Дәріс 9. Ақпараттық қауіпсіздендіруді қамтамасыз ету жүйелерінің сипаттамалық қасиеттері

Жоспары:

1 Ақпараттық қауіпсіздендіру қағидалары
2 Желілерді қорғау
3 Ақпаратты қорғаудың бағдарламалық мүмкіншіліктері
4 NetWare желілеріндегі деңгейлер
5 Ақпаратты қорғаудың әкімшілік-ұйымдастыру қорғаныс құралы
6 Операциялық жүйелерді парольмен жабдықтау

Ақпараттық қауіпсіздендіру келесі жүйелік қағидаларда құрылу тиісті:
-жинақтылық;
- қорғаудың үздіксіздігі;
- ақылды жеткіліктілік;
- басқару және қолдану иілгіштігі;
- қорғау алгоритмдерінің және механизмдарының ашықтығы;
- қорғау шараларын және құралдарын қолдану қарапайымдылығы.

Жинақтылық қағидасы. Қорғау тұтас жүйелері құру жанында әдістердің және құралдарды комплексті қолдану АЖ қорғау әр текті құралдардың келісілген қолдануын болжайды, қауіптерді орындау маңызды каналдары барлық қайта жабушының және компоненттердің оның бөлек жапсарларда әлсіз орындарды ұстаушының еместің. Есепке ала тек қана емес қорғау жүйесі тиісті салып алу, сонымен қатар қауіпсіздік қауіпларының орындау принципшіл жаңа жолдарының көріну мүмкіншілігі есепке ала. Үздіксіздік қағидасы. Ақпаратты қорғау - бір жолғы шара емес және өткізілген шаралардың айқын жиынтық емес тіпті және анықталған қорғау құралдары, ал толассыз мақсатқа бағытталған процес, АЖ барлық тіршілік циклы кезеңдерінде лайықты шараларды қабылдау. Қорғау жүйесін өңдеу қорғайтын жүйені өңдеумен паралельді жасалу тиісті.

Ақылды жеткіліктілік қағидасы. Абсолютті қорғау жүйесін жасау принципиалды мүмкін емес. Уақыттың және құралдарды жеткілікті саны жағдайында кез-келген қорғауды жеңуге болады. Сондықтан тек қана қауіпсіздік қабылдауға болатын деңгейінде әңгіме қозғау мәні бар.

Қорғау иілгіштік қағидасы. Қорғау жүйесін жасау белгісіздік жағдайында жиі кездеседі. Сондықтан, қабылданған шаралар және анықталған қорғау құралдары, бастапқы дәуірге әсіресе оларды пайдалану, шамадан тыс сияқты, дәл осылай қорғау жеткіліктісіз деңгейін қамсыздандыра алады. Қамтамасыз етуге арналған түрлендіру мүмкіншіліктері қорғанушылық деңгейімен, қорғау құралдары айқын иілгіштікке ие болу тиісті.

Алгоритмдердің және қорғау механизмдарының ашықтық қағидасының

мәні тек қана ұйымдық құрылымның және оның ішкі жүйелерінің жұмыс жасау алгоритмдері құпиялығынан қорғау қамтамасыз етілмеу тиісті. Қорғау жүйесінің жұмыс алгоритмдерін білу оны жеңуге мүмкіндік туғызу тиісті емес.

Қорғау құралдарын қолдану қарапайым қағидасы. Қорғау механизмдары интуициялық мәлім болуға тиісті және қолдануда қарапайым. Қорғау құралдарын қолдану арнайы тілдерді білу немесе әрекеттердің орындалуымен байланысты болу тиісті емес, көп әрекетті талап ететін маңызды қосымшалар ресми пайдаланушылары әдеттегі жұмысына, сонымен қатар ескішіл түсініксіздеу операциялардың орындалу пайдаланушыларынан талап ету тиісті емес (бірнеше пароль және аттарды енгізу және т.б.).

Компьютерлік жүйеге ойластырылған қатерлердің типтік тәсілдері және әсер ететін каналдары келесі болады:

- Қолжетімдік объектілеріне тікелей қатынасы;
- Қорғау құралдарын айналып қол жетімдік объектілеріне қатынас жасайтын бағдарламалық және техникалық құралдарды жасау;
- Қол жетімдік жасауға мүмкіндік беретін қорғау құралдарын өзгерту;
- Компьютерлік жүйенің техникалық құралдарына, функцияларын және құрылымын бұзатын және қол жетімдікті жүзеге асыруға мүмкіндік беретін бағдарламалық және техникалық механизмдерді енгізу.

Ақпаратты алу тәсілі бойынша қол жетімдік каналдарды мыналарға бөлуге болады: физикалық; электромагниттік (сәулелерді ұстап алу); ақпараттық (бағдарламалық - математикалық). Қол жеткізу әдістері: ақпаратты жазу; ақпаратты оқу; ақпаратты жоюға немесе оны өңдеу және сақтау ережелерін бұзуға әкеліп соғатын КЖ элементтеріне физикалық әсер ету.

Ең көп таралған белгілі әдістер және әсер ететін каналдар мыналар:

- Өңдеуден кейін қалған ақпаратты жинау;
- АЖ-ге оның интерфейстері арқылы біреудің паролін алу жолымен ену;
- «Люк» деп аталатын компьютер мүмкіндіктерін жасырын, құжатталмаған өңдеушілерді қолдану;
- АЖ-ге ақпаратты тасымалдау құралдары арқылы (дискета, CD-ROM) немесе желі арқылы (ЭП, FTP...) бағдарламаларды енгізу;
- Жүйені зерттеуге арналған дизассемблерлер мен отладчиктерді қолдану;
- Қоректену көзін және АЖ компоненттерінің схемасын желі бойынша жоғары күшті импульстерді беру арқылы істен шығару;
- Қосымша электромагниттік сәулелер мен нысаналаулардың (ПЭМИН) эфир немесе комуникация сызықтары бойынша ұстап алу;
- Intranet және Internet желілері арқылы желілік шабуылдарды жүргізу.

Әкімшілік аутентификациясының мәліметтерін табуға арналған каналдар маниторингі және ақпараттық ағындардың келесі мүмкіндіктері бар желі протоколдардың анализаторлары:

- Желі ресурстарын қашықтықтан басқару, торабтарға қол жетімдік;
- Желілік трафик жайлы статистикалық мәліметтерді жинау;
- Желі бойынша жіберілетін пакеттерді декодтау.

- Ақпаратты талдау үшін ұстап қалу кезінде мәліметтерді іріктеу.
- Жасырын тыңдау - желілік ағынды ұстау және оны талдау ("sniffing")
- TCP sequence number (IP-spoofing) болжау;
- "десинхрониздік жағдайда" қосуды енгізу
- Пассивті сканерлеу: демондардың қандай TCP-порттарда жұмыс істейтінін анықтау;
- ICMP-пакеттермен ("ping flood") басылу;
- SYN-пакеттермен ("SYN flooding") басылу.
- Жіберушінің жалған адрестері: Интернеттің электрондық поштасында жіберушілердің адрестеріне сенуге болмайды. Хатты ұстап алу. Пошталық бомба – электрондық пошта арқылы шабуыл жасау:
- Пошталық ақпаратламалар диск толғанша қабылдана береді
- Кіріс кезек тағы өңдеу және беру керек хаттамалармен толады
- Қолданушыға диск квотасы шектен шыққан болуы мүмкін.

Желілерді қорғау

Бір компьютерде жұмыс істеуден бірнеше компьютерлер желісінде жұмыс істеуге көшу барысында ақпаратты қауіпсіздендіруді қиындататын келесі себептері бар:

- желіде бірнеше пайдаланушылардың жұмыс істеуі және олардың күнделікті ауысып отыруы, пайдаланушының аты мен пароль арқылы ақпаратты бөтен пайдаланушылардан қауіпсіздендіру жеткіліксіз;
- желіге көптеген потенциалдық каналдардың кіріп кетуі;
- эксплуатациялық процесте туындайтын аппараттық және бағдарламалық қамтамасыз етудің жеткіліксіздігі.

Кез-келген қосымша байланыстар басқа сегменттермен немесе Интернет желісіне қосылу жаңа проблемаларды туындатады, оған қоса компьютерлік вирустармен зақымдау мүмкіншілігін көбейтеді. Әрбір құрылғы желіде, сәйкес өрістерді идеалдық емес экрандаудан электромагниттік сәулендірудің потенциалдық көзі болып табылады, әсіресе жоғары жиіліктерде. Электромагниттік сәулелендіруден басқа потенциалдық қауіпті кабелдік жүйеге контактілі емес электромагнит әсер етеді. Бірақ коаксиалдық кабелдер немесе “витых пар”, оларды “медные кабелы” деп атайды.

Проводтық қосудың бұл типтерін физикалық жалғаудағы кабелдік жүйеге қолдану мүмкін. Егер желіге кіру үшін пароль белгілі болса, онда мұндай пайдаланушыларға желіге кіру файл-сервер арқылы, немесе жұмыс орындарының бірінен іске асуы мүмкін. Сол себепті желіден тыс орналасқан ақпаратты сақтайтын құрылғылардан ақпарат жоғалу мүмкін.

Желідегі ақпаратты қорғауды арнайы “шуыл генераторын” қолдану арқылы жүзеге асыруға болады. Оптоволокондық кабелдер электромагниттік өрістің әсерінен оқшауланған, және бұлар санкционирленбеген қосуларды таба алады. Ақпаратты қорғауды қамтамасыз ететін құралдарды үш топқа бөлуге болады:

1. **Техникалық құралдар**, бұлар физикалық кіруге кедергі жасайды (кілттер, терезедегі решеткалар, сигнализация және т.б.). Техникалық құралдың құндылығы субъектілік факторлардан тәуелсіздігімен және жоғары модификацияға беріктігімен байланысты. Кемшіліктері – жеткіліксіз сапасы, қымбат тұратындығы және т.б.

2. **Бағдарламалық құралдар**, бұған қоса пайдаланушыларды идентификациялауға арналған бағдарламалар, ақпаратты шифрлау, уақытша файлдарды жою, жүйені қауіпсіздендіретін текстік бақылау және т.б. Бағдарламалық құралдың құндылығы – универсалдығы, беріктігі, орнатудың қарапайымдылығы, модификациялауға мүмкіншілігі. Кемшіліктері – желінің физикалық мүмкіншілігін шектеуі, файл-сервердің және жұмыс орындардың жарты ресурстарын қолдану, кездейсоқ немесе келісілген өзгертулерге жоғары сезімталдығы, компьютердің типіне (аппараттық құралына) тәуелді мүмкіндігі.

3. **Ұжымдық құралдар**, бұған қоса ұжымдық-техникалық және ұжымдық-құқықтық құралдар. Ұжымдық құралдардың құндылығы - әр түрлі мәселелерді шешуге мүмкіншілігі, құрудың қарапайымдылығы, желідегі өзгерістерге тез сезімталдығы, модификациялауға мүмкіншілігінің шексіздігі. Кемшіліктері – субъектік факторларға жоғары тәуелдігі және нақты бөлімшелердің жалпы ұжымдық жұмыстармен байланысы. Мәліметтерді шифрлау ақпаратты қауіпсіздендіруге арналған әр түрдегі бағдарламалық құралдардан тұрады. Шифрлау түсінігі -“*Криптография Firewalls*” ұғымымен байланысты жиі қолданылады. Криптография - шифрлау және шифрлық мәліметтерді ауыстыруға байланысты қосымша мәселені шешу жолдарын қарастырады. Шифрлауға арналған бағдарламалар саны шектеулі және олардың жартысы де-факто немесе де-юре стандарттары болып табылады. Бірақ шифрлау алгоритмін білмей дешифрлауды жүргізу қиын.

Ақпаратты қорғаудың бағдарламалық мүмкіншіліктері

Желілік операциялық жүйелерде орнатылған қауіпсіздік құралдары жеткіліксіз, себебі олар тәжірибе жүзінде пайда болатын жағдайларды толық шеше алмайды. Мысалыға, NetWare 3x, 4x желілік операциялық жүйелері аппараттық бүліну және құртылудан ақпараттардың эшалондаған қауіпсіздігінің беріктігін қамтамасыз ете алады.

Novell фирмасының SFT (System Fault Tolerance) бағдарламасы үш негізгі деңгейді қарастырады:

▪ SFTLevel I. Бірінші деңгей FAT және Directory Entries Tables-тің қосымша көшірмелерін жасауды қарастырады. Сонымен қатар файлдық серверге жаңадан жазылған берілгендердің блогын тездетіп верификациялауды және де кез-келген қатты дискіде 2% көлемді резервтеуді ұйымдастырады. Бүліну табылған жағдайда, берілгендер дискінің резервтелген облысына бағытталады, ал бүлінген блок “нашар” блок ретінде белгіленіп, келесіде ол қолданылмайды.

▪ SFTLevel II. Екінші деңгейдің “Арнайы дискілер” құру мүмкіндігі бар. Одан басқа қосымша дискілік бақылаушылар, ток көзін және интерфейстік кабельдерді дубльдеу мүмкіншіліктері бар.

▪ SFTLevel III. Үшінші деңгей локалды желіде серверлердің көшірмесін пайдалануға мүмкіндік береді. Олардың біреуі - “негізгі”, 17 екіншісі – “барлық” ақпараттың көшірмесін сақтайды. Егер “негізгі” сервер істен шықса, екіншісін қолдануға болады.

NetWare желілеріндегі басқару және кіру құқығын шектеу жүйесі де бірнеше деңгейден тұрады:

- бастапқы кіру деңгейі пайдаланушы аты мен паролінен, жұмысқа рұқсат беру және бермеу типіндегі есептік шектеудің жүйесінен тұрады. ▪пайдаланушылар құқығының деңгейі.
- файлдар мен каталог атрибуттарының деңгейі.
- файл-сервердің консолдық деңгейі.

Бірақ NetWare-дің операциялық жүйедегі бұл ақпаратты қорғау жүйесіне сену барлық кезде дұрыс емес. Өйткені, Интернеттің көптеген ережелері және дайын бағдарламалары санкциясыз кіруге болмайтын кейбір элементтерін бұзуға мүмкіндік береді. Мұндай ескерту сонымен қатар орнатылған ақпаратты қорғау құралдары бар мықты желілік операциялық жүйелерге де қатысты (Windows, Unix). Себебі, бұл желілік операциялық жүйелерінің шешетін есебі көптеген есептердің тек бір бөлігі ғана болып табылады.

Бір функцияны алға шығарып, басқа функцияларға көңіл аудармау желілік операциялық жүйелерінің дамуының магистралды бағыты бола алмайды. Бірақ та, NetWare 4.1 желілік операциялық жүйесінде “ашық кілт” принципі негізінде RSA-алгоритмі көмегімен берілгендерді кодтау мүмкіндігі қарастырылған. Ақпаратты қорғаудың арнайы бағдарламалық құралдарының санкциясыз кіруден қауіпсіздігі орнатылған желілік операциялық жүйелерге қарағанда мүмкіндіктері көп және мағыналы сипатталған. Шифрлау бағдарламаларынан басқа ақпаратты қорғау құралдары өте көп.

Олардың ішінен екі жүйе көп қолданыс тапқан. Олар ақпараттық ағынды шектеуге көмектеседі.

1. Firewalls - брандмауэрлер (Firewalls – ағылшын тілінен аударғанда – “отты дуал”). Жергілікті және аумақты желі арасында арнайы аралық серверлер құрылады. Олар өзі арқылы өтетін желілік-транспорттық деңгейлер трафигін бақылап, фильтрлейді. Бұл жүйе корпоративтік желідегі санкциясыз кіруді азайтады, бірақ оны тіптен жоя алмайды. Бұдан қауіпсіз түрі – ол маскарад әдісі (masquerading). Бұл әдісте жергілікті желіден өтетін трафик firewall-сервері атынан жіберіледі. Сондықтан жергілікті желі тәжірибе жүзінде көрінбей қалады.

2. Proxy-servers. Жергілікті және аумақты желі арасындағы барлық желілік-транспорттық деңгейлер трафигі толығымен шектеледі, яғни маршрутизация типті болмайды, ал жергілікті желі аумақты желімен арнайы делдал-серверлер арқылы байланысады. Бұл жағдайда жергілікті және аумақты желілер арасындағы байланыс тіпті мүмкін емес. Сонымен қатар бұл әдіс жоғары деңгейлі қауіпсіздікті қамтамасыз ете алмайды.

Ақпаратты қорғаудың әкімшілік-ұйымдастыру қорғаныс құралы

Әкімшілік-ұйымдастыру қорғаныс құралдарына ақпаратты және мәліметтерді өңдеу жүйелерінің функциялық процестеріне енуді 18 регламенттеу, қызметкерлердің іс-әрекеттерін регламенттеу және т.б. жатады. Олардың мақсаты қауіптің іске асуын мейілінше болдырмау.

Ең көп тараған әкімшілік-ұйымдастыру қорғаныс құралдарына мыналар жатады:

▪ЭЕМ және басқа ақпаратты өңдеу құралдары орналасқан жерде кіріп шығуға бақылау - рұқсат беру әдісін қолдану;

▪арнайы рұқсат қағаздарын дайындау және онымен өз адамдарын қамтамасыз ету;

▪мәліметтерді өңдеуге қатысатын қызметкерлерді таңдауға байланысты іс-шаралар өткізу; ▪құпия ақпараттарды беруге немесе өңдеуге тек қызмет бабымен рұқсаты бар адамдарды ғана жіберу;

▪өзіндік құпиясы бар магниттік және басқалай ақпарат тасымалдағыштарын және тіркеу журналдарын сейфте немесе басқа адамдар кіре алмайтын жерлерге сақтау;

▪ақпараттарды өңдеуге арналған бөлмеге тыңдағыш құралдар қойылуына қарсы қорғаныс ұйымдастыру;

▪құпия ақпараттардың құжаттарының қолданылуы мен жойылуының есепке алынуын ұйымдастыру;

▪компьютер құралдарымен және ақпарат тасымалдағыш жүйелерімен жұмыс істеуге арналған қызмет бабына байланысты ережелер жасау;

▪ақпараттық және есептеу қорларына енуге тек қана өз қызметіне байланысты функционалдық міндетін атқаратын адамдарға ғана рұқсат беруі.

Операциялық жүйелерді парольмен жабдықтау

Операциялық жүйелерді парольдік қорғау компьютерлік тораптардағы ақпараттарды қорғаудың негізгі деңгейі болып саналады. Бұл қорғау жүйесі барлық операциялық жүйелерде қолданылады. Компьютермен жұмыс бастағанда, қолданушы операциялық жүйелерге кірерде өзін тіркеу тиіс, яғни аты мен паролін енгізу керек. Аты операциялық жүйелерге қолданушыны идентификациясы үшін керек етіледі. Ал пароль енгізілген идентификацияның дұрыстығын дәлелдейді. Диалогтық режимде қолданушының енгізген ақпараты операциялық жүйелерінің үкімінде бар ақпаратпен салыстырылады. Егер салыстыру сәтті аяқталса, онда қолданушы операциялық жүйелердің барлық ресурстарымен жұмыс жасауына болады. Қазіргі таңдағы операциялық жүйелердегі қолданушылардың парольдарын шифрлауға арналған криптографиялық алгоритмдер көп жағдайда өте берік келеді. Мұндай парольдарды бұзу үшін арнайы бағдарламалар – парольды бұзу бағдарламалары жасалынған. Парольды бұзу бағдарламалары операциялық жүйелерге қойылған парольді сол криптографиялық алгоритмдердің көмегімен кері шифрлау арқылы тауып, табылған сөзді жүйелік файлдағы жазылған сөзбен салыстырады. Белгілі бір символдар жиыны мен автоматты реттелген символдар тізбегін парольдық

бұзу бағдарламалары варианттар есебінде қолданады. Бұл әдіс барлық парольдарды бұзуға мүмкіндік береді. Егер парольдық шифрланған түрі белгілі болып және ол осы жиын символдарынан тұратын болса, парольды бұзуға кететін максимальді уақытты келесі формуламен есептеуге болады:

$$T = \frac{1}{S}\sum_{i=1}^{L} N^i;$$

мұндағы N – жиындағы символдар саны;
L - әр секундтағы тексеру саны;
S – парольдың шектік ұзындығы;
S –парольдың қауіпсіздігін бұзатын компьютердің жылдам істеуі мен операциялық жүйеге тәуелді. Операциялық жүйелердің парольдық қауіпсіздігін бұзуға арналған бұл әдіс өте көп уақытты алады.

Ұсынылған әдебиеттер:

Негізгі әдебиеттер:

1. Нестеров, С. А. Основы информационной безопасности: учебник для вузов/ С. А. Нестеров. - Санкт-Петербург : Лань, 2021., 324 с. — ISBN 978-5-8114-6738-9.

2. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9

3. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3

Қосымша әдебиеттер:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534- 07248-8

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0