ДӘРІС №1: Компьютерлік желілер шабуылдары ұғымы және жіктелуі.

1) Компьютерлік желілер шабуылдары ұғымы;
2) Компьютерлік желілер шабуылдарының жіктелуі.

1) Компьютерлік желілер шабуылдары ұғымы

Соңғы бірнеше онжылдықта ақпараттық қауіпсіздік талаптары айтарлықтай өзгерді. Деректерді өңдеудің автоматтандырылған жүйелерін кең қолданғанға дейін ақпараттық қауіпсіздік тек физикалық және әкімшілік шаралармен қамтамасыз етілді. Компьютерлердің пайда болуымен деректер файлдарын және бағдарламалық ортаны қорғаудың автоматты құралдарына деген қажеттілік айқындала түсті. Автоматты қорғаныс құралдарын жасаудың келесі кезеңі деректерді өңдеудің таратылған жүйелері мен компьютерлік желілердің пайда болуымен байланысты, бұл кезде желілер арқылы берілетін деректерді қорғау үшін файлдарды және бағдарламалық ортаны қорғаудан басқа желілік қауіпсіздік құралдары қолданылуы керек. Желілік қауіпсіздік арқылы барынша толық түсіндіру кезінде біз ақпараттың желілер арқылы берілуі кезінде пайда болатын қауіпсіздік бұзылуларының алдын-алу шараларын, сондай-ақ осындай қауіпсіздік бұзушылықтарының болғанын анықтайтын шараларды түсінеміз.

Компьютерлік желілерді пайдалану кезінде туындайтын қауіпсіздікке қатысты бірнеше мысалдар келтірейік:

1. Фирманың бір-бірінен едәуір қашықтықта орналасқан бірнеше филиалдары бар. Жалпыға ортақ желі арқылы (мысалы, Интернет) құпия ақпаратты жіберген кезде, сіз ешкім бұл ақпаратты тыңдай алмайтынына немесе өзгерте алмайтындығына сенімді болуыңыз керек.

2. Желілік әкімші компьютерді қашықтан басқарады. Зиянды қолданушы басқару хабарламасын ұстап алады, оның мазмұнын өзгертеді және хабарламаны берілген компьютерге жібереді.

3. Қолданушының қашықтағы компьютерге заңды қолданушының құқығымен немесе құқығы бар рұқсатсыз кіруі. компьютерге қол жеткізу әлдеқайда үлкен құқықтармен қол жетімділікті алады.

4. Компания төлемді электронды түрде қабылдайтын интернет-дүкен ашады. Бұл жағдайда сатушы іс жүзінде төленген тауарды шығаратындығына сенімді болуы керек, ал сатып алушы біріншіден, ол төленген тауарды алатынына, екіншіден, оның несиелік картасының нөмірі ешкімге айналмайтындығына кепілдік беруі керек. атақты.

5. Компания интернетте өзінің веб-сайтын ашады. Белгілі бір уақытта сайттың мазмұны жаңасымен ауыстырылады, немесе сайтқа кірудің осындай ағыны мен тәсілі бар, сервер сұраныстарды өңдеуді жеңе алмайды. Нәтижесінде қарапайым сайтқа кірушілер фирмаға ешқандай қатысы жоқ ақпаратты көреді немесе фирманың сайтына кіре алмай қалады.

Ақпараттық қауіпсіздікке және олардың өзара байланысына байланысты негізгі түсініктерді қарастырайық.

Жекеменшік иесі әр түрлі шабуылдардан қорғалуы керек ақпараттық құндылықтар жиынтығын (активтерін) анықтайды. Шабуылдарды қорғалатын активтердегі әртүрлі осалдықтарды қолданатын қауіп агенттері немесе қарсыластар жүзеге асырады. Қауіпсіздіктің негізгі бұзушылықтары - бұл ақпараттық активтерді жария ету (құпиялылықты жоғалту), оларды рұқсатсыз өзгерту (тұтастығын жоғалту) немесе осы активтерге рұқсатсыз қол жетімділікті жоғалту (қол жетімділікті жоғалту).

Ақпараттық активтердің жекеменшік иелері қорғалатын ресурстардың осалдығын және белгілі бір ортада болуы мүмкін шабуылдарды талдайды. Осы талдау нәтижесінде ақпараттық активтердің берілген жиынтығы үшін тәуекелдер анықталды. Бұл талдау қауіпсіздік саясатымен анықталатын және қауіпсіздік механизмдері мен қызметтерін қолдану арқылы жүзеге асырылатын қарсы шараларды таңдауды анықтайды. Қауіпсіздік механизмдері мен қызметтерін қолданғаннан кейін де кейбір осалдықтар сақталуы мүмкін екенін есте ұстаған жөн. Қауіпсіздік саясаты қорғалатын активтерге және олар қолданылатын ортаға сәйкес келетін қауіпсіздік механизмдері мен қызметтерінің дәйекті жиынтығын анықтайды.

1 -суретте жоғарыда аталған ақпараттық қауіпсіздік тұжырымдамаларының өзара байланысы көрсетілген.

1 –сурет. Ақпараттық қауіпсіздік тұжырымдамаларының өзара байланысы

Осалдық - бұл жүйенің әлсіз жері, оның көмегімен шабуыл жасалуы мүмкін.

Тәуекел дегеніміз - белгілі бір осалдықты қолдану арқылы белгілі бір шабуыл жасау ықтималдығы. Сайып келгенде, әр ұйым өзі қабылдай алатын тәуекел деңгейі туралы шешім қабылдауы керек. Бұл шешім ұйым қабылдаған қауіпсіздік саясатында көрініс табуы керек.

Қауіпсіздік саясаты - ұйымда және ақпараттық жүйелер арасында ақпараттық активтермен қалай жұмыс істеуді, қорғауды және бөлуді басқаратын ережелер, директивалар және тәжірибелер; қауіпсіздік қызметін ұсыну критерийлерінің жиынтығы.

Шабуыл дегеніміз - ақпараттық жүйенің қауіпсіздігін бұзатын кез келген әрекет. Ресми түрде біз шабуыл дегеніміз - бұл берілген ақпараттық жүйенің осал тұстарын пайдаланатын және бұзушылыққа әкеп соқтыратын әрекет немесе өзара байланысты әрекеттер тізбегі деп айтуға болады.

Қауіпсіздік механизмі - бұл шабуылды анықтайтын және болдырмайтын бағдарламалық жасақтама / немесе аппараттық құрал.

Қауіпсіздік қызметі - бұл жүйеде және саясатта көрсетілген деректердің қауіпсіздігін қамтамасыз ететін, шабуылдың орындалуын анықтайтын қызмет. Қызметте бір немесе бірнеше қауіпсіздік механизмдері қолданылады.

Қауіпсіздікті қамтамасыз ету үшін қол жетімділікті, тұтастықты, аутентификацияны, құпиялылықты және істен шықпауды қамтамасыз ететін ақпараттық және ақпараттық жүйелерді қорғайтын механизмдерді анықтау қажет. Бұл ақпараттық жүйелердің қалпына келуін қамтамасыз етуді де қамтиды.

1.2 Желілік шабуылдардың жіктелуі

XXI ғасыр – ақпарат пен техниканың ғасыры. Бүгінгі таңда ақпараттың иесі бүкіл дүниенің иесі дегенді жиі естиміз. Сондықтан ақпаратты қорғау сұранысы пайда болды. Сұраныс болған жерде әрдайым ұсыныс та, пайда болады. Кез келген ақпаратты қорғау шаралары кешенді жүргізілуі қажет. Қазіргі уақытта әр мемлекетте көптеген ұйымдар мен мекемелер жұмыс істеуде. Сонымен қатар, мемлекеттік өте құпия ақпараты болады, сондықтан да ақпараттың қауіпсіздігіне және қорғанышына зор көңіл бөлу қажет. Ал мемлекеттік деңгейдегі ақпарат өте маңызды болып келеді.

Компьютерлік желілер әдетте үш санатқа: жергілікті, корпоративті және ауқымды болып бөлінеді. Компьютерлік желілер, кейбір мағынада, коммутатор көмегімен және трафикті басқаратын орталық станцияларда телефон арасын қосуға болатын – телефон сымдарымен жұмыс істейді. Келесі негізгі түсініктер:

- Желіде жұмыс істейтіндер жұлдыз немесе құрсым пішінүйлесімі типтері нің түрлі топологияларымен компьютерлік желілерді пішінүйлесімдіреді.
- Компьютерлік желілерде компьютер арасындағы деректердің тиімді жә не сенімді жіберілуі үшін бағдарлауыштар, ретқақпалар, көпірлер, қайталауыштар пайдаланылады.
- Желілер аппараттық және бағдарламалық деңгейден тұрады.
- Желілік үлгі ISO/OSI (Халықаралық ұйымдастырулар стандартының ашық жүйелердің өзара әрекеттігі) желіні функционалды деңгейде сипаттайды.

Корпоративті желі бір- бірінен тәуелсіз үш топқа бөлінеді:

- Деректерді жіберудің желілерін құру;
- Дауыстық ақпаратты жіберу желілерін құру;
- Видеоақпаратты жіберу желілерін құру.

Жіберілетін деректер ағынын тиімді сығуды қамтамасыз ететін, көлікті арнаның технологиясы және сигналдың цифрлық өңдеуі дамуымен барлық жоғарыда көрсетілген шарттар бір корпоративті желіге интеграциялауға мүмкіндік пайда болды.

Барлық желілік қызмет көрсету интеграция негізінде бір корпоративті желіге ену деректерді жіберуді ұстау, дауыс және видео, техника жағындағы мамандарға кеткен шығындарды төмендетуге мүмкіндік береді, ал сонымен қатар бір әкімші-техникалық саясатқа біріктірілгенді қарауды қамтамасыз етеді.

Желілік шабуылдар – бұл компьютерді кеңінен пайдаланатын кез келген адамға таныс сөз тіркесі. Оның астарында жеке деректерді, маңызды корпоративтік қорларға рұқсатсыз қатынас құру, мемлекеттік және басқа да құпияларды жария ету қаупі жатыр. Шабуылдарды ұйымдастырып, іске асыру күннен күнге дамып және оны іске асыру жеңілдеп келеді. Оның негізгі екі себебі бар:

Біріншісі Интернет жүйесінің кең таралуы арқасында осал құрылғыларға қол жеткізу ықтималдығы арта түсіп, қасгөйлерге ауқымды масштабта өзара ақпарат алмасу мүмкіндігі туып отыр.

Ақпараттық жүйеге шабуыл деп осы ақпарат жүйесінің олқылықтарын пайдалану арқылы қауіп-қатерлерді іске асыруға мүмкіндік беретін қасгөйлердің іс-әрекеттерін немесе өзара байланысқан іс- әрекеттер тізбегін айтады.

Шабуылды жүзеге асыру мынадай кезеңдерден тұрады:

Шабуылға дайындық, яғни шабуыл алдында ақпарат жинау (information gathering), шабуылды іске асыру (expolotation) және шабуылды аяқтау.

Шабуыл болғанын жасыруды білдірмеу үшін қаскөй мынадай іс әрекеттерге баруы мүмкін:

- Шабуыл жасаушының мекен жайын басқамен ауыстыру;
- Жалған дестелер құру;
- Шабуыл жасаушы түйін ретінде басқа біреудің компьютерін көрсету;
- Шабуылдың стандарттық орындалуын өзгерту;
- Тіркеу журналдарын тазалау;
- Файлдарды жасыру;
- Шабуылды үзінділеу;

Шабуылдар жіктелімінің бірнеше түрлерін көрсететін болсақ:

- Қашықтан ену;
- Жергілікті ену;
- Қашықта тұрып қызмет көрсетуден бас тарқызу;
- Жергілікті қызмет көрсетуден бас тартқызу;
- Желілік сканнерлер;
- Осалдықтар сканері;
- Құпиясөз бұзғыштары;
- Хаттамалар талдаушы;

Желілік өзара әрекеттесу кезінде жіберушіден (файл, қолданушы, компьютер) алушыға (файл, қолданушы, компьютер) ақпарат ағыны жүреді (2-сурет):

Жіберуші Алушы

2-сурет. Ақпарат ағыны

Компьютерлік шабуылдардың көпшілігі жүйенің кейбір қауіпсіздік параметрлерін ғана бұзады. Мысалы, шабуылдар шабуылдаушыға жіберілген хабарларды көруге мүмкіндік береді, бірақ оларды өзгертуге мүмкіндік бермейді. Басқа шабуылдар шабуылдаушыға кейбір жүйелік компоненттерді өшіруге мүмкіндік беруі мүмкін, бірақ ешқандай файлдарға қол жеткізе алмайды.

Бақылау сұрақтары:

1) Қауіпсіз АТ инфрақұрылымының үштігі - құпиялылық, толықтық, қол жетімділік (конфиденциальность, целостность, доступность);

2) Өнімділікті қамтамасыз ету;

3) Тәуекелділікті талдау.