# ĮMONĖS TINKLŲ APSAUGA

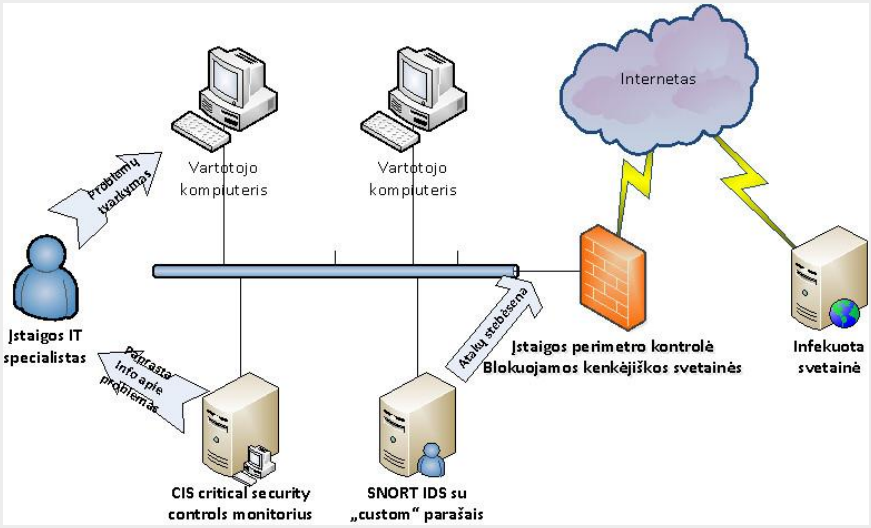
## Įmonės grėsmių valdymas - vartotojų darbo vietos

Remiantis CIS Critical Security Controls saugumo gidais buvo sukurtas aktualiausių grėsmių valdymo gynybinės sistemos modelis. Gynybinės sistemos modelis buvo kuriamas atsižvelgiant į tai, kad įmonės / įstaigos neturi saugumo specialistų, komerciniai saugumo įrankiai sudėtingi ir brangūs, o jų rezultatai dideli pagal apimtį ir nesuprantami paprastam IT darbuotojui. Sukurtas sprendimas / sistema aiškiai ir paprastai įstaigos IT specialistui pasako, kokias konkrečiai problemas reikia tvarkyti.

### Sistema susideda iš:

- darbo vietos kontrolės įrangos, nurodančios kritiškiausias darbo vietos saugumo spragas;
- reguliariai atnaujinamo infekuotų svetainių sąrašo, kuris yra blokuojamas ant įstaigos perimetro;
- SNORT IDS paruoštų ir Lietuvoje labiausiai paplitusių infekcijų parašų;
- Saugos incidentų tyrimo (papildoma paslauga);
- t.t.

### Sistemos principinė schema




### Darbo vietų patikrinimo posistemė

Ši posistemė kasdien surenka informaciją apie darbo vietose įdiegtą programinę įrangą. Renkama yra ši informacija:

- operacinė sistema;
- programinė įranga ir jos versijos;
- programinės įrangos saugumo atnaujinimų būsena.

Turint informaciją apie nesaugią programinę įrangą galima identifikuoti pažeidžiamas darbo vietas. Taip pat kiekvieną dieną yra renkama informacija apie darbo vietose esančių vartotojų turimas administratoriaus teises. Darbo vietos kasdien tikrinamos aktyviu režimu, kai informacija apie darbo vietas paimama iš Microsoft Active Directory. Yra galimybė darbo vietas tikrinti pasyviu režimu pagal įvykį, kai informacija apie darbo vietos aktyvumą tinkle paimama iš tinklo srauto, einančio į internetą. Šiai informacijai gauti naudojama interneto srauto kopija („mirror port"). Sistemoje yra galimybė aprašyti darbo vietas, kuriose tiek programinė įranga, tiek administratoriaus teisės būtų tikrinamos, tačiau nebūtų įtraukiamos į ataskaitas. Iš surinktų duomenų reguliariai formuojamos šios ataskaitos:

- Ataskaita apie darbo vietas su pažeidžiama programine įranga ir/ar perteklinėmis administratoriaus teisėmis;
- Ataskaita apie darbo vietas, kurios tinkle buvo aktyvios, tačiau jų tikrinimai buvo nesėkmingi.

Šios ataskaitos pateikiamas HTML formatu, patalpintos WWW serveryje ir pasiekiamos per interneto naršyklę. Ataskaitos apie darbo vietų būseną sistemos vartotojams generuojamos kiekvieną dieną.

## Organizacijos perimetro apsaugos posistemė

Identifikavus infekuotas svetaines, prieiga prie jų įmonės / organizacijos darbuotojams gali būti blokuota ant perimetro. Darbuotojams bandant patekti į šias svetaines, organizacijos perimetro apsaugos sistema blokuos bandymus prisijungti prie šių svetainių. Lietuvoje vartotojai daugiausiai lankosi lietuviškose svetainėse. Pastebime, kad infekuotų lietuviškų svetainių skaičius sparčiai auga. Mes aktyviai stebime lietuviškų svetainių būklę bei operatyviai atnaujiname infekuotų svetainių sąrašą. Mūsų siūloma perimetro apsaugos posistemė efektyviai stabdo atakas prieš vartotojus, kurie jungiasi prie infekuotų lietuviškų svetainių.

## SNORT IDS

Įsilaužimo aptikimo sistemos tikslas yra detektuoti ir stebėti atakas prieš vartotojus jiems lankantis interneto WWW svetainėse. Sistema yra atnaujinama pagal identifikuotas infekuotas Lietuvoje WWW svetaines, yra sukuriami ir atnaujinami įdiegtos įsilaužimų aptikimo sistemos parašai. Sistema incidentus registruoja duomenų bazėje. Incidentų peržiūra atliekama naudojant interneto naršyklę. Sistemoje galima matyti agreguotą informaciją už tam tikrą laikotarpį pagal incidentą.

Kompiuterinių tinklo infrastruktūros stebėjimo sistema stebi ir identifikuoja infekuotas LT svetaines, kadangi mūsų šalies įstaigų ir įmonių darbuotojai dažniausiai lankosi lietuviškose interneto svetainėse.

Sistema leidžia vykdyti atakų prieš vartotojus stebėseną, vartotojui bandant aplankyti užkrėstą svetainę naudojant „open source“ IDS SNORT su standartiniais (open source, komerciniais ir kt.) bei „proprietary“ parašais pagal iš analitinės sistemos gautą informaciją. Naudojant sukurtus IDS parašus pagal iš analitinės sistemos gautą informaciją, IDS SNORT leidžia gerokai anksčiau aptikti infekuotas svetaines bei atakas prieš vartotojus, kai to dar neaptinka didieji saugumo produktų gamintojai.

| | | | | | | |
|---|---|---|---|---|---|---|
| 40 | 1 | MALWARE-CNC Win.Trojan.Tosct variant outbound connection [sid 33084] [url www.virustotal.com/en/file/d9eb155c016dc105c2290dd72a003894e71cc854a1c9cc75bd37432c6db45634/analysis/] | 1 | 1 | 1 | Summary |
| 41 | 1 | BLACKLIST User-Agent known malicious user-agent string MSIE 4.01 - Win.Trojan.Careto [sid 29760] [url www.virustotal.com/en/file/19e818d0da361c4feedd456fca63d68d4b024fbbd3d9265f606076c7ee72e8f8/analysis/] | 1 | 1 | 1 | Summary |
| 42 | 1 | MALWARE-CNC Win.Trojan.MSIL.Gareme variant outbound connection [sid 31911] [url www.virustotal.com/en/file/c9186bb347ff40e424673600d31ffefa4d10fa41f47c00e2351f539e47c1cf00/analysis/] | 1 | 1 | 1 | Summary |
| 43 | 1 | FILE-OFFICE Microsoft Office Excel malformed XLS out of bounds memory read attempt [sid 39223] [cve 2016-3233] [url technet.microsoft.com/en-us/security/bulletin/MS16-070] | 1 | 1 | 1 | Summary |
| 44 | 1 | MALWARE-CNC Win.Trojan.NetWiredRC variant read logs [sid 38356] [url www.circl.lu/pub/tr-23/] | 1 | 1 | 1 | Summary |
| 45 | 2 | SERVER-OTHER OpenSSL TLSv1.1 heartbeat read overrun attempt [sid 30524] [cve 2014-0160] | 8 | 4 | 7 | Summary |
| 46 | 2 | SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt [sid 30515] [cve 2014-0160] | 2 | 2 | 2 | Summary |
| 47 | 2 | SERVER-OTHER OpenSSL TLSv1.1 large heartbeat response - possible ssl heartbleed attempt [sid 30516] [cve 2014-0160] | 1 | 1 | 1 | Summary |
| 48 | 2 | SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt [sid 30514] [cve 2014-0160] | 1 | 1 | 1 | Summary |
| 49 | 3 | DP: Malicious hosts [sid 1500030] | 960 | 53 | 34 | Summary |
| 50 | 3 | FILE-IDENTIFY Microsoft Windows help file download request [sid 17407] [cve 2004-1306] [cve 2006-3357] [cve 2006-4138] | 615 | 24 | 19 | Summary |
| 51 | 3 | DP: Settimeout(1) [sid 1500019] | 199 | 9 | 13 | Summary |
| 52 | 3 | DP: Malicious domain bestpennystocks.today [sid 1500024] | 104 | 2 | 4 | Summary |
| 53 | 3 | DP: Next hop for Joomla infection [sid 1500004] | 97 | 1 | 2 | Summary |
| 54 | 3 | DP: Malicious jquery.min.php, possibly related to 4lmbkpqrklqv.net [sid 1500022] | 93 | 25 | 19 | Summary |
| 55 | 3 | DP: www.nolovenopain.com [sid 1500010] | 93 | 3 | 4 | Summary |
| 56 | 3 | FILE-IDENTIFY Microsoft emf file download request [sid 2435] [bugtraq 10120] [bugtraq 28819] [bugtraq 9707] [cve 2003-0906] [cve 2007-5746] [url technet.microsoft.com/en-us/security/bulletin/MS04-011] [url technet.microsoft.com/en-us/security/bulletin/MS04-032] [url technet.microsoft.com/en-us/security/bulletin/MS05-053] [url technet.microsoft.com/en-us/security/bulletin/MS06-001] | 85 | 8 | 7 | Summary |
| 57 | 3 | Possible maliciuos users 51.la [sid 1500011] | 84 | 10 | 5 | Summary |
| 58 | 3 | DP: Possible Joomla infection [sid 1500003] | 35 | 7 | 5 | Summary |
| 59 | 3 | DP: Pastebin [sid 1500007] | 29 | 9 | 8 | Summary |
| 60 | 3 | DP: Malicious hosts [sid 1500030] | 12 | 2 | 2 | Summary |
| 61 | 3 | DP: Malicious hosts_2 [sid 1500042] | 12 | 5 | 7 | Summary |
| 62 | 3 | DP: Infection www.sabkuchh.net, possibly related to 4lmbkpqrklqv.net [sid 1500018] | 9 | 3 | 2 | Summary |
| 63 | 3 | DP: Infection redirectoffers.org, related to 4lmbkpqrklqv.net [sid 1500017] | 9 | 3 | 2 | Summary |
| 64 | 3 | BLACKLIST DNS request for known PUA domain mytransitguide.com - MyTransitGuide Toolbar [sid 31705] [url www.virustotal.com/en/ip-address/74.113.233.180/information/] | 9 | 3 | 3 | Summary |
| 65 | 3 | Snort Alert [1:1500041:2] [sid 1500041] | 6 | 2 | 3 | Summary |
| 66 | 3 | DP: Tongji infection [sid 1500008] | 5 | 1 | 1 | Summary |
| 67 | 3 | DP: JS/TrojanDownloader.FakejQuery.A trojan [sid 1500001] | 3 | 1 | 2 | Summary |
| 68 | 3 | DP: demo hack [sid 1500026] | 2 | 1 | 1 | Summary |
| 69 | 3 | DP: JS/Agent.NNS trojan [sid 1500002] | 2 | 1 | 2 | Summary |
| 70 | 3 | DP: www.nolovenopain.com [sid 1500010] | 2 | 1 | 2 | Summary |

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