

CENTRALIZUOTAI VALDOMOS IR ATNAUJINAMOS KENKSMINGOS PROGRAMINĖS ĮRANGOS APTIKIMO, STEBĖJIMO REALIU LAIKU PRIEMONIŲ TECHNINĖ SPECIFIKACIJA

1. PIRKIMO OBJEKTAS

- 1.1. Centralizuotai valdomos ir atnaujinamos kenksmingos programinės įrangos aptikimo, stebėjimo realiu laiku priemonės;
- 1.2. BVPŽ kodas – 48760000-3 Apsaugos nuo virusų programinės įrangos paketai.

2. PIRKIMO OBJEKTO PRITAIKYMO SRITIS

Šiuo pirkimu bus įsigyjamos centralizuotai valdomos ir atnaujinamos kenksmingos programinės įrangos aptikimo, stebėjimo realiu laiku priemonės skirtos VMU kompiuterinių darbo vietų ir tarnybinių stočių apsaugai nuo kenkėjiškų programų poveikio ir įsilaužimo į įmonės kompiuterinio tinklo infrastruktūrą užkardinimui.

3. TECHNINIAI REIKALAVIMAI

Eil. Nr.	Parametras	Minimali reikšmė
1.	Programinės įrangos tipas	Kompiuterinių darbo vietų, serverių, mobiliųjų ir planšetinių įrenginių, apsauga nuo virusų ir šnipinėjimo programų, su ugniasiene, bei apsauga nuo elektroninių šiukšlių. Visi programinės įrangos sprendimai privalo būti valdomi iš vienos administravimo konsolės.
2.	Programinės įrangos gamintojas	Turi būti nurodytas. Visi pateikti apsaugos nuo virusų bei apsaugos nuo el. šiukšlių produktai turi būti pagaminti to paties gamintojo.
3.	Programinės įrangos pavadinimas ir versija	Turi būti nurodyti.
4.	Palaikomos operacinės sistemos	Kompiuterinės darbo vietos: Microsoft Windows 10 32-bit, 64-bit; Microsoft Windows 8.1 32-bit, 64-bit; Microsoft Windows 8 32-bit, 64-bit; Microsoft Windows 7 32-bit, 64-bit; Microsoft Windows Vista 32-bit, 64-bit; Microsoft Windows XP SP3 32-bit; Microsoft Windows XP SP2 64-bit; mac OS 10.9.x ir naujesnės; Mobilieji įrenginiai: Android 5.0 ir naujesnės. Serveriai: Microsoft Windows Server 2003 SP2 (x86/x64); Microsoft Windows Server 2003 R2 SP2 (x86/x64); Microsoft Windows Server 2008 (x86/x64); Microsoft Windows Server 2008 Core (x86/x64); Microsoft Windows Server 2008 R2 (x64); Microsoft Windows Server 2008 R2 Core (x86/x64); Microsoft Windows Server 2012 (x64); Microsoft Windows Server 2012 R2 (x64); Microsoft Windows Server 2012 R2 Core (x64); Microsoft Windows Server 2016 (x64); Microsoft Windows Storage Server 2008 R2 Essentials SP1; Microsoft Windows Storage Server 2012; Microsoft Windows Storage Server 2012 R2; Microsoft Windows Storage Server 2016;

		Microsoft Windows Small Business Server 2003 (x86); Microsoft Windows Small Business Server 2003 R2 (x86); Microsoft Windows Small Business Server 2008 (x64); Microsoft Windows Small Business Server 2011 (x64); Microsoft Windows Server 2012 Foundation; Microsoft Windows Server 2012 Essentials; Microsoft Windows Server 2012 R2 Essentials; Microsoft Windows Server 2016 Essentials; Linux: Suse, Red Hat, Fedora, Ubuntu, Debian. Mandriva (x86/x64); FreeBSD 6.x, 7.x, 8.x ir 9.x (32-bit); Linux Kernel 2.6.x arba naujesnės; glibc 2.3.6 arba naujesnė; Virtualios aplinkos: Microsoft Hyper-V Server 2012 ir naujesnė; VMware vSphere/ESXi 5.0 ir naujesnė; VMware Workstation 9 ir naujesnė; Oracle VirtualBox 4.3 ir naujesnė; Citrix 7 ir naujesnė; Sprendimas turi palaikyti VMware vMotion ir vCenter technologijas. Nuotolinio administravimo konsolės: Microsoft Windows Server 2008 x64 R2 SP1; Microsoft Windows Server 2008 x64 R2 Core; Microsoft Windows Storage Server 2008 x64 R2; Microsoft Windows Server 2012 x64; Microsoft Windows Server 2012 x64 Core; Microsoft Windows Server 2012 x64 R2; Microsoft Windows Storage Server 2012 x64 R2; Microsoft Windows Server 2012 x64 R2 Core; Microsoft Windows Server 2016 x64; Microsoft Windows Storage Server 2016 x64; Microsoft Windows Small Business Server 2011 Standard (x64); Microsoft Windows Small Business Server 2011 Essentials (x64); Linux: RHEL, Debian, Ubuntu, SLED, SLES, OpenSUSE, Fedora ir CentOS bei dauguma kitų RPM ir DEB paketų valdymu pagrįstų platinamų programų. Web administravimo konsolė suderinta su naršyklėmis: Mozilla Firefox 57 ir naujesnė; Microsoft Internet Explorer 11 ir naujesnė; Microsoft Edge 41 ir naujesnė; Google Chrome 63 ir naujesnė; Safari 11 ir naujesnė; Opera 51 ir naujesnė.
5.	Veikimo kokybės reikalavimai	Programinės įrangos gamintojas turi turėti ISO 9001:2000 ir ISO 27001 standartą.
6.	Centralizuoto valdymo reikalavimai	Visi siūlomos programinės įrangos sprendimai turi būti valdomi centralizuotai. Valdymo sistemos diegimą turi atlikti tiekėjas.
7.	Diegimo metodai	Kompiuterinėms darbo vietoms turi būti galimybės:
8.	Būtinai kompiuterinių darbo vietų apsaugos funkciniai moduliai	Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų, grėsmių. Įsilaužimų prevencijos modulis (HIPS).

		Išorinių laikmenų apsaugos modulis. Galimybė atstatyti užkrėstą kompiuterį į ankstesnę būseną. Įsilaužimų blokatorius. Skydas nuo išpirkos reikalaujančių kenkėjų. Ugniasienė. Sprendimas turi leisti pasirinkti, kuriuos apsaugos modulius įdiegti.
9.	Funkciniai reikalavimai kompiuterinių darbo vietų antiviruso moduliui	Antiviruso modulis – programinė įranga, sauganti nuo virusų, šnipinėjimo programų; Sprendimas turi turėti tokias nuskaitymo parinktis: - išmanusis nuskaitymas; - kontekstinio meniu nuskaitymas; - giluminis nuskaitymas; - prie kompiuterio prijungtų išorinių laikmenų nuskaitymas (pvz CD/DVD/USB); - atlikti paskutinį kartą naudotą nuskaitymą; Galimybė vykdyti heuristinį (heuristic) nežinomų failų skenavimą. Galimybė slaptažodžiu apsaugoti nuo antivirusinės programinės įrangos nustatymų pakeitimo bei išdiegimo. Ugniasienės modulis – programinė įranga, sauganti nuo įsilaužimų; Apsaugos nuo elektroninių šiukšlių modulis (Anti-SPAM); Apsaugos nuo botnet tinklų modulis. Turi būti galimybė valdyti šiuos įrenginius: disko atminties įrenginius, CD/DVD, USB spausdintuvus, FireWire saugyklas, Bluetooth įrenginius, lustinių kortelių skaitytuvus, vaizdavimo įrenginius, modemus, LPT/COM prievadus, nešiojamuosius įrenginius. Sprendimas turi leisti/neleisti naudoti įrenginius pagal šiuos kriterijus: tiekėjas, modelis, serijinis numeris. Saugojimo įrenginiams sprendimas turi leisti nustatyti šiuos naudojimo leidimus: skaityti/rašyti, blokuoti, tik skaityti, įspėti. Įsilaužimų prevencijos modulis (HIPS) turi turėti šiuos režimus: automatinis, išsamusis, interaktyvusis, politika pagrįstas, mokymosi. Galimybė riboti prieigą prie internetinių šaltinių. Turi būti galimybė grafinę vartotojo sąsają pasirinkti lietuvių kalba. Kompiuterinių darbo vietų antivirusinės programos dokumentacija turi būti pateikta lietuvių kalba.
10.	Funkciniai reikalavimai darbo vietų ugniasienei	Turi apsaugoti nuo nepageidaujamų tinklo išorinių atakų pagal nustatytus kriterijus (pagal prievadus (port), programas) ribojant atakos šaltinio prieigą. Ugniasienė turi leisti/neleisti prisijungti, remiantis bet kuriuo iš šių režimų: automatinis, interaktyvus, politika pagrįstas, mokymosi. Darbo vietų ugniasienės valdymas turi būti atliekamas centralizuotai administravimo konsolės pagalba.
11.	Funkciniai reikalavimai mobiliųjų telefonų ir planšetinių kompiuterių antiviruso moduliui	Turi užtikrinti apsaugą nuo virusų ir kitų kenkėjiškų programų. Turi turėti galimybę skenuoti tiek vidinę, tiek išorinę (micro SD kortelių) įrenginio atmintį. Skenuoti tam tikrus nustatytus aplankus. Praradus įrenginį, turi būti galimybė nuotoliniu būdu saugiai ištrinti kontaktus, žinutes ir duomenis išorinėje laikmenoje (micro SD). Turi būti galimybė administratoriui SMS žinutėmis vykdyti įvairias saugumo komandas (GPS koordinacių gavimą, įrenginio užrakino, ištyrinimo komandų siuntimą) net kai prarasto įrenginio SIM kortelė pakeista. Turi būti galimybė apsaugoti įrenginį sukčiavimo atveju.

		Turi turėti apsaugos modulį nuo brukalų, leidžiantį apsaugoti įrenginį nuo nepageidaujamų skambučių ar SMS/MMS žinučių. Turi būti galimybė slaptažodžiu apsaugoti nuo antivirusinės programinės įrangos nustatymų pakeitimo bei išdiegimo.
12.	Funkciniai reikalavimai virtualizuotų aplinkų antiviruso moduliui	Sprendimas turi būti valdomas per administravimo konsolę. Turi gebėti atlikti on-access ir on-demand skenavimo užduotis. Turi gebėti atskirti jau nuskaitytus failus vienoje virtualioje mašinoje ir pakartotinai jų nenuskaityti nuo kitų virtualių mašinų per tą patį hypervizorių. Turi turėti galimybę nustatyti proceso išimtis. Turi turėti galimybę siūlomo sprendimo atnaujinimus ir modulius talpinti už virtualių mašinų ribų, kad grąžinant sistemas į ankstesnę momentinę kopiją atnaujinimai nebūtų parsijęti pakartotinai ir atstatymo laikas būtų trumpesnis. Turi būti įgyvendinta galimybė skenuoti išjungtas virtualias mašinas.
13.	Funkciniai reikalavimai mobiliųjų įrenginių valdymo moduliui	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Valdymas įgyvendinamas kuriant politikas, kurios vėliau priskiriamos įrenginiams ar įrenginių grupėms. Turi būti įgyvendinta galimybė užblokuoti mobiliąsias programėles arba jų kategorijas. Galimybė riboti programų naujinimąsi. Turi turėti galimybę uždrausti atstatyti įrenginio gamyklinius parametrus. Turi turėti galimybę uždrausti pašalinti tam tikras mobiliąsias programėles. Turi turėti galimybę žurnalizuoti WIFI, GPS, Roaming duomenis. Turi turėti galimybę masiškai visiems telefonams siųsti informacinį pranešimą tiesiai į ekraną. Turi turėti galimybę blokuoti galimas tekstines žinutes bei skambučius. Turi turėti galimybę matyti įrenginyje sudiegtas mobiliąsias programėles, jų versijas bei jas valdyti. Turi užtikrinti galimybę nuotoliniu būdu įdiegti mobiliąsias programėles be vartotojo pagalbos. Turi turėti galimybę užrakinti/atrakinti mobilųjį įrenginį per nuotolį be vartotojo pagalbos.
14.	Funkciniai reikalavimai valdymo konsolei	Turi palaikyti centralizuotą administravimą nuotoliniu būdu. Serveris turi bendrauti su galutiniais įrenginiais per agentą, kuris gali saugoti politiką ir vykdyti užduotis, kol įrenginys yra neprisijungęs. Serveris turi leisti pridėti įrenginius prie valdymo konsolės naudojant šiuos metodus: - synchronizavimas su Active Directory; - rankiniu būdu įvedus įrenginio vardą arba IP adresą; - technologija gebanti aptikti įrenginius tinkle; Serveris turi leisti sudiegti saugumo sprendimus nuotoliniu būdu ir be vartotojo įsikišimo. Serveris turi leisti kurti statines ir dinamines grupes paprastesniam įrenginių administravimui. Serveris turi leisti nuotoliniu būdu vizualizuoti šią įrenginių informaciją: pagrindinė informacija; - konfigūracija; - atliktos užduotys; - įdiegtos programos; - perspektyvos;

		- karantinas; Turi turėti centralizuotą bendros politikos (politikų) nustatymą visiems programinės įrangos klientams. Turi būti centralizuotai ir automatiškai atnaujinama klientų programinės dalies ir virusų parašų bazė, nereikalaujant sistemos įkrovimo iš naujo. Turi turėti funkcionalumą vartotojų grupėms nustatyti skirtingus klientinės dalies konfigūracinius nustatymus, taip kuriant pasirinktai grupei bendrą saugumo taisyklių rinkinį. Turi turėti antrinio nuotolinio administravimo serverio nustatymo galimybę – nustojus veikti vienam nuotolinio administravimo serveriui administravimas automatiškai turi pereiti kitam nuotolinio administravimo serveriui. Serveris turi turėti mobiliųjų įrenginių valdymo modulį, kuris leidžia prijungti ir valdyti mobiliuosius įrenginius. Privalo turėti techninės priežiūros įrankį: įrankių kontrolės, duomenų bazės perkėlimo, kopijavimo, duomenų bazės lentelių išvalymo. Turi turėti galimybę paveldėti taisykles ir politikas iš aukštesnio lygio nuotolinio administravimo serverio. Turi būti užtikrinta galimybė siųsti informacinius pranešimus į visų rūšių įrenginius, įskaitant stalinius kompiuterius, mobiliuosius įrenginius ar planšetinius kompiuterius. Serveris turi leisti apibrėžti aktyvį, kuris įvykdytų numatytą veiksmą, kai tam tikras įvykis įvyksta tinkle. Pagal numatytuosius nustatymus serveris turi pateikti keletą standartinių ataskaitų bei leisti kurti naujus ataskaitų šablonus. Turi būti galimybė ataskaitas automatiškai gauti el. paštu arba generuoti valdymo konsolėje. Interneto konsolės sąsaja turi dirbti su informacijos skydais. Jie turi būti visiškai interaktyvūs ir leisti atlikti reikiamas užduotis iš kelių sekcijų. Turi būti realizuota galimybė keisti grafines naudotojo informacijos juostas realiuoju laiku. Turi būti galimybė prieigos profilius konfigūruoti naudojant skirtingus leidimus skirtingoms užduotims, pvz.: administratorius, ataskaitų kūrėjas, operatorius ir kita. Po 10 nesėkmingų bandymų prisijungti iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso. Po 15 nesėkmingų bandymų vedant netinkamą seanso ID iš to paties IP adreso, serveris turi laikinai blokuoti tolesnius bandymus prisijungti iš šio IP adreso.
15.	Kiti reikalavimai	Sprendimas turi turėti mechanizmą, kuris leidžia pašalinti bet kurį kitą saugumo sprendimą, esantį galiniame įrenginyje. Šis mechanizmas turi būti: - integruotas į saugumo sprendimą; - pateiktas kaip atskiras įrankis; - pasiekiamas per centralizuotą administravimo konsolę.
16.	Atnaujinimai	Klientinės dalies programinė įranga privalo turėti funkcionalumą parsiųsti atnaujinimus tiesiai iš: - gamintojo atnaujinimų serverio; - centralizuoto valdymo serverio; - kitų klientų. Klientinės dalies programinė įranga privalo turėti funkcionalumą veikti kaip atnaujinimų serveris kitiems klientams tam, kad būtų galima taupyti tinklo pralaidumo resursus.

17.	Aktualumo reikalavimas	Pateikiamoms licencijoms turi būti užtikrinamas gamintojo palaikymas sutarties galiojimo laikotarpiu, užtikrinantis teisę šiuo laikotarpiu be papildomo mokesčio operatyviai gauti naujausius virusų aprašus (signature), virusų paieškos mechanizmo (engine) atnaujinimus. Programinės įrangos gamintojas privalo turėti internetinį puslapį, kuriame būtų žalingų programų ir jų sukeltų pažeidžiamumų duomenų bazė, informacija apie produktus.
18.	Versija	Turi būti siūloma naujausia stabili programinės įrangos versija, oficialiai gamintojo paskelbta internete.
19.	Diegimo failas	Turi būti galimybė diegimo failą atsisiųsti internetu. Pardavėjas turi pateikti bent tris skirtingus valdymo serverio diegimo formatus: - viskas viename; - įdiegimas pagal programos komponentus; - virtualizacijos įrankis.
20.	Dokumentacija	Turi būti pateikta aktuali dokumentacija, apimanti programinės įrangos įdiegimo, bendro naudojimo, administravimo, sistemos atstatymo procedūras.
21.	Gamintojo aptarnavimo (angl. support) sąlygos	Gamintojo atstovas turi teikti nemokamą pagalbą, konsultacijas telefonu, kreipiantis į pagalbos centrą darbo dienomis darbo valandomis lietuvių kalba.
22.	Reikalavimai programinės įrangos naudojimo taisyklėms (licencijavimui)	Licencija turi suteikti teisę pakartotinai diegti siūlomą programinę įrangą neišnaudojant papildomos licencijos. Programinės įrangos licencijavimo taisyklėse licencija turi būti nepririšama prie aparatūrinės įrangos. Licencijos įsigijimo metu turi būti pateiktas vienas licencijos raktas, tinkantis visiems įrenginiams, nepriklausomai nuo licencijos įsigijimo kiekio bei įrenginio tipo. -