**№2 Қосымша**

**шартқа № \_\_\_**

**бастап "\_\_\_\_" \_\_\_\_\_\_\_\_\_ 202\_қ.**

**Техникалық ерекшелік**

Осы техникалық ерекшелік сатып алуға құрастырылды желіаралық экранның.

1. **Жалпы талаптар**

Жеткізуші жеткізуді жүзеге асыруы керек тауардың, қашықтан орнатумен желіаралық экрандардың.

1. **Жеткізу көлемі келесі компоненттерді қамтуы керек:**

|  |  |
| --- | --- |
| **Атауы** | **К-ша дана** |
| Желіаралық экран (Checkpoint 1595) (CPAP-SG1595-SNBT-SS-PREM-1Y 1595 appliance.) | 2 |

1. **Желіаралық қалқанға қойылатын талаптар.** 
   1. Қауіпсіздік шлюзі желі ағынын қадағалау және басқару үшін егжей-тегжейлі байланыс талдауы мен қолданба күйіне негізделген қосылым күйін бақылауды пайдалануы керек.
   2. Шешім қолдау көрсетуі керек DHCP, сервер және relay.
   3. Шешім режимде жұмыс істеу мүмкіндігін қамтуы керек Transparent/Bridge.
      1. Шешім OSI үлгісінің (режим) 2-деңгейіндегі жұмысты қолдауы керек bridge).
      2. Шешім брандмауэрді, IPS, URL сүзгісін қолдауы керек, Antibot, Antivirus, Басқарма қосымшаларымен, Identity Awareness
      3. Шешім кластерлеуді қолдауы керек Active/Standby режимде bridge.
   4. Шешім мыналарға негізделген саясатты қолдауы керек QoS.
      1. Шешім өткізу қабілеттілігіне кепілдік беруге немесе шектеуге және белгілі бір уақытқа кідірісті басқаруға мүмкіндік беруі керек IP дереккөзден, IP межелі орынның немесе сервистің.
      2. Шешім ережелерді өз бетінше қолдану мүмкіндігіне ие болуы керек QoS үшін VPN трафик.
   5. Шешім функционалдылықты қамтамасыз етуі керек IPS (интрузияның алдын алу жүйелері).
      1. Жүйе IPS келесі анықтау механизмдеріне негізделуі керек: қолтаңбаларды пайдалану, хаттамалардың ауытқуларын қадағалау, қолданбаларды басқару және мінез-құлыққа негізделген анықтау.
   6. Шешім пайдаланушыларды сәйкестендіру функционалын қамтамасыз етуі тиіс.
      1. Сұрау салу арқылы пайдаланушы идентификаторларын жинауға қабілетті болуы керек Microsoft Active Directory қауіпсіздік оқиғалары негізінде.
      2. Браузерге негізделген пайдаланушы идентификаторын аутентификациялау әдісі болуы керек домендік емес пайдаланушылардың немесе компьютерлердің.
      3. Пайдаланушылардың компьютерлерінде саясат бойынша орнатылатын және жеке куәліктерді жинап, қауіпсіздік шлюзіне жібере алатын арнайы агент болуы керек.
   7. Шешім қосымшаларды басқарудың функционалдығын қамтамасыз етуі керек және URL-сүзгілеу.
      1. Қолданбаларды басқару дерекқорында 10 000-нан астам белгілі қолданбалар болуы керек.
      2. Шешім кем дегенде 250 000 үшін қауіпсіздікті егжей-тегжейлі бақылауды қамтамасыз етуі керек Web 2.0 виджеттер.
      3. Шешім міндетті түрде қамтамасыз ету URL санаттауды, оның ішінде 200 миллионнан астам URL.
   8. Шешім Anti функционалын қамтамасыз етуі тиіс-Bot және Anti-Virus.
      1. Қосымша Anti-bot күдікті әдеттен тыс желілік әрекеттерді анықтауға және тоқтатуға қабілетті болуы керек.
      2. Қосымша Anti-Bot беделді қамтитын көп деңгейлі анықтау механизмін қолдануы керек IP, URL және DNS мекенжайлар және байланыс протоколының үлгілері арқылы боттарды анықтау.
      3. Қосымша Anti-virus зиянды веб-сайттарға кіруге жол бермеуі және кіретін зиянды файлдарды тоқтатуы керек.
      4. Қосымша Anti-virus қабілетті болуы керек шифрланғанын тексеру SSL трафик.
   9. Шешім "құм жәшігінің" функционалдығын қамтамасыз етуі керек Sandboxing (тексеру – бұлтта немесе арнайы жергілікті құрылғыда).
      1. "Құм жәшігінің" функционалдығы келесілерден қорғауды қамтамасыз етуі керек нөлдік күндік шабуылдар.
      2. Құм жәшігін енгізу топологиясы:
         * Желілік құмсалғыш режимін қолдау (network based);
         * Режимді қолдау ішкі (bridge mode);
         * Пошта агенті режимін қолдау (mail transfer agent).
         * Айна порты режимін қолдау (TAP/SPAN порты).
      3. Шешім орындалатын файлдарды, мұрағаттарды, құжаттарды, соның ішінде Java және эмуляциялауы керек flash.
      4. Эмуляция қозғалтқышы керек әртүрлі операциялық жүйелерді, мысалы, XP және Windows 7 жүйелерін, соның ішінде арнайы конфигурацияланған кескіндерді (customized images).
      5. Эмуляция қозғалтқышы керек тексеруге, еліктеу, алдын алу және беру оқиғалар жылы инфрақұрылымға қорғау зиянды БҚ-дан.
      6. Шешім тиіс қамтамасыз ету эмуляцияға файлдарды қалай шағын өлшем, солай және өлшемімен жоғарыдан 10Mбайт.
      7. Шешім орындалу сатысындағы шабуылдарды анықтауы керек экслойта (exploitation) – б. қабық коды іске қосылғанға дейін (shell code) және жүзеге асырылады жүктелуде/орындалуы өзінің кодтың зиянды бағдарламалық қамтамасыз ету.
      8. Шешім тиіс анықтау ROP (return oriented programming) және басқалар техникалар пайдалануларды (ал том оның ішінде эскалацияға артықшылықтар – privilege exploitation) орталық процессордың нұсқауларының орындалу реттілігін бақылау арқылы.
      9. Шешім нөлдік күндік (0-day) шабуылдардан қорғау үшін пошта хабарлары ішіндегі сілтемелерді сканерлеуді қамтамасыз етуі керек attacks), сондай-ақ белгісіз зиянды бағдарламадан.
      10. Шешімде құм жәшігіндегі өнімділікті анықтау әдістерімен күресу құралдары болуы керек.
      11. Шешім оны орталықтандырылған басқарудан басқару мүмкіндігін қамтамасыз етуі керек.
      12. Шешім әрбір вирус жұққан файлды талдау нәтижелері туралы егжей-тегжейлі есеп жасауы керек.
   10. Шешім IPSEC VPN функционалдығын қамтамасыз етуі керек.
   11. Ішкі қолдау болуы керек CA (Certificate Authority), сондай-ақ сыртқы бөгде CA.
   12. Шешім 3-ті қолдауы керекDES және AES-256 үшін шифрлау IKE фазалар I және II IKEv2, сондай-ақ "Suite-B-GCM-128" және "Suite-B-GCM-256" фаза үшін II.
       1. Шешім кем дегенде келесі топтарды қолдауы керек Diffie-Hellman: 1-топ (768 бит), 2-топ (1024 бит), 5-топ (1536 бит), 14-топ (2048 бит), 19-топ және 20-топ
       2. Шешім деректердің тұтастығын құралдармен қамтамасыз етуді қолдауы керек md5, sha1 SHA-256, SHA-384 және AES-XCBC
   13. Шешім қолдауды қамтуы керек үшін VPN типті site-to-site келесі топологияларда:
       1. Толық байланысқан желі (барлығы-барлығымен бірге),
       2. Жұлдыз тәрізді желі (қашықтағы кеңселер к орталық сайтқа)
       3. Желдеткіш желісі (орталық сайт арқылы басқа қашықтағы сайтқа қашықтағы сайт)
   14. Қашықтан мобильді қолжетімділік
       1. Шешім пайдаланушылардың бір мезгілде кемінде 200 қосылымы үшін қашықтан мобильді қолжетімділік функционалын қамтамасыз етуі тиіс.
       2. Шешім функционалдылықты қамтамасыз етуі керек SSL VPN корпоративтік ресурстарға қосылу үшін сұраныс бойынша 3-деңгей. Шешім кез келгенін қолдауы керек IP-қосымшаны қоса алғанда ICMP, TCP және UDP, әрбір қолданбаны қолдау үшін күрделі конфигурацияны қажет етпей. Ол қашықтағы компьютерлерде әкімші артықшылықтарын қажет етпей жұмыс істеуі керек.
       3. Шешім екі факторлы аутентификация шешімдерімен интеграцияны қолдауы керек.
       4. Шешім веб -қосымшаларда берілетін зиянды кодтан енудің алдын алу үшін интеграцияланған жүйенің функционалдығын енгізуі тиіс. Шешім құрттарды, буфердің толып кетуі, SQL және командалық инъекциялар, сайттар аралық сияқты әртүрлі шабуылдарды блоктауға қабілетті болуы керек скриптинг, реттелетін HTTP құрттарын блоктау модулі, каталогты айналып өтуден қорғау (directory traversal), қорғауды тақырыптардың ауытқуы (header rejection),қорғауды бастап зиянды HTTP-кодтың.
   15. Шлюзге қойылатын аппараттық және жұмыс талаптары.
       1. Өнімді желілік интерфейстер (ең төменгішы талаптар):
          1. 1х1 Гбит / с/с мысші WAN порт
          2. 1х1 Гбит / с/с балных/оптикалық DMZ порт
          3. 8x1 Гбит мыс LAN порттардың
          4. арналған 1 слот SD карталар
          5. 1 консольдық порт
          6. 1 USB порт
   16. Брандмауэрдің өткізу қабілеттілігі: минимум 2.8 Гбит/с.
   17. IPS өткізу қабілеттілігі: минимум 1.4 Гбит/с.
   18. NGFW өткізу қабілеттілігі (брандмауэр, қолданбаларды басқару және IPS функционалдығы белсендірілген): кемінде 1300 Мбит/с.
   19. Өткізу қабілеті Threat Prevention (Firewall функционалы, Application Control, URL белсендірілген Filtering, IPS, Antivirus, Anti-Bot және бұлтты Sandbox): кем дегенде 660 Мбит/с.
   20. Бір мезгілде қосылулар: минимум 1 000 000.
   21. Жаңа қосылымдар: секундына кемінде 21 000.
   22. Қолдау және жазылу.
       1. Өндірушіден 1 жылдық қолдау және жазылым, 24x7, жабдықты кепілдікпен ауыстыру, қауіпсіздік қызметтеріне барлық қажетті жазылымдарды қосу керек.
2. **Жеткізушіге қойылатын талаптар**
   1. Жеткізуден кейін тауардың желіаралық қалқандарды қашықтықтан баптауды жүргізу арналған іс жүзіндем серверде басқарманың Checkpoint SmartConsole, тапсырыс берушімен бірлесіп.
3. **Жеткізу орны мен шарттары:**

Жеткізу шарттары DDP Ақтөбе қ., даңғ. Әбілқайыр хан 10.