrašas.
- Grėsmių šaltinių sąrašas.
- Rizikos vertinimo rezultatai:
  - numeris ir trumpas aprašymas
  - poros „Pažeidžiamumas/Grėsmė“ aptarimas;
  - riziką mažinančių esamų apsaugos priemonių rinkinys;
  - grėsmės realizavimo tikimybės analizė ir jos įvertinimas
  - poveikio analizė ir jo įvertinimas
  - rizikos įvertinimas (reitingas)
  - rekomenduojamos apsaugos priemonės arba kiti rizikos sumažinimo būdai.
- Išvados.

Įvadas

Tikslas

Įvertinti pasirinktos informacinės sistemos (IS) rizikas, rasti būdus joms sumažinti bei galiausiai sudaryti šios IS saugumo politiką.

Rizikos vertinimo ribos

Renkuosi nagrinėti vienos IRT / Telco kompanijos ***Bastionų* IS**, priklausančią kompanijos *Mobility* infrastruktūrai ir aptarnaujančią visas kitas, daugiausiai duomenų centrų (DC) IS, bet taip pat ir kelias Telco (ne DC) IS.

Bastionai kai kur pasaulyje dar vadinama *Jumphosts* (angl., išvertus būtų maždaug „Peršokimo mazgais“).

Ši IS skirta **atlikti OAM funkcijas** (angl. *Operation, administration, maintenance*) — **komandinės eilutės** (CLI, angl. *Command-line interface*) **prisijungimus prie kitų IS**, veikiančių daugiausiai ***nix OS** pagrindu.

Bastionų IS sudaro keli atskiri mazgai (angl. *Host*) — serverinės mašinos su Linux OS.

Šioje IS vartotojų paskyros priklauso OS ir yra lokalios, kuriamos rankiniu būdu. Jos skirtos serverių ir tinklo sistemų administratoriams. Sutrumpintai juos vadinu *sysadminais* (reikėtų nesumaišyti su *aplikacijų sistemų* ar tiesiog *aplikacijų* administratoriais).

Bastionų mazgai priima prisijungimus saugiu `SSH` protokolu. Prisijungę sysadminai gauna galimybę jungtis jau į tolimesnius infrastruktūros mazgus, į kitas IS.

Taip pat bastionų mazguose veikia `cron`, automatinis užduočių vykdymas pagal laiką (angl. *Scheduled jobs*). Užduotys atlieka panašius veiksmus, kaip ir darbuotojai, tik veikia ne personalinėse, o techninėse OS paskyrose.

Į Bastionų IS jungiamasi iš KDV (kompiuterinių darbo vietų), įprastai esančių nebe DC, o biuro patalpose. Kadangi KDV pagrindas yra nešiojamieji kompiuteriai, įmanoma iš KDV prisijungti ir atvykus į duomenų centrą.

Tačiau tai jau kitų IS sritis, čia brėžiu ribą ir rizikų jose nevertinsiu.

Rizikos vertinimo būdas

Trumpai aprašomas pasirinktas grėsmių įvertinimo būdas, tame tarpe:

- riziką vertinančios grupės sudėtis;
- informacijos surinkimo metodai;
  (klausimynai, programinės priemonės ir pan.);
- pasirinktos rizikos vertinimo skalės aprašymas.

Sistemos charakteristikos

Vienas bastionų mazgas yra fizinis, ir įrengtas duomenų centre tiesiogiai, kaip atskiras įrenginys.

Kiti mazgai buvo virtualizuoti ir veikia kaip virtualios mašinos (VM) VMware klasteryje — taip pat duomenų centre, tik kitame, su kuriuo yra pilnavertis tinklo ryšys.

Du mazgai (vienas fizinis ir vienas VM) yra labiausiai skirti OS administratoriams, o dar trys mazgai (tik VM) skirti tik DC tinklų ir TelCo tinklų administratoriams.

Tris jų vienetus pavaizdavau 1 pav., L2 lygmens viduryje:

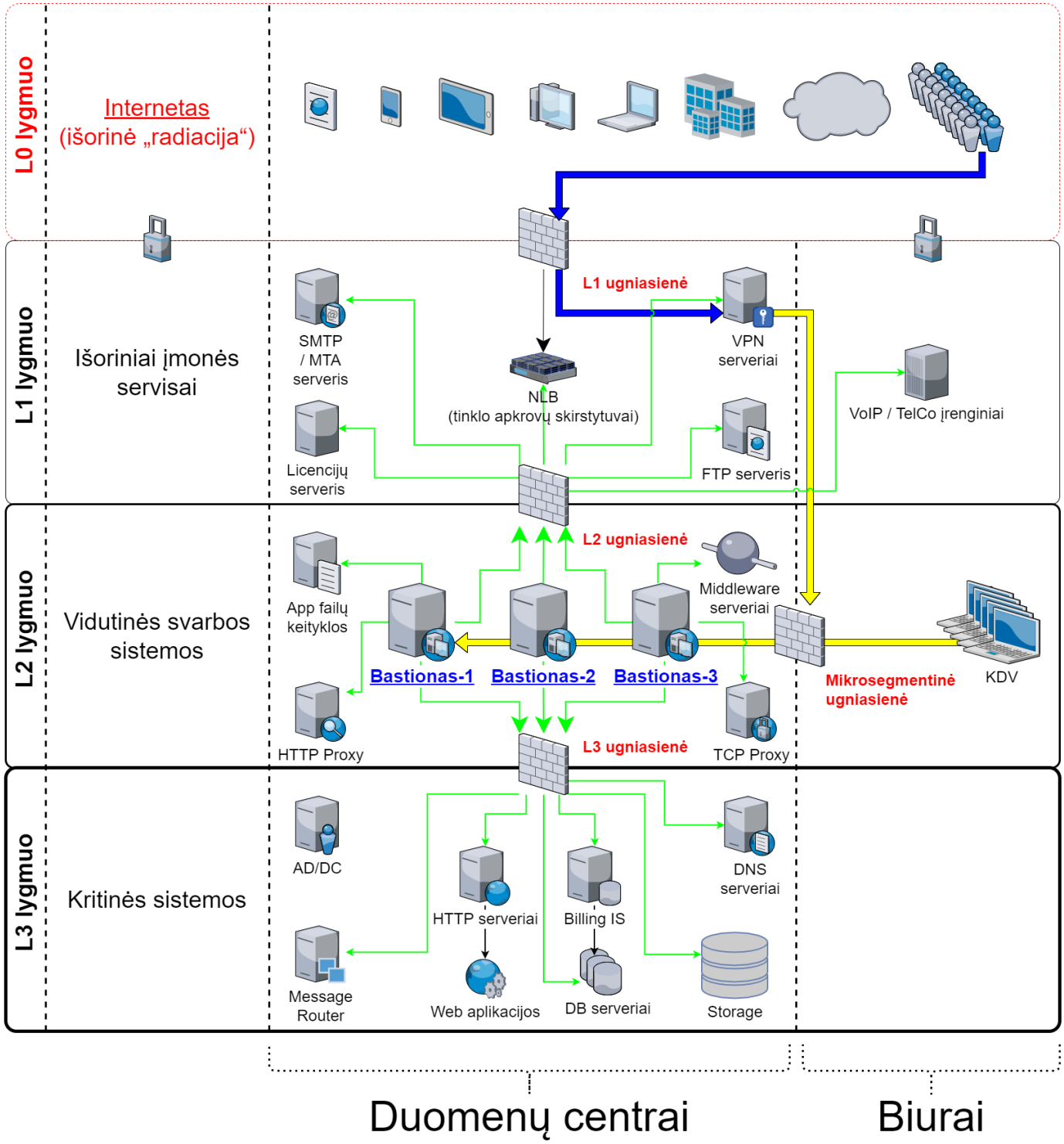

Figure 1. **1 pav.** *Supaprastinta IT infrastruktūra ir Bastionų IS tinklo srautai joje*

Aprašoma sistema, įskaitant aparatūrą (serverius, tinklo įrangą ir t.t.), programinį aprūpinimą

(taikomąsias programas, bazinę PĮ, protokolus), duomenis, vartotojus. Pateikiama sąryšių diagrama, duomenų įėjimo ir išėjimo srautai.

Čia matyti, jog visi *Mobility* infrastruktūros tinklo mazgai (angl. *Hosts*) ir mašinos yra suskirstyti į tris saugumo lygmenis (pagal kitų IS svarbumus ir įtakas įmonės veiklai):

- L3 — kritiškiausios IS;
- L2 — vidutinės įtakos IS;
- L1 — nekritinius išorinius servisus aptarnaujančios ir mažiausiai kritinės IS.

Dėl bendros tvarkos ir aiškumo infrastruktūros išorę irgi pažymiu (sąlyginai):

- L0 — internetas ir tolimai susijusios, visiškai kitos įmonės IT infrastruktūros.

Į šiuos bastionų mazgus administratoriai įprastai jungiasi iš savo KDV (kompiuterinių darbo vietų). Jungimosi protokolas vienintelis — `SSH`, o šiuos srautus diagramoje pažymėjau geltona spalva.

KDV — nešiojamieji kompiuteriai su Windows OS, įmonės biure kasdien jungiami prie įmonės LAN tinklo ir prie *Docking* periferijos.

Jie yra pririšti prie AD (angl. Active Directory) ir vadinamojo Domain kontrolerio (DK). KDV mašinos (o gal ir vartotojo) autentifikavimui naudojamas `.1x` protokolas ir į Windows integruotas sertifikatas. Pastaruoju remiantis autentifikuojamas ir KDV prisijungimas VPN kanalu (naudojamas Juniper PulseVPN). Srautus iki VPN serverių pažymėjau mėlyna spalva, o srautą už VPN IS pažymėjau vėlgi geltonai, kaip ir srautą iš KDV. Tačiau tai jau atskiros, kitos IS, ir jų nenagrinėju.

Fizinis prisijungimas prie vienintelės fizinės Bastionų IS mašinos per VGA konsolę ir klaviatūrą būtų naudojamas tik rimto gedimo atveju, kai jau nuvykstama į DC.

Taigi, įprastai prie Bastionų IS jungiamasi `SSH` protokolu, o vartotojas autentifikuojamas SSH raktu. Veikia autentifikacija ir pagal vartotojo slaptažodį, tačiau tai mažiau saugus ir laikui imlesnis būdas.

`SSH` prisijungimai galimi tik iš biure prijungto kompiuterio arba iš namuose prijungto komputerio, bet su sąlyga, kad naudojamas biuro VPN tunelis.

Prisijungus prie bet kurios Bastiono mašinos į savo personalinę paskyrą, toliau vartotojas per CLI jungiasi į kitas savo ūkio infrastruktūros mašinas (įprastai tuo pačiu `SSH` protokolu).

Įprastai tai skirtingos **Unix šeimos OS** (HP-UX, Solaris, OpenBSD) ir **Linux distribucijų** (Debian, RHEL, Oracle Linux, CentOS) versijos. O viena aptarnaujama, kritinė IS naudoja ir iš principo kitokią, artimesnę Windows OS — **OpenVMS**. Tačiau dėl savo CLI valdymo sąsajos ją valdyti priskirta irgi *nix sysadminams ir irgi yra valdoma iš bastionų.

Į didžiąją dalį tolimesnių IS yra jungiamasi irgi `SSH` protokolu (įskaitant ir OpenVMS mašinas). Vartotojas autentifikuojamas tik `SSH` rakto pagalba.

Prisijungimui tik į pora mašinų su HP-UX (vienoje *Legacy* sistemoje) dar naudojamas ir `RSH` protokolas. O itin mažai daliai mašinų (keletui vienetų iš kelių šimtų) sykis nuo sykio prireikia `Telnet` prisijungimų (kai nustoja veikti `SSH`).

Iš bastionų jungiamasi į kitų IS ne tik OS tinklo interfeisus / OAM IP adresus, bet ir į tų IS mašinų fizinio valdymo (angl. *Management*) modulių interfeisus: HP iLO, Dell DRAC, IBM IMM, HP MP, Sun/Oracle ALOM/ILOM/XSCF.

Čia `Telnet` jau naudojamas žymesniam mašinų skaičiui aptarnauti (~30%).

Šiuos, tolimesnius jungimosi srautus diagramoje pažymėjau žalia spalva.

Beje, diagramoje tokie srautai į mažą dalį serverių šioje nepažymėti, pvz. į AD (Active Directory) / DC (Domain Controller), nes ten veikia Windows OS, ir *nix sysadminai su jais neturi nieko bendro. Diagramoje šios IS pavaizduotos tik siekiant pavaizduoti pilnesnį saugumo lygmenų paveikslą.

Tai reiškia, kad tiek tarp skirtingų saugumo lygmenų, tiek mikrosegmentuojant sistemas tame pačiame saugumo lygmenyje, ugniasienėse yra sukurtos prieigos iš Bastionų IS į beveik visas *nix ir OpenVMS mašinas per transportinius `22/TCP` (o kai kur per `512-514/TCP` ar net `23/TCP`) portus.

Dalis šių mašinų yra virtualios ir valdomos VMware vSphere sprendimo pagalba, taigi, srautai keliauja ir per VMware infrastruktūrą.

Taip pat bastionų mazguose veikia automatinis užduočių vykdymas pagal laiką: `cron`. Šios užduotys — tai skriptai ar atskiros binarinės programos, kurie jungiasi į jau paminėtas kitas IS ir yra skirti nuimti pasikartojančius veiksmus nuo sysadminų pečių bei juos vykdyti kitose IS pagal tvarkaraštį.

Pvz.:

- archyvuoti naujus logus,
- senus patalpinti į logų IS,
- bei ištrinti originalus,
- atlaisvinti failų sistemas (FS) ištrinant kitus susikaupusius ir nebeaktualius failus,
- vykdyti *Storage* sistemos SAN „diskų“ (LUNų) snapšotus.
- stebėti diskinių kaupiklių (HDD, angl. *Hard disk drive*) būsenas.

Tolimesnis planas

Pagalvojimui:

- SSH raktai, jų auditas
- papildomos (automatinės) funkcijos/perimetras: `cron`
  - suarchyvuoti logus, ypač aplikacijų, kurie kuriami ne `Syslog` mechanizmu.
- Somewhat HA (VM ir ne VM)
- VMware infra flapping IFaces
- senas Debian, sąlyginai naujas CentOS
  - iššūkis migruojant, pvz. Perl skriptus
- `sudo` ir `uid` elevacija
- Prasta SSH implementacija pas OpenVMS (dėl to daug patogesnis / spartesnis darbas su Telnet)
- VMware infros saugumas, ar ne per daug?

Pažeidžiamumų sąrašas

Sudaromas galimai egzistuojančių potencialių IS pažeidžiamumų sąrašas.

Grėsmių šaltinių sąrašas

Sudaromas potencialių, aktualių vertinamai sistemai grėsmių sąrašas.

Rizikos vertinimo rezultatai

Pateikiamas nustatytų rizikų sąrašas (pora „Pažeidžiamumas/Grėsmė“).
Į kiekvieną šio sąrašo elementą turi įeiti:

- numeris ir trumpas aprašymas
  (pvz. „1. Vartotojų slaptažodžiai gali būti atspėti arba parinkti“);
- poros „Pažeidžiamumas/Grėsmė“ aptarimas;
- riziką mažinančių esamų apsaugos priemonių rinkinys;
- grėsmės realizavimo tikimybės analizė ir jos įvertinimas
  (pvz. „didelė [1,0]“, „vidutinė [0,5]“, „maža [0,1]“);
- poveikio analizė ir jo įvertinimas
  (pvz. „didelis [10]“, „vidutinis [50]“, „mažas [100]“);
- rizikos įvertinimas (reitingas)
  (pvz. didelė, vidutinė, maža);
- rekomenduojamos apsaugos priemonės arba kiti rizikos sumažinimo būdai.

Table 1. **Lentelė nr. 1***: Rizikos vertinimo rezultatai*

Nr.	Grėsmė	Galima grėsmės tikimybė	Žala	Rizikos lygis	Rekomenduojamos apsaugos priemonės	Likutinis rizikos lygis
		Taip / Ne	Maža =0,1 Vidutinė =0,5 Didelė =1,0	Maža =10 Vidutinė =50 Didelė =100		
1	Kenkėjiškos PĮ paleidimas					
2	Neleistinas taikomųjų programų naudojimas					
3	Neleistinas išteklių naudojimas					
4	Įsiskverbimas į tinklą					
5	Tinklu perduodamų duomenų perėmimas					
6	Neleistinas tinklo srauto maršruto pakeitimas					
7	Ryšių klaida					
8	Ryšių sutrikimas					
9	Serverių gedimas					

Nr.	Grėsmė	Galima grėsmės tikimybė	Žala	Rizikos lygis	Rekomenduojamos apsaugos priemonės	Likutinis rizikos lygis
10	Kompiuterių tinklo įrangos gedimas					
11	Elektros tiekimo sutrikimai					
12	Kompiuterių tinklo paslaugų sutrikimas					
13	Taikomųjų programų klaidos					
14	Tyčinis klaidingų duomenų įvedimas					
15	Atsitiktinis klaidingų duomenų įvedimas					
16	Aparatinės įrangos priežiūros klaida					
17	Programinės įrangos priežiūros klaida					
18	Darbuotojų apsimetimas vienas kitu					
19	Išorinių darbuotojų apsimetimas organizacijos darbuotojais					
20	Gaisras					
21	Padegimas					
22	Vandens žala					
23	Stichinės nelaimės					
24	Vagystė (iš vidaus)					
25	Vagystė (iš išorės)					
26	Sąmoningas išorės asmenų kenkimas					
27	Sąmoningas vidaus asmenų kenkimas					
28	Terorizmas					
29	Vandalizmas					

Išvados