Дәріс 15
Тақырыбы. Қауіпсіздік және жан-жақты интернет
Дәріс жоспары:
Қауіпсіздік стратегиясы
Қауіпсіздік архитектурасы
Қауіпсіздік құрылғылары
Қосымшаларға бағытталған қауіпсіздік

Қауіпсіздік стратегиясы

Интернетті қамтитын шешімнің мөлшері мен интеграциясы неғұрлым үлкен болса, желі орталықтандырылмаған болады. Бұл желіге көбірек кіру нүктелерін ұсынады, бұл көптеген осалдықтарды білдіреді. Бір-біріне толық Интернетке қосылған көптеген құрылғылар қорғалмаған жерлерден деректер алмасады, бірақ бұл процесс қорғалуы керек. Алайда, сенсорлардың, ақылды объектілердің және желіге қосылған құрылғылардың көптігіне байланысты, толық интернетті шешудің қауіпсіздігін қамтамасыз ету оңай емес. Қауіпсіздік мамандары үшін негізгі проблема-қорғалмаған құрылғылар үшін ұйым желісіне қол жетімділікті қамтамасыз етумен байланысты ықтимал қауіптер.

Ұйым немесе жеке пайдаланушы өзін және өз желісін қауіп төндірмей, толық Интернеттің артықшылықтарын қалай пайдалануға болады. Толық ақпарат төменде суреттерде келтірілген.

15.1 - сурет

Қазіргі уақытта қауіптердің алдын алу тактикасы желілік қауіпсіздік жүйесінің негізгі стратегиясы болып табылады. Дәрігерлер науқастың қазіргі диагнозымен күресу арқылы жаңа аурулардың алдын алуға тырысқандай, желілік қауіпсіздік мамандары ықтимал қауіптердің алдын алуға тырысады, бұл сәтті шабуылдардың салдарын азайтады.

Жан-жақты интернет аясында қауіпсіздік жүйесі барлық жерде болуы керек. Қауіпсіздікті қамтамасыз ету тәсілі болуы тиіс:

* дәйекті және автоматтандырылған, сондай-ақ басқа ұйымдардың қорғалған шекараларына қол жеткізу
* нақты уақыттағы алдын-ала талдау арқылы қауіпсіздік қатерлерін тану үшін динамикалық
* барлық қосылымдар мен инфрақұрылым элементтерін толық бақылауды қамтамасыз ету үшін зияткерлік
* өсіп келе жатқан ұйымның қажеттіліктерін қанағаттандыру үшін масштабталады
* адаптивті және нақты уақыттағы қауіп-қатерлерге жауап бере алады
* кешенді, толыққанды шешім

Кең таралған қауіпсіздік жүйесін шешу басқару қиын және үлкен мемлекет пен кең техникалық білімді қажет ететін оқшауланған қорғаныс құралдарын болдырмауға мүмкіндік береді.

Қауіпсіздік архитектурасы

Жан-жақты интернет желілерінің қауіпсіздігін қамтамасыз ету кезінде сіз тек жеке құрылғыларды қорғаумен шектеле алмайсыз. Мұнда Қауіпсіздіктің кешенді шешімін жүзеге асыру маңызды.

Бүкіл желі бойынша саясатты орталықтандырылған басқарумен және оларды үлестірумен қорғауды қамтамасыз ететін қауіпсіздік шешімі өрістетілуі тиіс. Қосылған Орта бойынша деректерді жинау және салыстыру үшін алынған мәліметтерді кейіннен пайдалана отырып және қажетті шараларды қолдана отырып, желідегі қызметтің үздіксіз мониторингі қажет.

Қауіпсіздік архитектурасының құралдары мен жүйелерінің жиынтығын қамтамасыз ету үшін Cisco Инфрақұрылым деңгейлерін, платформалар мен қосымшаларды пайдаланады. Бұл құралдар мен жүйелер нақты уақыт режимінде қауіпсіздікті қамтамасыз етуде қолданылатын ақпаратты алу үшін бірлесіп жұмыс істейді. Сонымен қатар, желі өздігінен де, қызметкерлердің елеусіз араласуымен де қауіпсіздікке төнетін қатерлерге жауап ретінде әрекет ете алады және қайта құрылуы мүмкін. Қауіпсіздік архитектурасының қағидаттары бойынша толық мәліметтер:

* Кіруді бақылау пайдаланушыларға немесе құрылғыларға белгіленген саясатқа сәйкес бөлінген желіге қол жеткізуді қамтамасыз етеді. Пайдаланушылар аутентификациядан және авторизациядан өтеді. Соңғы құрылғылар қауіпсіздік саясатының талаптарын орындайтындығын анықтау үшін де талданады. Принтерлер, бейнекамералар, датчиктер және контроллерлер сияқты аутентификацияланбайтын құрылғылар да автоматты түрде сәйкестендіріліп, түгендеуден өтеді.

* Контекстке негізделген саясат. Мәнмәтінді ескере отырып, саясатта жеңілдетілген сипаттамалық-іскерлік тіл жағдайдың толық мәнмәтініне негізделген қауіпсіздік ережелерімен анықталған: кім және қандай ақпарат, қашан, қайда және қалай анықтайды. Бұл қауіпсіздік саясаты бизнес-саясаткерлерге қатаң бағынады, сондықтан олардың бүкіл ұйымда сақталуын бақылау қиын емес. Олар ұйымдарға тиімді қорғауды және нормативтік талаптарға сәйкестікті қамтамасыз етуге, сондай-ақ жұмыс тиімділігі мен желіге кіруді бақылау деңгейін арттыруға көмектеседі.

* Мәтінмәндік саясатты тексеру және қолдану желі бойынша саясатты сақтау туралы шешім қабылдау үшін желілік және ғаламдық ақпаратты пайдаланады. Интеграцияланған қауіпсіздік қызметтері, автономды құрылғылар немесе бұлтты қауіпсіздік қызметтері сияқты икемді орналастыру опциялары әр пайдаланушыға қорғаныс құралдарын ұсынады.

* Желілік және ғаламдық ақпараттық жүйе зиянды белсенділігімен танымал медиа туралы ақпаратты беру үшін ғаламдық деректер байланысын пайдаланады. Бұл жүйе жылдам және мінсіз қорғауды және саясатты сақтауды қамтамасыз ету үшін желінің белсенділігі мен қауіптері туралы егжей-тегжейлі ақпарат береді.

Суретте Cisco қауіпсіздік архитектурасы көрсетілген. 1-суретте сипатталған қауіпсіздік принциптері архитектураның барлық деңгейлерінде қолданылады. Архитектураның төменгі бөлігінде қолданбалы бағдарламалау интерфейстерінің (API) жиынтығын қамтамасыз ететін инфрақұрылым деңгейі орналасқан. Бұл интерфейстер жоғарыда орналасқан қауіпсіздік платформасының деңгейіне белгілі бір мүмкіндіктер мен қосымшаларды ұсынады. Платформаның жоғарғы жағында бүкіл платформаны басқаратын жалпы қауіпсіздік және басқару саясаты бар.

15.2 - сурет

Cisco қауіпсіздік архитектурасын іске асыру суретте көрсетілген артықшылықтарды, сондай-ақ қауіпсіздік оқиғаларына немесе шабуылдарға дейін, кезінде және одан кейін үздіксіз қолдауды ұсынады.

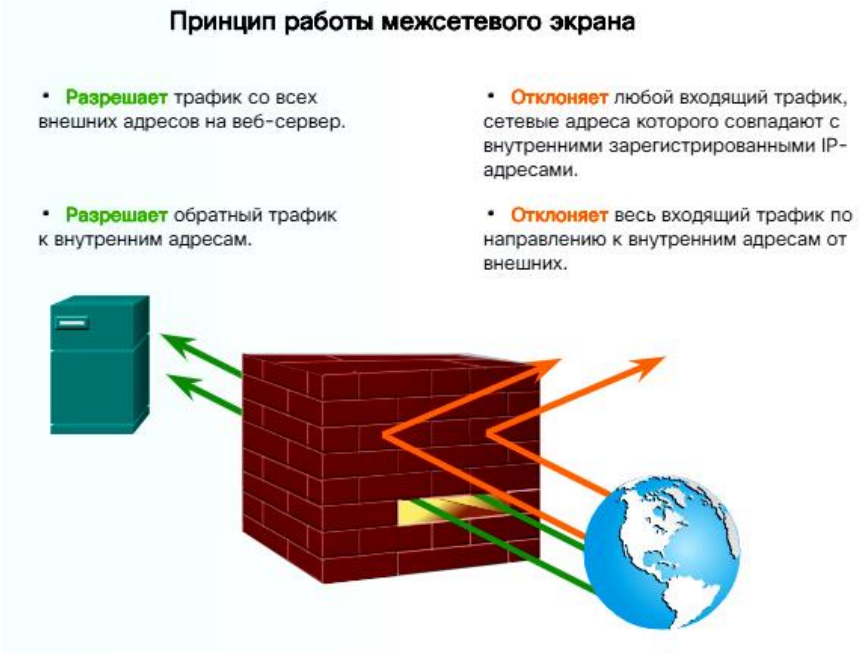
15.3 - сурет

Кешенді интернет нарығында Cisco корпорациясы ерекше орынға ие. Қауіпсіздік саласындағы ізашар бола отырып, Cisco корпорациясы кешенді шешімдері бар өнімдер желісін ұсынады.

Қауіпсіздік құрылғылары

Кіруді бақылау, мазмұнды тексеру және саясатты сақтау үшін пайдалануға болатын қауіпсіздік архитектурасының құрылғыларына мыналар жатады.

* Желіаралық экрандар - екі желі арасында кедергі жасайды. Онда бағдарламаланған ережелерге сүйене отырып, желі аралық экран екі желі арасында беруге болатындығын анықтау үшін желілік трафикті талдайды.



15.4 - сурет

* Басып кіруді болдырмау жүйелері (IPS) — желідегі әрекеттерді бақылайды және олардың зиянды екенін анықтайды. IPS трафикті зиянды құрылғыдан ауытқу немесе қосылысты үзу арқылы шабуылдың алдын алуға тырысамыз

15.5 - сурет

Қосымшаларға бағытталған қауіпсіздік

Ұйымдар қосымшаларға бағытталған ортаға ауысқан кезде, дәстүрлі қауіпсіздік шешімдері өзектілігін жоғалтады. Cisco ASA қауіпсіздік шешімдері белгілі бір қосымшаны қорғау үшін реттелген қауіпсіздік технологияларын толық интеграциялау арқылы қоршаған ортаны қорғайды. ACI қауіпсіздік шешімдерін орталық контроллердің көмегімен қосымшалар мен операцияларға қосылған ресурстар пулымен басқаруға болады. Бұл шешім сұраныс бойынша автоматты түрде масштабталуы мүмкін, бұл саясат негізінде қауіпсіздіктің тұтас жүйесін қамтамасыз етеді.

Шешім шығындарды азайтатын және қорғаныс процедурасын жеңілдететін саясатқа негізделген қауіпсіздікті қамтамасыз етудің бірыңғай тәсілін ұсынады. Сондай-ақ, ол физикалық және виртуалды қауіпсіздік технологияларын бұлт инфрақұрылымына және деректер орталығына тікелей біріктіреді.

СымсызқауіпсіздікСымсыз желінің қауіпсіздігін қамтамасыз ету сымды желіні қорғаудан да қиын. Кіру нүктесінің ауқымында сымсыз желі тиісті тіркелгі деректері бар барлық адамдар үшін ашық.

Сымсыз желілердің қауіпсіздік жүйесі көбінесе кіру нүктесінде немесе желіге сымсыз қосылу жүзеге асырылатын жерде жүзеге асырылады. Сымсыз желілердің негізгі қауіпсіздік жүйесі келесі параметрлерді қамтиды.

* Тұрақты парольдермен сенімді аутентификация хаттамаларын теңшеу.
* Әкімшілік кіруді қорғауды орнату.
* Шифрлауды қосу.
* Барлық әдепкі параметрлерді өзгерту.
* Микробағдарламаларды уақтылы жаңарту.

Алайда, жоғарыда аталған параметрлерді қолдануға қарамастан, сымсыз құрылғыға қол жеткізе алатын және бұзу технологияларын білетін хакер жеке пайдаланушының да,

ұйымның да желісін бұзуы мүмкін. Сонымен қатар, толық Интернетке қосылған көптеген жаңа сымсыз құрылғылар сымсыз қорғаныс функцияларына ие емес.

Сондықтан сымсыз байланысы бар ақылды және мобильді құрылғылардың трафигі, сондай-ақ сенсорлар мен кіріктірілген нысандардың трафигі қауіпсіздік құрылғылары мен контекстке негізделген желілік қосымшалар арқылы өтуі керек.

Шамадан тыс және қол жетімділіктің жоғары деңгейі

Егер желіге қосылулар көп болса, оның қол жетімділігі мен сенімділігін қамтамасыз ету маңызды.

Артық болу желілік инфрақұрылымның қосымша компоненттерін, байланыс арналарын және негізгі ресурстарды олар істен шыққан жағдайда резервтеу үшін қуат элементтерін қажет етеді. Сондай-ақ, артықтық келісім-шартта келісілген өлшеу кезеңінде алдын-ала белгіленген пайдалану деңгейінің сәйкестігін қамтамасыз ететін жүйенің жоғары қол жетімді құрылымын қамтамасыз ете отырып, ресурстардың жүктемесін бөлуді қолдайды.

Артық қосылымдар мен жабдықтардан басқа, деректерді сақтау қажет. Қауіпсіз резервтер деректерді шифрланған форматта мұрағаттайды, бұл сақталған мұрағатқа рұқсатсыз кіруге жол бермейді.

Адамдар-ең әлсіз байланыс

Кейбір адамдар зұлым мақсаттарды көздейді, ал қалғандары қателіктер жібереді және олардың жабдықтары мен деректерін қауіп төндіретін қауіпсіздіктің жеткілікті деңгейін қамтамасыз етпейді. Активтерді қорғау үшін пайдаланушылардың мінез-құлқын реттейтін ережелер мен нормалар қолданылуы керек, рұқсат етілген және тыйым салынған әрекеттер, сондай-ақ жүйелер мен деректерге қол жеткізу тәсілі анықталуы керек.

Қауіпсіздік саясаты

Қауіпсіздік саясаты ұйымды, оның қызметкерлері мен жүйелерін қорғау үшін сақталуы керек барлық ережелерді, нормалар мен рәсімдерді анықтайды. Қауіпсіздік саясатын қауіптердің белгілі бір түрлерімен күресуге бағытталған көптеген түрлі салаларға бөлуге болады. Толық ақпаратты көру үшін әрбір саясат түрін басыңыз.

Пайдаланушыларды оқыту-қауіпсіздік саясатының маңызды құрамдас бөлігі. Іс-әрекеті қауіпсіздік саясатымен реттелетін қызметкерлер бұл туралы біліп қана қоймай, оны түсініп қана қоймай, сонымен қатар адамдардың, мәліметтер мен заттардың қауіпсіздігін қамтамасыз ету үшін осы саясатты толығымен ұстануы керек.

15.6 - сурет

Ұйымдар жеке деректердің барлық түрлерін жинай алады. Алайда, қол жетімділік пен құпиялылық арасында әрқашан заңдылық пен этика мәселелерінде қайшылықтар болады. Деректер блоктары метадеректермен толықтырылады, олар деректерді жасау орны, автор және тағайындау орны туралы ақпаратты қамтиды. Осылайша, деректер алмасуға болатын меншікке айналады. Бұл өзгеріс проблемалар туындаған жағдайда саясат пен заңдарды сақтау мақсатында ақпаратты бақылауға мүмкіндік береді.

Алайда, жеке деректердің анықтамасы кеңеюде. Бір адам үшін жеке деректер басқа адам үшін болмауы мүмкін. Мысалы, онкологиялық науқас пен сау науқас құпия түрде қалдырғысы келетін медициналық ақпаратты басқаша қабылдайды.

15.7 - сурет

Жан-жақты Интернет ұйымның басқару және ақпараттық технологиялар жүйелерін біріктіруді талап етеді.

"Машина-машина" (M2M) түрін қосу — бұл желі арқылы қосылған құрылғыларға ақпарат алмасуға және адамның қолмен араласуынсыз әрекеттерді орындауға мүмкіндік беретін технология. Адам машинасы (M2P) түріндегі қосылыстарда техникалық жүйелер ақпарат беру немесе алу үшін қызметкерлермен және ұйымдармен өзара әрекеттеседі. Адам-адам (P2P) түріндегі қосылымдар — бұл адамдар арасындағы үздіксіз байланыс пен бірлескен жұмысты қамтамасыз ету үшін қолданыстағы желілік инфрақұрылымды, құрылғылар мен қосымшаларды қолданатын бірлескен шешімдер. Барлық осы байланыс түрлері транзакциялық болып табылады.

Кешенді Интернеттің шешімін іске асыру үшін ең алдымен ағымдағы процестер мен процедураларды түсіну қажет. Бизнес-процестерден басқа, ақпараттық технологиялардың қолданыстағы желілік инфрақұрылымын, Желілік операцияларды және желіні басқару құралдарын зерттеңіз.

Қауіпсіздік жүйесі нақты уақыттағы қауіп-қатерлерге жауап беруі үшін ол жоғары өнімді және ауқымды болуы керек. Cisco қауіпсіздік архитектурасы нақты уақыт режимінде қауіпсіздікті қамтамасыз етуде қолданылатын ақпаратты алу үшін бірлесіп жұмыс істейтін құралдар мен жүйелердің толық жиынтығын ұсынады. Сонымен қатар, желі өздігінен де, қызметкерлердің елеусіз араласуымен де қауіпсіздікке төнетін қатерлерге жауап ретінде әрекет ете алады және қайта құрылуы мүмкін.

Қауіпсіздік саясаты ұйымды, оның қызметкерлері мен жүйелерін қорғау үшін сақталуы керек барлық ережелерді, нормалар мен рәсімдерді анықтайды. Жеке деректерді анықтау кеңеюде.