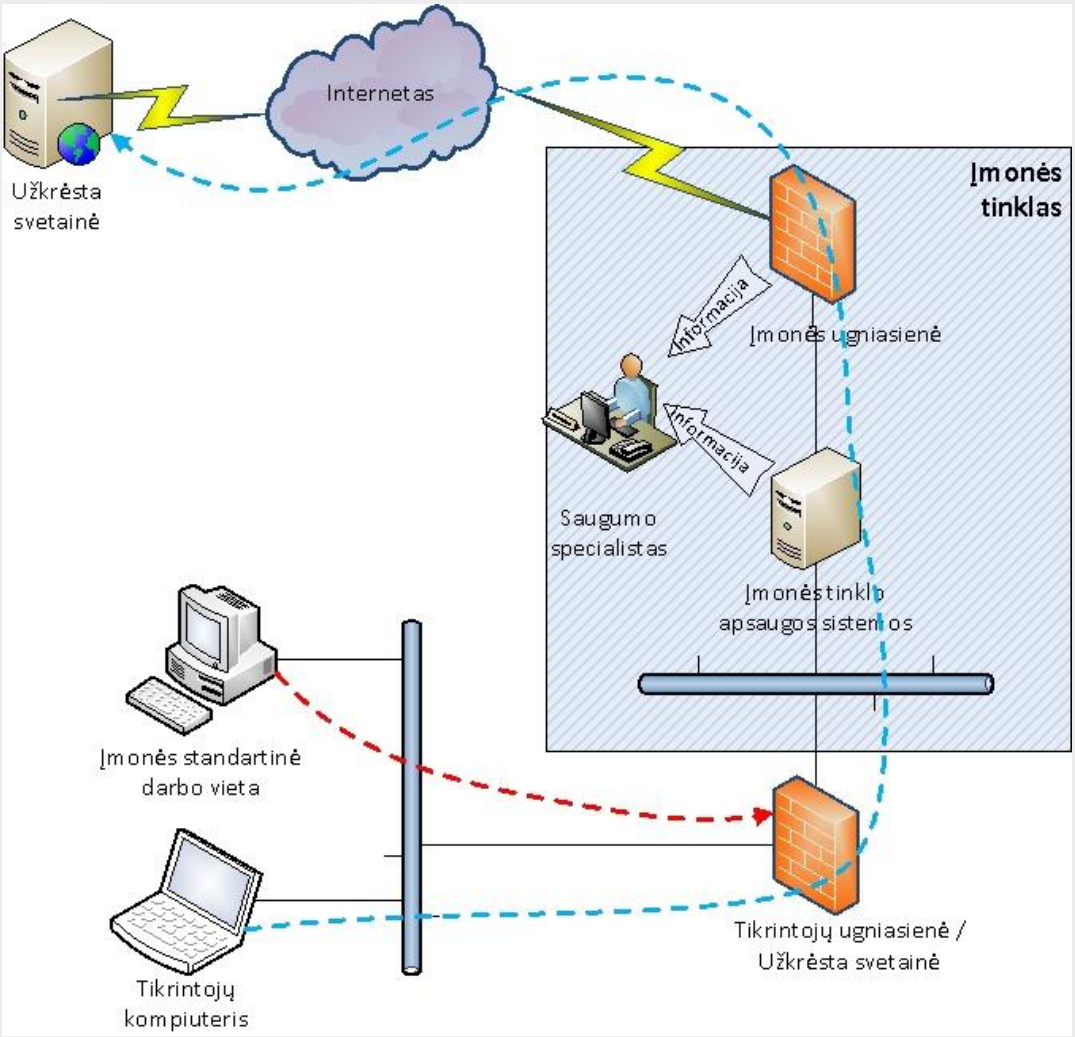
# ĮMONĖS TINKLO SAUGUMO PATIKRINIMAS

Tiek įmonės sistemų, tiek jose laikomos informacijos saugumą užtikrina įvairūs faktoriai. Įmonės tinklą gali saugoti pati geriausia ugniasienė, tačiau jei į vartotojo darbo vietos kompiuterį pateks virusas (pvz., bus atneštas su USB raktu), tai ugniasienė neapsaugos nuo galimos informacijos vagystės ar darbo vietos užšifravimo. Lygiai taip pat svarbus ir žmogiškasis faktorius. Nesvarbu, kaip gerai bus paruošta ir sukonfigūruota įsilaužimo aptikimo sistema (*angl. IDS=Intrusion Detection System*) - jei administratoriai arba už IT saugą atsakingi asmenys neanalizuos IDS ataskaitų, tai net ir pakankamai paprastas įsilaužimas gali būti aptiktas tik po laiko.

Įmonės tinklo saugumą galima tikrinti įvairiais aspektais. Čia neaptariamos tikslinės (*angl. targetted*) atakos, nes jų spektras labai platus ir labai priklauso nuo įmonės naudojamos infrastruktūros. Siūlomas patikrinimas įvertinti įmonės galimybę apsisaugoti nuo atakų, kurios vyksta apsilankius WWW svetainėse ir su kuriomissusiduriama dažniausiai. Žemiau pateikta tokio patikrinimo schema:




Remiantis tokia schema būtų tikrinama:

- apsauga IT tinklo bei infrastruktūros lygyje;
- darbo vietos kompiuterio apsauga;

- tinklo administratorių ir/arba saugos specialistų pasirengimas pamatyti ir sustabdyti problemas.

### Tinklo ir saugos infrastruktūros patikrinimas

Tikrinant tinklo bei infrastruktūros atsparumą naudojama įmonės standartinė darbo vieta ir užkrėsta svetainė, esanti internete. Svetainė yra specialiai parengta tikrinimui, kad kiekvienas kreipinys į ją grąžintų ne tik įprastinį svetainės turinį, bet ir vienokio ar kitokio tipo ataką. Galimi įvairūs atakų tipai, tiek patys naujausi iš pastaruoju metu sutinkamų Lietuvoje, tiek ir senesni. Naršymas atliekamas naudojant tiek paprastą HTTP protokolą, tiek šifruotą - HTTPS.

Užkrėsta svetainė paruošta tokiu būdu, kad iš jos vienos būtų pateikiama visa atakos grandinė. Standartinis toks grandinės pavyzdys būtų toks: 1) įterptas HTML kodas, skirtas nukreipti vartotoją į užkratą platinančią svetainę; 2) užkrato programinis kodas, skirtas patikrinimui ar darbo vieta tinkama užkrėtimui (galimi įvairūs tokio patikrinimo būdai); 3) užkrato vykdomieji failai, kuriuos atsiuntus į darbo vietą atliekamas pastarosios užšifravimas arba kitokio pobūdžio valdymas. Suprantama, realybėje sutinkama užkrato seka gali būti ir sudėtingesnė.

Šiuo būdu siekiama patikrinti ar tinklo infrastruktūra sugeba aptikti užkratą jam dar nepasiekus darbo vietos. Infrastruktūros mazgai, galintys aptikti tokias užkrato grandines, gali būti įvairūs ir priklauso nuo to, kokios tinklo apsaugos priemonės yra naudojamos. Laikoma, kad tinklo infrastruktūra veikia sėkmingai, jei darbo vietos užkratas nepasiekia (nepriklausomai nuo to, kuris mazgas sustabdo srautą).

## Darbo vietos kompiuterio patikrinimas

Tikrinant darbo vietos kompiuterį užkrėstoji svetainė yra ne Internete, bet tikrintojų kompiuteryje. Pastarąjį darbo vieta pasiekia tiesiogiai, t.y., tinklo infrastruktūra užkrato sustabdyti neturi galimybės. Tokiu atveju užkrato sustabdymą lemia tokie veiksniai kaip:

1. Darbo vietoje esančios programinės įrangos būklė, t.y., ar suinstaliuoti naujausi saugumo atnaujinimai;
2. Antivirusinės programos gebėjimas aptikti kenkėjiškas programas. Pastarąjį gebėjimą apsprendžia tiek pats antivirusinės programos modelis, tiek tai, ar antivirusinė programa turi naujausią informaciją apie šiuo metu veikiančius užkratus.

Panašiai, kaip ir infrastruktūros patikrinimo atveju, patikrinimui naudojami skirtingi atakos / užkrato tipai bei skirtingi protokolai (tiek HTTP, tiek HTTPS). Laikoma, kad darbo vietos kompiuterio apsauga veikia sėkmingai, jei užkratas nesuveikia (pvz., darbo vieta nėra užšifruojama, jei tikrinimui naudojamas cryptoware tipo užkratas).

## IT personalo gebėjimo aptikti problemas patikrinimas

Šis patikrinimas atliekamas netiesiogiai, atliekant tiek infrastruktūros, tiek darbo vietos patikrinimus. Jei tinklo infrastruktūroje ar darbo vietoje yra fiksuojamas bandymas įkelti kenkėjišką kodą į vartotojo kompiuterį, tai tokį įvykį turi pastebėti ir įmonės IT saugos specialistai. Jų reakcija reikalinga, nes infrastruktūroje užfiksuoti įvykiai gali būti ne vieninteliai, susiję su konkrečiu užkratu ir paprastai yra reikalinga detalesnė įvykių analizė.

Daugiau informacijos rasite svetainėje http://tyrimai.esec.lt.