**Жұмыс станцияларын қорғауға арналған орталықтандырылған басқаруы бар кешенді антивирустық қорғаныс жүйесі арналған техникалық спецификациясы.**

**Көңіл бөліп оқитын әлеуетті Жеткізушілерге: Ұсынылатын антивирустық бағдарламалық қамтамасыз ету осы техникалық тапсырманың барлық тармақтарына толық сәйкес келуі тиіс. Жартылай сәйкестікке рұқсат етілмейді және қабылданбайды. Әлеуетті жеткізуші тұтынушы орналасқан жерде физикалық орнатуды жүзеге асыруы керек.**

1. **Жалпы талаптар**
   1. Жеткізуші, жеңімпаз ретінде танылған, Тауарды/Қызметті жеткізген кезде өндірушімен серіктестік қатынастарын растайтын жазбаша растаманы ұсынуы тиіс. Растау ретінде серіктестің атын көрсете отырып сертификат, авторизациялау хат немесе жеткізушінің «Серіктестер» бөлімінде көрсетілген ресми өндіруші сайтындағы сілтеме пайдаланылуы мүмкін.
   2. Лицензия кемінде 14 құрылғыны қорғауды қамтуы тиіс, соның ішінде кемінде 14 жұмыс станциясы (Windows, Linux және macOS) және файлдық серверлер үшін.
   3. Лицензияның әрекет ету мерзімі тұтынушы лицензияны іске қосқан сәттен бастап кемінде 12 (он екі) айды құрауы тиіс.
   4. Қызметтерді көрсету шеңберінде Әлеуетті Жеткізуші **Тұтынушының орналасқан жерінде жеткізілетін бағдарламалық құралды физикалық орнату бойынша қызметтерді көрсетуге міндетті.**
   5. Өндірушінің Қазақстан Республикасындағы жергілікті техникалық қолдауды орыс және қазақ тілінде көрсету қызметінің болуы шарт.
   6. Барлық антивирус құралының бағдарламалық интерфейсі орыс және қазақ тілінде жасалған болуы керек.
   7. Microsoft Windows операциялық жүйесімен басқарылатын бүкіл антивирус құралында, соның ішінде басқару құралдарында, орыс және қазақ тіліндегі мәнмәтіндік анықтамалық жүйе болуы шарт.
   8. Конкурсқа қатысушы барлық жеткізілетін өнімдерге біріңғай сериялық нөмірді беруі керек. Бүкіл жеткізілетін бағдарламалық өнімдердің лицензиялық негізгі файлдарының жарамдылық мерзімі сериялық нөмірді іске қосқан сәттен басталуы керек.
   9. Контрафактілік бағдарламалық қамтамасыз етуді жеткізуді болдырмау мақсатында әлеуетті өнім беруші бағдарламалық қамтамасыз етудің заңды шығу тегін растайтын өндіруші компаниядан хат ұсынуы тиіс.
   10. Жеткізілетін өнімге сенімділіктің есептік деңгейі (СЕД4) бойынша ҚР СТ ISO/IEC 15408-3-2017 стандарты талаптарына сәйкестігін растайтын Қазақстан Республикасының Мемлекеттік техникалық реттеу жүйесі сертификатының болуы.
2. **Антивирус қорғанысына қойылатын жалпы талаптар**
   1. Жүйенің бағдарламалық құралдары келесі түрдегі қауіптерді анықтауды қамтамасыз етуі керек: классикалық вирустар, трояндық бағдарламалар, руткиттер, желілік құрттар, жарнамалық бағдарламалар, ақылы сайттарға автоматты қоңырау шалу, ықтимал қауіпті қолданбалар және басқа да зиянды бағдарламалар.
   2. Антивирус қорғанысы мыналарды қамтамасыз етуі тиіс:
      1. 64 разрядты операциялық жүйеге бағытталған қатерді анықтау, соның ішінде модуль антируткитінің арнайы 64 битті нұсқасының көмегімен анықтау;
      2. мұрағаттар мен қапталған файлдарды тексеруді жеделдету мақсатында ашу құралын іске қоспай зиянды бағдарламаларды анықтау;
      3. файлдағы PKLITE, LZEXE, DIET, COM2EXE және с.с. типті бағдарламалармен қапталған вирустарды тауып жою;
      4. шифрланған контейнерлері бар ACE (2.0 нұсқасына дейін), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO (соның ішінде NRG, сектордың бейстандартты форматы бар және сигнатуралары жоқ бейнелер), ZLIB, VCLZIP, VISE, PST, DMG, PDF, GHOST INSTALLER форматындағы контейнерлер мен мұрағатталған файлдардағы вирустарды тексерілетін нысандардың салыну деңгейіне қойылатын шектеуге қарамастан анықтау;
      5. қатаң форматы жоқ (HTML, MIME), контейнерлердегі вирустарды анықтау;
      6. нысан мөлшері анық емес контейнер ішіндегі вирустарды анықтау (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES және т.с.с.);
      7. форматы Smart Install Maker (SIM); DMG, HFS, XAR, Universal Binary (MacOS); SIS (Symbian 9); INNO SETUP (5.3.9 және жоғары); SETUP FACTORY (7,8 тізбегіндегі); XENOCODE; TARMA INSTALL (3-тізбек); XZ (UNIX); COMPRESS; SQUAHFS; CHILKAT ZIP; LHA (AWARD BIOS) бумасы бар файлдар мен нысандарда вирустың болуы тексеру;
      8. қаптамадан өздігінен шығатын мұрағаттардағы вирустарды тексеру: AppPackager, Astrum Install Wizard, Create Install, Fly Ina Studio, GSFX, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Mad Thunder Setup System, Wise Installation System, Alloy;
      9. төмендегідей қаптағыштармен қапталған орындалатыны файлдарды тексеру: PELOCK, ENIGMA Protector, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR, ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, RCRYPTOR, PECRYPT, сондай-ақ Mozilla Thunderbird поштасындағы файлдарды олардың мөлшеріне қарамастан тексеру;
      10. форматталмаған пошта базаларын талдау және тіркемесі үлкен хаттарды өңдеу (мысалы, жауаптары көп хаттарды және қайта жіберілген хаттарды RE/FW), TNEF форматын қолдау;
      11. Тиісті ақпаратты антивирус базаларына енгізгеннен кейін жасалған және әлі антивирустық зертханаларға талдауға түсе қоймаған антивирус базаларында ақпараты бар зиянкес бағдарламалар тобына жататын зиянкес бағдарламалардан эвристикалық талдау негізінде және файл ішінде кодтардың орналасу аймағын талдауға негізделген ұқсас вирустарды іздеу технологиясы арқылы қорғау;
      12. HTML және PDF құжаттарда зиянкес нысандарды, соның ішінде осы типтегі құжаттарда тұрған JavaScript ішіндегі обфускацияланған эксплойттарды табу. «көрінбейтін» IFRAME-элементтерді шығарып талдау мүмкіндігі. Кез келген күрделі скриптілерді шығару мүмкіндігі және олардың қорғанысын алып тастау;
      13. лицензиялық деректерге келетін қатерді анықтау (ASPROTECT, PEP және ENIGMA);
      14. DEX-файлдардағы (Android) зиянкес нысандарды анықтау;
      15. белгісіз қаптағыштармен жасырынған вирустарды тауып жою.
3. **Microsoft Windows тобының операциялық жүйесімен басқарылатын жұмыс станциялары мен серверлердің антивирустық қорғаныс құралдарына қойылатын талаптар**
   1. Тендерді өткізу кезінде өзекті БҚ түрін пайдаланғанда, жүйе (орталықтандырылған басқару жүйесі көмегімен бірге) операциялық жүйенің басқаруымен жұмыс станциялары мен серверлердің қорғанысын қамтамасыз етуі тиіс.

* MS Windows XP SP2 / Windows Vista SP2/ Windows 7 SP1/ Windows 8 / Windows 8.1 / Windows 10 / Windows 11.
* MS Windows Server 2003 SP1 / Windows Server 2008 SP2/ Windows Server 2008 R2 SP1/ Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016 / Windows Server 2019 / Windows Server 2022.
  1. Жүйенің бағдарламалық құралы жұмыс станцияларында антивирус және спамға қарсы қорғанысты жүзеге асыруды, оның ішінде руткиттер технологияларынан тұрақты қорғауды, резидент антируткит драйверінің болуын қамтамасыз етуі керек.
  2. Жүйеде зиянкес бағдарламалар вирус жұқтырған желі нысандарын алдын ала емдеместен, оларға өз компоненттерін орнату мүмкіндігі болуы керек.
  3. Нысанда іске қосылып тұруы ықтимал зиянкес бағдарламаларға қарсы әрекет ету мақсатында, орнату үшін антируткитпен қорғалған орнатқыш бағдарлама (Windows Installer-ді қолданбай) пайдаланылуы шарт.
  4. Интернет желісіне қосылу арнасының ықтимал шектеулеріне байланысты қорғау жүйесін орнату Интернет желісіне қосылмастан мүмкін болуы керек – дистрибутивті қорғау жүйесінің барлық компоненттері, сондай-ақ зиянкес бағдарламалар мен Интернет желісі ресурстарының дерекқоры болуы тиіс.
  5. Қорғаныс жүйесінің жұмысы үшін сыртқы кітапханалар және .Net Framework ортасы пайдаланылмауы тиіс, олардың бүтіндігі өзін-өзі қорғау жүйесінің бақылауында тұрмаған және оларды әшкерелеу салдарынан қорғаныс жүйесінің ақпараты қате көрсетілуі немесе қорғаныс жүйесінің интерфейсіне байланысты басқа да проблеманы туындатуы мүмкін.
  6. Жүйе компоненттерінде пайдаланушылардың жайлы жұмыс істеуін қамтамасыз ету үшін, соның ішінде «оқу үшін» ашылатын файлдарды кейін тексеру мүмкіндігі есебінен ДК ресурстарын пайдалануды басқару, сондай-ақ заманауи құрылым ерекшеліктерін пайдалану мүмкіндігі болуы керек.
  7. Жүйе жергілікті желіде және Интернет желісінде жұмыс істеген кезде қорғанысты қамтамасыз ететін конфигурациямен, Web-беттермен, электрондық поштамен, жергілікті қатты дискілермен және алмалы-салмалы тасығыштармен бірге жеткізілуі тиіс. Кіріс және шығыс электрондық хаттар зиянкес бағдарламалардан және спамнан қорғалған болуы шарт.
  8. Жүйе пайдаланушылардың Интернеттегі жұмыс уақытын, сонымен қатар компьютерде жұмыс істеу уақытын шектей алуы керек.
  9. Пайдаланушыларға арналған антивирус топтамасы компоненттерінің баптауларына кіру рұқсатының құқықтарын Жүйе әкімшісі белгілеуі тиіс және пайдаланушыларда әкімші берген құқықтар шегінде ғана оларды өз бетінше және құпия сөзді қолданбастан баптау мүмкіндігі болуы керек.
  10. Жұмыс станцияларын қорғау жүйелері Mail.Ru Agent, ICQ, Jabber, QIP, Pidgin және басқа қолданбалардағы лезделік хабарламалардың трафигін сүзуді, соның ішінде қайта жолданатын тіркемелердің антивирустық тексерісін, сондай-ақ хабарламалардан зиянкес және фишингтік сайттарға апаратын сілтемелерді автоматты түрде жоюды қамтамасыз етуі керек.
  11. Жұмыс станцияларын қорғау жүйесі Google, Yandex, Yahoo! Bing, Rambler іздеу жүйелері нәтижелерінің шығарылуын тек іздеу жүйелері мен қорғау жүйесі тұрғысынан қауіпсіз деп саналатын ресурстарды көрсетіп сүзуі тиіс.
  12. Қолданбалар деңгейінде, нақты бағдарламалар мен процестердің желі ресурстарына қол жеткізуін басқаруға және қолданбалар журналында қол жеткізу әрекеттері туралы ақпаратты тіркеуге мүмкіндік беретін желілік қосылымдарды басқару.
  13. Қосылымға бастама болатын бағдарламаларға тәуелсіз Интернет желісіне кіруді басқаруға мүмкіндік беретін бумалар деңгейіндегі сүзу.
  14. Жүйеде төмендегідей компоненттерден тұратын сигнатуралық және эвристикалық талдауға қосымша алдын ала қорғау жүзеге асырылуы керек:
* бопсалаушылардан қорғағыш – трояндық-шифрлаушылардан қорғауға мүмкіндік береді;
* эксплойттардан қорғағыш – жүйеге ену үшін танымал қолданбаларда осалдықтарды пайдалануға тырысатын зиянды нысандардан қорғауға мүмкіндік береді;
* әрекет талдауы – жүйе тұрғысынан маңызды болып табылатын барлық салаларда іске қосылған бағдарламалардың әрекетін бақылау, мысалы: HOSTS файлы; іске қосылған қолданбалардың тұтастығы; дискіге төмен деңгейлі қол жеткізу; драйверлерді жүктеп салу; қолданбаларды іске қосу параметрлері; мультимедиялық құрылғы драйверлері; Winlogon қабықшасының параметрлері, Winlogon нотификаторлары; Windows қабықшасының автоматты іске қосылуы; орындалатын файлдардың ассоциациялары; бағдарламаларды іске қосуды шектеу саясаты (SRP); Internet Explorer плагиндері (BHO); бағдарламаларды автоматты іске қосу; саясаттарды автоматты іске қосу; қауіпсіз режимді конфигурациялау; Windows сеансы диспетчерінің параметрлері; жүйелік қызметтер.
  1. Жүйе өзінің барлық объектілерін, соның ішінде маңызды файлдарды, процестерді, терезелерді, кілттерді және т.б. пайдаланушылардың рұқсатсыз кіруінен және зиянды бағдарламалардан өзін-өзі қорғауды жүзеге асыруы керек, олар жүйенің ең төменгі деңгейінде жұмыс істеуі керек және антивирустық жүйенің драйвелреін түсіру және тоқтату мүмкіндігін шектеуі керек.
  2. Виртуалды агенттерді орнату арқылы виртуалды жұмыс орындарын қорғауды жүзеге асыру мүмкіндігі.

1. **Linux тобының операциялық жүйесімен басқарылатын жұмыс станциялары мен серверлердің антивирустық қорғаныс құралдарына қойылатын талаптар**
   1. Құрылымы төмендегідей процессорларды және пәрмендер жүйесін қолдау:

* Intel/AMD: 32-бит (IA-32, x86); 64-бит (x86-64, x64, amd64);
* ARM64;
* IBM POWER (ppc64el).
  1. Жүйе операциялық жүйелердің басқаруымен 3.6 - 4.16 Samba немесе Novell Storage Services (NSS) версияларын пайдаланатын жұмыс станциялары мен серверлердің қорғанысын қамтамасыз етуі тиіс:
* 2.6.37 және жаңа нұсқалы ядро негізінде жасалған, PAM және 2.13 мен жаңа нұсқалы glibc кітапханасын пайдаланатын Linux;
* FreeBSD 11, 12;
* Novell Open Enterprise Server SP2 на базе SUSE Linux Enterprise Server 10 SP3 және жаңалары.
  1. Жүйенің Samba-мен бірігуі VFS (Virtual File System) модулінің көмегімен жасалуы тиіс.
  2. Нұсқасы жоғарыда көрсетілгендерден басқа Samba нұсқасын немесе Linux тобының 64-битті платформаларына арналған Samba пайдаланылған жағдайда, біріктіру модульдерін бастапқы кодтардан компиляциялау мүмкіндігі болуы тиіс.
  3. Операциялық жүйенің типі мен нұсқасына қарамастан, UNIX-жүйелеріне арналған әмбебап топтамадан репозиторийді немесе операциялық жүйеде топтама менеджері пайдаланатын жұмысқа есептелген топтаманы орнату мүмкіндігі.
  4. Жүйені пәрмен жолағынан және графикалық орнатқыш көмегімен орнату және жаңарту мүмкіндігі.
  5. Жүйенің қажетті компоненттерін орнату үшін қажет модульдерді автоматты түрде орнату мүмкіндігі.
  6. Жүйенің компоненттерін зиянкес бағдарламалар вирус жұқтырған нысандарды алдын ала емдемей сол нысандарға орнатып, одан кейін белгіленген файл аймақтарын емдеу мүмкіндігі.
  7. SELinux қосымша қауіпсіздікті қамтамасыз ететін ішкі жүйелерге, PARSEC рұқсатын мандаттық басқару жүйесін, сондай-ақ тұйық бағдарлама ортасын (ТБО) режимін қолдау.
  8. Операциялық жүйе ұсынатын fanotify механизмін пайдалану арқылы және Linux (Linux kernel module) ядросының арнайы модулінің көмегімен файл жүйесін мониторингілеу мүмкіндігі.
  9. Файл жүйесінің жаңа томдарын орнату және бөлшектеу сәтін (мысалы, USB-flash, CD/DVD жинақтағыштарында, RAID массивтері және т.б.) автоматты түрде анықтау және қажетіне қарай бақылау жасалатын аймақтар тізімін түзету мүмкіндігі.
  10. Файл кеңістігін сканерлеу кезінде сервер ресурстарын пайдалану процесін басқару мүмкіндігі.
  11. Мұрағат, пошта файлдары, қапталған нысандар мен басқа да контейнерлер сияқты құрамдас файлдарды тексеру параметрлерін басқару мүмкіндігі.
  12. Жүйеде SSL және TLS негізіндегі протоколдарды пайдаланатын қорғалған желі қосылыстары арқылы берілетін трафикті тексеру мүмкіндігі бар орнаған желі қосылыстарын тұрақты түрде бақылау функциясы қарастырылуы тиіс.
  13. Жүйеде Интернет ресурстарын санаттары бойынша құлыптау, сондай-ақ Ақ/Қара тізімдер режимінде жұмыс істеу мүмкіндігі бар веб-сүзгі болуы тиіс.
  14. Жүйе бір уақытта бірнеше тексеру процесін жасау мүмкіндігін қолдауы тиіс.
  15. Жүйенің бағдарламалық құралдары келесі функционалдық мүмкіндіктердің орындалуын қамтамасыз етуі керек:
      1. түрі белгілі барлық вирустарды тауып жою;
      2. қауіп-қатердің болуын толық немесе таңдап тексеруге негізделген және әкімшінің пәрмені бойынша не кесте бойынша жасалатын антивирустық сканерлеу;
      3. Серверге жүктелетін не одан шығатын файлдарды «жолдан ұстап» орындалатын антивирустық тексеру;
      4. Операциялық жүйе жүктелген кезде антивирустық бағдарламалық құралдың және басқа да қажеті компоненттердің автоматты түрде бірге іске қосылуы;
      5. тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу;
      6. іске қосу параметрлері көрсетілген сканерлеу кестесін баптау.
  16. Бағдарлама веб-интерфейс арқылы да, тікелей конфигурациялық файлдар арқылы да басқарылуы тиіс. Антивирустық тексеріс жүргізілуі тиіс файлдар мен каталогтарды, сондай-ақ әртүрлі зиянкес нысандарға қатысты қолданылатын әрекеттерді көрсетуге болатын антивирустық сканерлеу параметрлерін баптау мүмкіндігі.
  17. Сканерлеуші ядро файлдардағы және диск құрылғыларының жүктеу жазбаларынан MBR - Master Boot Record, VBR - Volume Boot Record) вирустарды және басқа да зиянкес нысандарды іздеуді қамтамасыз етуі тиіс.
  18. Файлдарды тексеру үшін лектік тексеру әдісін (flow), сондай-ақ проксилеу әдісін (proxy) қолдану мүмкіндігі.
  19. Желі арқылы алынған файл түрінде көрсетілмеген деректерді тексеру, сондай-ақ файлдарда қауіп-қатердің болуын бөліп тексеруді ұйымдастыру мүмкіндігі.
  20. Басқару веб-интерфейсіне кіруге болатын жергілікті құрылғыдағы файлдарда қауіп-қатердің болуын шұғыл тексеру мүмкіндігі.
  21. Жойылған желі тораптарында тұрған файлдарда қауіп-қатердің болуын тексеру мүмкіндігі. Осындай тораптар ретінде жұмыс станцияларымен және серверлермен қатар, роутерлер, ТД-тіркемелер және Secure Shell немесе Telnet кіру рұқсатын беретін «Интернет заттарды» құрайтын өзге де «ақылды» құрылғылар бола алады.
  22. Жүйе құрамында мониторинг жүйелерімен (Munin, Nagios, Zabbix) біріктіруге арналған SNMP-агент болуы тиіс.
  23. Антивирус қорғанысын орталықтан басқаратын жүйеге біріктіру жүйе әкімшісіне барынша қолайлы болатын антивирус қорғанысы жүйесін «бір жерден» басқаруға мүмкіндік береді.

1. **Android операциялық жүйесімен жұмыс істейтін мобильді құрылғыларға арналған антивирустық қорғаныс бағдарламалық құралына қойылатын талаптар**
   1. Смартфондарға арналған антивирустық қорғаныс бағдарламасы: Android 4.0 және одан жоғары нұсқалармен жұмыс істеуі қажет.
   2. Қолданылатын бағдарламалық құрал қамтамасыз етуі тиіс:
      1. файлдық жүйені үздіксіз қорғау, қармау және тексеру:

* GPRS/IR порты/Bluetooth/Wi-Fi/USB қосылымдары арқылы (соның ішінде поштамен жұмыс істеу кезінде және файлдарды браузер арқылы жүктеп алу кезінде) немесе компьютермен синхрондау кезінде алынған файлдар;
* APK, ZIP, SIS, CAB, RAR, JAR архивтеріндегі файлдарды тексеру;
* смартфон интерфейсінен орнатылған бағдарламаларды тексеру.
* смартфонда немесе қосылған жад кеңейту карталарында орналасқан файлдық жүйе объектілерін пайдаланушының өтініші бойынша және кестеге сәйкес толық және таңдамалы сканерлеу;
  + 1. алдын ала анықталған және пайдаланушы жасаған қауіпсіздік профильдері негізінде кіріс қоңыраулар мен SMS хабарламаларды (жарнамалық хабарламаларды, сондай-ақ белгісіз нөмірлерден келетін қоңыраулар мен хабарламаларды қоса) сүзгілеу, олардың әрқайсысы үшін нөмірлер тізімін жасауға және қоңыраулар мен хабарламалар үшін әрекетті анықтауға болады. Арнайы жасалған қара тізімдерді, сондай-ақ құрылғының телефон кітапшасын сүзу үшін пайдалану;
    2. бұғатталған қоңыраулар мен хабарларға арналған әрекеттерді көру және таңдау;
    3. автоматты іске қосылу файлдарын анықтау;
    4. карантиндік қоймадағы жұқтырған объектілерді жою немесе оқшаулау. Қауіптердің түрлері туралы толық ақпарат алу;
    5. жаңартуды өткізу:
* Кірістірілген GPRS модулін пайдалану арқылы HTTP хаттамасы бойынша;
* Infrared/Bluetooth/Wi-Fi/USB-қосылымы арқылы;
* зиянды бағдарламаларды сканерлеу және қауіпті нысандарды жою үшін пайдаланылатын вирусқа қарсы дерекқорлардың ActiveSync қосылымы арқылы компьютерді Интернетке кіру мүмкіндігімен синхрондау арқылы;
  + 1. мобильді құрылғыларды пайдаланатын ұжымдық саясат негізінде орталықтандырылған басқару;
    2. мобильді құрылғыны виджет негізінде басқару;
    3. Баптаулардан арылту, импорттау және экспорттау;
    4. жоғалған немесе ұрланған жағдайда мобильді құрылғыны қашықтан басқару, соның ішінде іздеу, құрылғыны апаттық блоктау, жеке деректерді жою, координаттарды алу, алдын ала анықталған құрылғылардан немесе кез келген құрылғыдан SMS пәрмендерін жіберу кезінде пайдаланушы орнатқан құпиясөз арқылы құрылғыны басқару;
    5. Android үшін VPN технологиясына негізделген желіаралық қалқан;
    6. қосымшаларды сүзу;
    7. төлем бағдарламарынан, құрылғыларды блоктаушы қолданбалардан қорғау;
    8. кірістірілген Android браузері, сондай-ақ Google Chrome, Google Chrome Beta, Firefox, Opera, Opera mini, Next, Amazon Silk, Yandex Browser, Yandex Browser Light, Boat Browser және Boat браузерлері арқылы интернеттегі ресурстарға қол жеткізуді бақылау Mini Browser, Adblock Browser, Dolphin Browser, Satellite, UME Browser, Microsoft Edge;
    9. құрылғы қауіпсіздігінің диагностикасы және келесі қауіпсіздік мәселелерін анықтау мүмкіндігі бар арнайы құрамдастың көмегімен анықталған ақаулар мен осалдықтарды жою бойынша ұсыныстар:
* осалдықтар, мысалы: BlueBorne, EvilParcel, Extra Field, Fake ID, Janus, ObjectInputStream Serialization, OpenSSLX509Certificate, PendingIntent, SIM Toolkit, Stagefright және Stagefright 2.0;
* жүйе параметрлері;
* қайшылықты бағдарламалық құрал;
* жасырын құрылғы әкімшілері;
* Fake ID осалдығын пайдаланатын қолданбалар.

1. **Антивирус қорғанысын басқару жүйесіне қойылатын талаптар**
   1. Жүйе тек серверлерде ғана емес, сонымен қатар келесі операциялық жүйелерде жұмыс істейтін жұмыс станцияларында орталықтандырылған антивирустық серверді орнату мүмкіндігімен клиент-сервер архитектурасына құрылуы керек:

* Microsoft Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11;
* Microsoft Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016 / Windows Server 2019 / Windows Server 2022;
* Linux, егер glibc 2.13 немесе одан кейінгі нұсқасы болса;
* FreeBSD 11.3 немесе одан кейінгі нұсқасы.
  1. Бұл ретте орталықтандырылған басқару сервері операциялық жүйелеріне қарамастан, барлық қорғалатын нысандар үшін бірдей болуы керек: Windows/Linux/macOS/Android.
  2. Басқару жүйесі Windows® Internet Explorer®, Microsoft Edge®, Mozilla® Firefox®, Google Chrome®, Opera®, Safari® (соның ішінде Microsoft Windows, Linux, FreeBSD ОЖ) браузерлері қолданылатын кез келген операциялық жүйеден қолдану үшін қолжетімді болуы керек әрі браузерлердің соңғы нұсқаларын пайдалану мүмкіндігі шектелмеген және басқару сервері жақтан да, Жүйе әкімшісі жақтан да қандай да бір бағдарламалық құралды қосымша орнату қажет болмауы шарт.
  3. Әкімшілердің аутентификациясы келесі тәсілдермен орындалуы тиіс:
* Сервердің дерекқорынан;
* LDAP/AD пайдалану арқылы;
* RADIUS пайдалану арқылы;
* PAM пайдалану арқылы.
  1. Лицензияларды сервис аралық байланыстар арқылы тарату мүмкіндігі бар басты, бағыныңқы және тең құқықты басқару серверлерінің иерархиялық жүйесін құру мүмкіндігі, сондай-ақ лицензиялық негізгі файлды автоматты түрде жаңарту мүмкіндігі қарастырылған болуы тиіс.
  2. Басқару жүйесінің төмендегідей мүмкіндігі болуы керек:
* бірнеше серверден алынған ақпаратты бір серверге біріктіру;
* желіге түсетін жалпы жүктемені азайту мақсатында жаңартуларды алу үшін жұмыс станцияларын серверлерге бөліп тарату;
* нұсқалары әртүрлі антивирус серверлері арасында бір иерархиялық желі шеңберіндегі статистикамен алмасу;
* әкімшілер мен пайдаланушылардың рөлдерін, сондай-ақ әр деңгейде берілетін есеп түрлерін баптауға болатын көп деңгейлі басқару жүйесін құру.
  1. iOS және Android операциялық жүйелерінде веб-браузерді пайдаланбай Жүйені мобильді басқару орталығын іске қосу мүмкіндігі қарастырылған болуы керек.
  2. Басқару жүйесінің төмендегідей мүмкіндігі болуы керек:
     1. сыртқы және ішкі ДҚБЖ (антивирус серверінің дистрибутивімен бірге жеткізіледі) пайдалану. Oracle, PostgreSQL, Postgres Pro, кез келген ДҚБЖ MS Windows және Linux операциялық жүйелеріне арналған ODBC драйвері арқылы сыртқы ДҚБЖ бола алады;
     2. Сервер бөлігін орнатқаннан кейін жұмыс барысында пайдаланылатын ДҚБЖ түрін алмастыру, бұл кезде Жүйенің сервер бөлігін қайта орнату қажет болмауы керек.
     3. басқару жүйесінің құралдарының дерекқорын басқаруы, соның ішінде дерекқорын тазарту, оны талдау мүмкіндігі, еркін түрде SQL-сұрау жасау;
     4. кірістірілген Web API арқылы сыртқы жүйе тармақтарымен біріктірілген жағдайда осы Web API функцияларының көмегімен әрекеттер аудитін жүргізу мүмкіндігі болуы шарт;
     5. оқиғалар өңдеушісінің Lua тілінде өз бетінше жазу, сондай-ақ басқару жүйесінің құралдары көмегімен еркін Lua-скрипттерді жасау;
     6. есептерді CSV, XML, HTML және PDF форматтарына экспорттау;
     7. басқару орталығының консолінде жүйе әзірлеушісінен өзекті қауіп-қатер туралы ақпарат беретін жаңалықтарды алу және сондай жаңалықтарға жазылу;
     8. қолданушы мен әкімшіге пошта хабарын, дауыстық хабарлама жолдау, қалқыма терезе шығару, оқиғалар журналына жазу, оповещения в веб-консоли, Push-оповещения, SNMP- протоколы, Syslog-протоколы RFC 5424 немесе CEF арқылы хабар жеткізу жолдарының көп болуы;
     9. хабарлама мәтіні, интернет-ресурстардың сілтемелері, кез келген графикалық суреті бар мазмұны еркін ақпараттық хабарламаны Жүйенің Web-интерфейсінен шынайы уақыт режимінде желі арқылы жолдау;
     10. агенттерді орнату және жаңарту кезінде желі трафигін шектеу;
     11. Android, macOS және UNIX тобының операциялық жүйесіне арналған антивирус агенттерін қосу баптаулары бар конфигурациялық файлдарды жүктеп алу;
     12. барлық қорғалатын нысандардағы, соның ішінде мобильді және off-line режимінде тұрған антивирус базаларын орталықтан жаңарту. Жаңартуларды нысандарға кесте бойынша алғаннан кейін бірден жеткізу;
     13. антивирус серверінің репозиториінде тұрған өнімдердің жаңартуларының ревизиясын, соның ішінде жаңартуларды кейін шегертуді басқару;
     14. топтық жаңартулар мүмкіндігінің болуы;
     15. SSL-сертификаттарды пайдаланатын қорғалған арна арқылы жаңарту;
     16. кейінге қалдырылған жаңартуды ұйымдастыру;
     17. орнатылған бағдарламалық құралдың жаңа нұсқаларға автоматты түрде көшуі, соның ішінде ж ртылатын компоненттерді таңдау мүмкіндігімен көшуі;
     18. орнатылатын компоненттерді клиент бөліктеріне антивирус топтамасын орнатқанға дейін таңдау;
     19. әкімшінің және қолданушының толық құжат топтамасын басқару орталығының консолінен тікелей оқу.
  3. Жүйе мобильді пайдаланушылар (ноутбуктер) үшін арнайы саясаты болуы керек , оны қолданған кезде мобильді пайдаланушылар антивирустық серверге қол жетімділік болмаған кезде антивирустық пакеттің параметрлерін редакциялауға және интернет арқылы жаңартуға қабілетті болуы керек. Саясатты қолдану \*.xml типті конфигурация файлдарын пайдалануды қажет етпестен Web-интерфейсі арқылы жүзеге асырылуы тиіс.
  4. Басқару жүйесінде маңызды деректерді автоматты түрде көшіру және алдын-ала белгіленген кесте бойынша антивирустық сервердің конфигурациясы, сондай-ақ серверді сақтық көшірмеден қалпына келтіру мүмкіндігі болуы керек.
  5. Басқару жүйесінде Active Directory-дағы NetBIOS, ICMP, TCP арқылы іздеу режимінде жұмыс станцияларының және антивирус агентінің болуын анықтау мақсатында желіні сканерлеуге мүмкіндік беретін компонент болуы керек.
  6. орталығында алдын ала орнатылған жүйелік және қолданушылық топтар негізіндегі топтық саясат жасалған болуы тиіс,. Алдын ала орнатылған жүйелік топтар барлық қорғалатын нысандарға Active Directory нысандары, операциялық жүйелер, саясаттар, баптау профильдері, желі протоколдары, нысан мәртебесі, дербес баптаулар арқылы жүгінуге мүмкіндік беруі тиіс.
  7. Басқару жүйесі қолданбалардың іске қосылуын тыйым салушы және рұқсат беруші ережелер негізінде әрі қолданбалардың функционалдық талдауы негізінде: қолданбаларды іске қосу, модульдерді жүктеу және орындау, скрипт түсіндірушілерін іске қосу, драйверлерді жүктеу, MSI-топтаманы орнату, орындалатын файлдардың толықтығы сияқты топтар бойынша бақылай алуы тиіс.
  8. Орталықтандырылған басқару сервері арқылы, антивирустық бағдарламалық құрал мониторингі бойынша есеп беру.
  9. Антивирустық қорғау жүйесінің жай-күйі туралы есептерді құру және оларды біріктіру арқылы статистикалық ақпаратты орталықтандырып жинау, одан әрі, кейіннен әкімшіге электрондық пошта арқылы жібере отырып, көрсетілген параметрлер бойынша статистикалық есептерді автоматты түрде жасау мүмкіндігі.
  10. Жүйеде лицензиялық кілттердің иерархиялық тізімін жүргізетін лицензиялар менеджері іске асырылуы керек. Лицензиялар менеджері келесі мүмкіндіктерді қамтамасыз етуі керек: лицензия туралы ақпаратты қарау, жаңа лицензиялық кілтті қосу, лицензиялық кілтті жаңарту, лицензиялық кілтті ауыстыру, нысанның лицензиялық кілттерінің тізімін кеңейту, лицензиялық кілтті жою және лицензиялау тізімінен нысанды жою, лицензияларды көрші басқару серверіне тасымалдау, көрші басқару серверіне тасымалданатын лицензияларды өңдеу.
  11. Жүйе құпия ақпараттың ағып кетуіне жол бермеу үшін серверлер мен қорғалған станциялар арасындағы трафикті шифрлай алуы керек.
  12. Жүйе өндірушісі вирус базаларының жаңартуларын тәулігіне кемінде 20 рет шығарғанда, ол Жүйе жасаған есепте расталуы тиіс;
  13. Антивирус серверлері орналастырылған жағдайда, Интернет желісі қолжетімді емес ішкі желіде репозиториді автономды түрде жүктейтін арнайы утилита көмегімен жаңартуларды алу мүмкіндігі болуы керек.
  14. Виртуалды инфрақұрылымды қолдау, виртуалды жұмыс орындары инфрақұрылымымен (VDI) біріктіру, VMware, Microsoft Hyper-V, Xen, KVM (Kernel-based Virtual Machine) гипервизорларын қолдау.