Techninės specifikacijos priedėlis Nr. 1

**REIKALAUJAMI ĮRANGOS PARAMETRAI IR FUNKCIONALUMAI**

| **Eil. Nr.** | **Parametras** | **Reikalaujama minimali reikšmė** | **Atitikimas reikalavimui (nurodyti konkretų techninį parametrą arba aprašymą, pateikti nurodytus dokumentus. Užpildyti įrašant tik žodžius „taip“ arba „ne“, negalima)** |
| --- | --- | --- | --- |
|  | Programinės įrangos licencijų paketų skaičius | 370 |  |
|  | Licencijų galiojimo terminas | 1 metai |  |
|  | Programinės įrangos paketo tipas | Kompiuterinių darbo vietų, tarnybinių stočių, tinklinės įrangos, valdymo ir atsarginių kopijų bei el. laiškų filtravimo programinė įranga. Programinė įranga privalo būti teikiama kaip debesijos paslauga.  Visi pateikti stebėjimo, valdymo ir apsaugos elementai turi būti to paties gamintojo. Jeigu siūloma keletas to paties gamintojo produktų, tarp jų privalo būti bendroji autentifikacija (angl. SSO) prisijungiant. |  |
|  | Programinės įrangos gamintojas (-ai) | Nurodyti. |  |
|  | Programinės įrangos pavadinimas (-ai) ir versija (-os) | Nurodyti. |  |
|  | Programinės įrangos reikalavimas saugumui | Tiekėjas negali siūlyti programinės įrangos, kuri kelia grėsmę Lietuvos Respublikos nacionaliniam saugumui. Tiekėjui siūlant programinę įrangą, kuri kelia grėsmę Lietuvos Respublikos nacionaliniam saugumui, pasiūlymas bus atmestas. |  |
|  | Programinės įrangos duomenų apsaugos reikalavimai | Sprendimas privalo atitikti BDAR (angl. GDPR) reglamentą.  Informacija esanti gamintojo duomenų centre turi būti šifruota ne mažesniu kaip AES 256-bit šifravimo raktu. |  |
|  | Kokybės reikalavimai | Programinės įrangos gamintojas (-ai) privalo turėti atitiktį ISO27001 ir ISO9001 standartams. |  |
|  | Veikimo principas | Kliento (agento) – serverio principu veikianti integruota, modulinė programinė įranga. Programinė įranga privalo veikti debesijos pagrindu, nereikalaujant lokalaus serverio esančio savame tinkle |  |
|  | Valdymo konsolė | Web administravimo konsolė suderinta su šiomis naršyklėmis:  *Mozilla Firefox*  *Microsoft Edge*  *Google Chrome*  *Safari*  Vartotojų ir administratorių portalas turi turėti dviejų faktorių autentifikacija. |  |
|  | Diegimo metodai | Diegti klientinę programinės įrangos dalį (agentą) į kompiuterines darbo vietas ir serverius, turi būti šios galimybės:  - centralizuotai iš valdymo konsolės;  - diegti programinę įrangą lokaliai iš diegimo laikmenos;  - diegti programinę įrangą per *Active Directory Group Policy* nustatymus.  - tiesiogiai iš kitų klientų (agentų) vietiniame tinkle. |  |
|  | Kompiuterinių darbo vietų, tarnybinių stočių, tinklinės įrangos ir tinklų monitoringas | Monitoringo modulis – agentinė programinė įranga nurodytu laiku ir/ar intervalu, stebinti fizinius parametrus, procesus, servisus, programinės įrangos versijas, tinklinę įrangą ir tinklus bei jų būklę. Sprendimas turi leisti konfigūruoti, pridėti ar atimti stebimus parametrus, rankiniu, bei automatizuotu būdais.  Sprendimas turi turėti galimybę stebėti kritinius duomenų bazės rodiklius. Sprendimas turi turėti galimybę stebėti kompiuterinės darbo vietos ir serverių kritinius rodiklius. Sprendimas turi turėti galimybę stebėti procesų ir servisų būkle.  Sprendimas turi turėti galimybę komunikuoti su tinkline įrangą per SNMP protokolą iš klientinės dalies.  Sprendimas turi turėti galimybę įkelti savo scenarijus ir palaikyti šiuos formatus: *sh, js, vbs, cmd, bat, pl, php, py, rb, ps1, amp.* |  |
|  | Palaikomos operacinės sistemos | Kompiuterinės darbo vietos:  *Palaikomos:*  *Windows 10 Pro, Enterprise 32-bit, 64-bit; Windows 11;*  *macOS 11.x, 12.x, 13.x, 14.x, 15.x;*  Serveriai:  *Microsoft Windows Server 2016*  *ir naujesnės;*  *RedHat RHEL 7, 8, 9;*  *CentOS 7, 8, 9;*  *Debian 10, 11, 12;*  *Ubuntu 20.04, 22.04* |  |
|  | Infrastruktūros inventorizavimas | Infrastruktūros inventorizavimo modulis – skirtas tinklo skanavimui ir infrastruktūros, bei įrangos inventorizacijai.  Sprendimas turi turėti galimybę atlikti tinklo skanavimą ir tinkle esančios įrangos, fizinės ir programinės įrangos auditą, bei matyti kliente įdiegtos programinės įrangos licencijų raktus. |  |
|  | Nuotolinis valdymas | Valdymo modulis – programinė įranga skirta valdyti įrenginius ar programinę įrangą nuotoliniu būdu.  Sprendimas turi turėti galimybę konfigūruoti kontrolės perėmimo politiką. Sprendimas turi turėti galimybę perimti įrenginio kontrolę iš vartotojo, pagal priskirtą įrenginio kontrolės perėmimo politiką.  Sprendimas turi turėti galimybę valdyti kompiuterinę įranga netrukdant galutinio vartotojo (angl. silent mode) režimu. Prie įrenginio prisijungus šiuo būdu turi būti galimybė naudotis cmd, powershell, perkelti failus, stabdyti procesus, stabdyti bei pradėti servisus, keisti registrų raktus. |  |
|  | Automatizavimas | Automatizacijos modulis – skirtas automatizuoti procesus ar užduotis, remiantis monitoringo rezultatais.  Sprendimas privalo turėti galimybę valdyti procesų ir užduočių automatizaciją, pagal monitoringo pateikiamas reikšmes. Sprendimas privalo leisti įsikelti ar kurti automatizuotas užduotis pasitelkus vidinius įrankius, nereikalaujant mokėti scenarijų kalbą (angl. script language). |  |
|  | Programinės įrangos naujinių ir saugumo spragų pataisų valdymas | Programinės įrangos naujinių ir saugumo spragų pataisų valdymo modulis – skirtas atnaujinti programinę įrangą kliento pusėje ir kamšyti saugumo spragas, atsižvelgiant į priskirtas politikas.  Sprendimas turi turėti galimybę valdyti saugumo spragų pataisų diegimą. Sprendimas turi turėti galimybę atnaujinti, naujai įdiegti ir išdiegti trečiųjų šalių programinės įrangos atnaujinimus. Sprendimas turi turėti politikų mechanizmą ir politikomis, valdyti saugumo spragų pataisų diegimą ar išdiegimą.  Sprendimas turi galėti atnaujinti aplikacijas Windows, bei MacOS įrenginiuose.  Klientinės dalies programinė įranga privalo turėti galimybę klientą (angl. Agent) paskirti kaip lokalų atnaujinimų serverį, taip užtikrinant jog atnaujinimai būtų siunčiami vidiniu tinklu.  Privalo turėti funkcionalumą, leidžiantį peržiūrėti atnaujinimų diegimo istoriją ir įvykusių atnaujinimų būklę.  Programinė įranga privalo turėti galimybę diegti atnaujinimus pagal nustatytą grafiką, atsižvelgiant į darbo laiko apribojimus.  Programinė įranga turi pateikti detalias ataskaitas apie įrenginius, kuriems reikalingi saugumo pataisymai. |  |
|  | Kompiuterinių darbo vietų rezervinės kopijos ir jų atstatymas | Sprendimas privalo atlikti Windows, Linux ir MacOS rezervines kopijas. Turi būti galimybė rezervines kopijas atliekti ne rečiau, nei kas 15 minučių. Atsarginės duomenų kopijos turi būti saugomos gamintojo teikiamame duomenų centre. Turi būti galimybė laikyti antrinę rezervinę kopiją lokaliai, siekiant spartesnio atstatymo. Kompiuterinių darbo vietų rezervinės kopijos turi būti saugomos ne mažiau kaip 10 metų.  Turi būti galimybė atstatyti vieną ar kelis pasirinktus failus, visą įrenginį kaip virtualią mašiną, bei į pradinę (neįdiegtą) aparatinę įrangą. Sprendimas privalo leisti pasirinkti laiką kuomet būtų apribojamas tinklo duomenų sunaudojimas atliekant rezervines kopijas.  Sprendimas privalo užtikrinti duomenų saugumą dvigubu šifravimu, duomenys turi būti užšifruoti kliento (angl. Agent) pusėje ir siunčiamas į gamintojo duomenų centrą šifruotu kanalu, AES 256-bit standartu. |  |
|  | Microsoft 365 rezervinės duomenų kopijos ir avarinis jų atstatymas | Rezervinių kopijų ir avarinio atstatymo modulis – skirtas apsaugoti svarbią darbinę informaciją nutolusiame serveryje.  Atsarginės duomenų kopijos turi būti laikomos gamintojo siūlomame duomenų centre.  Sprendimas privalo atlikti Exchange Online, Sharepoint, Onedrive ir Teams atsarginęs kopijas.  Sprendimas privalo atlikti ne mažiau kaip 4 atsargines kopijas per parą.  Rezervinė duomenų kopija privalo būti saugoma ne mažiau kaip 7 metus.  Sprendimas privalo užtikrinti duomenų saugumą dvigubu šifravimu, duomenys turi būti užšifruoti kliento (angl. Agent) pusėje ir siunčiamas į gamintojo duomenų centrą šifruotu kanalu, AES 256-bit standartu. |  |
|  | Microsoft 365 el. pašto apsauga | Sprendimas turi būti paremtas debesų pagrindu. Sistema turi veikti be vietinės infrastruktūros, užtikrinant pasiekiamumą per internetą. Turi užtikrinti apsaugą nuo šlamšto, virusų, kenkėjiškų programų, apsimestinių laiškų, nuo kompromituotų paskyrų ir kitų grėsmių.  Sistema turi aptikti ir blokuoti šlamštą, virusus, ransomware, phishing, spoofing.  Galimybė siųsti ir gauti laiškus net pagrindinio serverio prastovos metu.  Ilgalaikis el. pašto archyvavimas su galimybe nustatyti saugojimo laikotarpį.  Naudojamas TLS šifravimas duomenų perdavimui, AES-256 duomenų saugojimui.  Sistema turi palaikyti SPF, DKIM ir DMARC protokolus. Dinaminis politikų tikrinimas ir ataskaitos.  Didesnis nei 99,9% filtravimo tikslumas.  Vidutinis laiškų apdorojimo laikas, ne didesnis nei 30 sekundžių.  Automatinė pašto dėžučių sinchronizacija, SSO palaikymas.  Naudojamas mašininis mokymasis ir dirbtinis intelektas aptikti naujas grėsmes (zero-day).  Detali veiklos istorija, eksportas į CSV/PDF.  REST API galimybė integracijai su kitomis sistemomis (ITSM, SIEM, M365).  Galimybė siųsti užšifruotus laiškus, saugus portalas gavėjams.  Blokavimas pagal šalį, IP adresą, regioną.  Automatinis atsarginių MX serverių valdymas. Užtikrinamas el. pašto srautas net pagrindinio serverio gedimo metu.  Karantino valdymas, pranešimų peržiūra iš mobiliųjų įrenginių.  Galimybė blokuoti pavojingus priedus (makro, skriptus, vykdomuosius failus).  Vartotojų ir administratorių portalas su dviejų faktorių autentifikacija.  Įtartini priedai izoliuojami ir analizuojami saugioje aplinkoje. |  |
|  | Mobilioji aplikacija | Platforma turi turėti mobiliąją aplikaciją, skirtą stebėti darbo vietas, serverius ir tinklinę įrangą. Atlikti nuotolinę pagalbą tiesiai iš mobiliojo įrenginio. |  |
|  | Pranešimai | Pranešimų modulis – skirtas informuoti platformos administratorius pagal sukonfigūruotus parametrus ar priskirtas politikas.  Sprendimas turi turėti galimybes informuoti platformos administratorius, elektroniniu paštu, sms žinute, atvaizduojant platformos mobiliojoje aplikacijoje ar centrinėje administravimo konsolėje.  Sprendimas turi turėti galimybę kurti ir redaguoti pranešimų politikas. |  |
|  | Ataskaitos | Ataskaitų modulis – skirtas generuoti ataskaitas.  Sprendimas turi turėti galimybę pateikti standartines, iš anksto sudarytas ataskaitas  Sprendimas turi turėti galimybę ataskaitas siųsti el. paštu automatiškai arba generuoti valdymo konsolėje. |  |
|  | Vartotojų teisių valdymas | Vartotojų teisių modulis – skirtas konfigūruoti ir priskirti vartotojo roles.  Sprendimas turi turėti galimybę kurti ir konfigūruoti vartotojų roles, leisti jas priskirti vartotojams pvz.: administratorius, ataskaitų kūrėjas, operatorius ir kita. |  |
|  | Administravimas | Administravimo modulis – skirtas numatyti centralizuotos valdymo konsolės nustatymus.  Sprendimas turi leisti kurti, redaguoti, panaikinti ar sujungti politikas.  Sprendimas turi turėti galimybę paveldėti politikas (angl. Policies) iš aukštesnio lygio dinaminės grupės, nustatant tai centrinėje valdymo konsolėje, bei leisti konfigūruoti politikas atskiroms įrenginių grupėms. |  |
|  | Prieigos saugumas | Sprendimas privalo turėti dviejų veiksnių (faktorių) autentifikaciją.  Sprendimas turi turėti IP adresų apribojimo galimybę prisijungiant. |  |
|  | Funkciniai reikalavimai valdymo konsolei | Turi palaikyti centralizuotą administravimą nuotoliniu būdu.  Centralizuota valdymo konsolė turi bendrauti su galutiniais įrenginiais per klientą (angl. Agent), galėti saugoti politikas ir vykdyti užduotis, kol įrenginys yra neprisijungęs.  Sprendimas turi leisti pridėti įrenginius prie centrinės valdymo konsolės naudojant šiuos metodus:  - rankiniu būdu su instaliacinių paketu;  - aptikti įrenginius vidiniame tinkle;  Sprendimas turi leisti sudiegti klientinę dalį nuotoliniu būdu ir be vartotojo įsikišimo.  Sprendimas turi leisti kurti statines grupes lengvesniam įrenginių administravimui.  Sprendimas turi turėti galimybę iš centrinės valdymo konsolės valdyti ir priskirti politikas, nustatymus visiems programinės įrangos klientams (angl. Agents).  Gamintojas turi užtikrinti sprendimo kaip debesijos paslaugos, serverių pasiekiamumo aukštą patikimumą (angl. High Availability). |  |
|  | Atnaujinimai | Atnaujinimų modulis – skirtas atnaujinti klientinės programinės įrangos dalį.  Sprendimas turi turėti galimybę atnaujinti klientinę programinę įrangą automatiškai, iš centrinės valdymo konsolės. |  |
|  | Versijų valdymas | Gamintojas privalo pranešti apie programinės įrangos versijos ir klientinės dalies (angl. agent) versijos atnaujinimus oficialiame tinklapyje ir techninėje sprendimo dokumentacijoje. |  |
|  | Dokumentacija | Turi būti pateikta aktuali dokumentacija, apimanti programinės įrangos įdiegimo, bendro naudojimo, administravimo, sistemos atstatymo procedūras. |  |
|  | Diegimas ir mokymai | Diegimui turi būti numatytas reikiamų valandų kiekis, taip pat nemažiau kaip 12 val. mokymai 3 administratoriams. |  |
|  | Gamintojo aptarnavimo (angl. support) sąlygos | Gamintojo atstovas turi teikti nemokamą pagalbą, konsultacijas telefonu ar paštu, kreipiantis į pagalbos centrą darbo dienomis darbo valandomis lietuvių kalba. |  |