20-дәріс

ҚАЗАҚСТАННЫҢ АШЫҚ УНИВЕРСИТЕТІ

ИНТЕРНЕТ ПСИХОЛОГИЯСЫ

Интернеттегі мәліметтерді қорғау

Интернетті қолдану арқылы қаржылық операциялар орындау, тауарлар мен қызметтерге тапсырыс беру, несиелік карточкаларды пайдалану, жабық ақпараттық ресурстарға қол жеткізу, телефондағы әңгімелерді жіберу сәйкес қауіпсіздік деңгейін қамтамасыз етуді талап етеді. Интернет желісі арқылы жіберілетін құпия ақпарат белгіленген пунктіге жетпес бұрын бағдарлауыштар мен серверлердің белгілі бір санынан өтеді.

Жіберу қауіпсіздігі мәселелерін негізгі бес түрге бөлуге болады:

- ақпаратты қағып әкету;
- ақпараттың бүтіндігі сақталады, бірақ оның құпиялығы бұзылады;
- ақпараттың түрленуі – бастапқы хабарлама өзгереді немесе оны басқа біреу өзгертіп, адресатқа жібереді;
- ақпарат авторлығын өзгерту;
- хабарламаны алып тастау арқылы қағып әкету.

Әдетте бағдарлауыштар олардан өтетін ақпарат ағымдарын аңдымайды, бірақ ақпараттың қағып әкетілу мүмкіндігі бар. Сонымен қатар, ақпарат өзгертіліп, адресатқа өзгертілген күйде жіберілуі мүмкін. Өкінішке орай, Интернет желісі сәулетінің өзі арам ниетті қолданушы үшін осындай әрекеттерге баруға мүмкіндік береді.

Желі қауіпсіздігінің сипаттамалары:

1. Аутентификация – бұл жүйе қолданушысын тану және оған белгілі бір құқықтар мен өкілеттіктер беру процесі.
2. Бүтіндік — мәліметтердің әртүрлі әсер етулер барысында өзінің ақпараттық мазмұны мен түсіндіру бірмәнділігін сақтау қасиеті.
3. Құпиялық — ақпаратқа рұқсат етілмеген қол жеткізудің алдын алу.

Құпиялықты қамтамасыз ету үшін мәліметтерді бастапқы ақпаратты тек кілт болған кезде ғана алуға болатын шифрланған түрге түрлендіруге мүмкіндік беретін **шифрлау немесе криптография** қолданылады.

Шифрлау негізгі екі түсінікке негізделді: алгоритм және кілт. Алгоритм – бұл бастапқы мәтінді нәтижесінде шифрланған хат алынатындай кодтау әдісі. Оны тек кілт көмегімен түсіндіруге болады.

Хатты шифрлау үшін алгоритмнің жеткілікті екені анық.

Келесі қорғаныс түрі — **электронды-сандық қолтаңба.**

ЭСҚ – бұл электронды құжатты оның көшірмесінен ажыратуға арналған реквизит. ЭСҚ ақпаратты жабық кілтті пайдалану арқылы криптографиялық түрлендіру нәтижесінде алынады және қолтаңба кілті сертификатының иесін теңестіруге, сонымен қатар электронды құжаттағы ақпараттың бұзылмағанын анықтауға мүмкіндік береді.

Электронды-сандық қолтаңба – бұл келесілерді қамтамасыз ететін бағдарламалық-криптографиялық құрал:

- құжаттардың бүтіндігін тексеру;
- құжаттардың құпиялығын тексеру; құжатты жіберуші тұлғаны анықтау.

Электронды-сандық қолтаңбаны пайдалану келесідей мүмкіндіктер береді:

- келісімді рәсімдеуге және құжаттар алмастыруға кететін уақытты айтарлықтай азайту;
- құжаттарды дайындау, жеткізу, есепке алу және сақтау процедурасын жетілдіру және арзандату;
- құжаттың растығын кепілдендіру;
- ақпараттық алмасу құпиялығын арттыру арқылы қаржылық шығындар тәуекелін барынша кеміту;
- құжаттарды алмастырудың корпоративтік жүйесін құру.

Электронды-сандық қолтаңбаның үш түрі бар: қарапайым, күшейтілген біліксіз және күшейтілген білікті электронды-сандық қолтаңба.

Кодтар, құпия сөздер және басқа да құралдар көмегімен қарапайым электронды-сандық қолтаңба электронды қолтаңбаны белгілі бір тұлғаның қалыптастыру дерегін растайды.

Қарапайым электронды-сандық қолтаңбаның қорғаныс деңгейі төмен болады. Ол тек құжаттың авторын анықтауға мүмкіндік береді де, құжатты көшірмеленуден қорғамайды.

Күшейтілген біліксіз электронды-сандық қолтаңба:

1) ақпаратты электронды қолтаңба кілті көмегімен криптографиялық түрлендіру нәтижесінде алынады;
2) электронды құжатқа қол қойған тұлғаны анықтауға мүмкіндік береді;
3) электронды құжатқа қол қойған соң өзгеріс енгізу дерегін анықтауға мүмкіндік береді;
4) электронды қолтаңба құралдар арқылы құрылады.

Күшейтілген біліксіз электронды-сандық қолтаңбаның қорғаныс деңгейі орташа болады. Оны пайдалану үшін оны тексеруге арналған кілттің сертификаты керек.

Аутентификация ең маңызды құрауыштардың бірі болып табылады. Қолданушыға қандай да бір ресурсты алуға құқық бермес бұрын оның шын мәнінде өзін таныстырып жатқан тұлға екендігіне көз жеткізу керек.

Қандай бір қолданушының атынан ресурсты пайдалануға сұраныс алған кезде берілген ресурсты ұсынатын сервер басқаруды аутентификация серверіне береді.

Корпоративтік ақпараттық желілерді қорғау үшін брандмауэрлер — желіні екі немесе одан да көп бөліктерге бөлуге және пакеттердің бір бөліктен басқа бөліктерге өту шарттарын анықтайтын ережелер жиынын іске асыруға мүмкіндік беретін жүйе немесе жүйелер топтамасы.

Фишинг – бұл қолданушының несиелік карта нөмірі, құпия сөздер, банктік шоттар жайлы деректер сияқты құнды жеке мәліметтерін ұрлауға бағытталған қаскүнемдіктің бір түрі.

Қаскүнемдер өнерлерін арттырып, электронды поштаның фишинг-хабарламалары мен сырғымалы терезелерді әрдайым жетілдіріп отырады. Олар көбінесе шынайы ұйымдардың ресми танымбелгілері мен көшірме веб-түйіндерден алынған басқа да теңестіруші деректерді пайдаланады.

Фишинг-хабарлама сенімдірек болуы үшін қаскүнемдер оған нағыз веб-түйінді көрсететін, бірақ, шын мәнінде ресми веб-түйін сияқты көрінетін алаяқтық сайтқа апаратын сілтеме қосуы мүмкін.

Электронды поштаның алаяқтық хабарламасын қалай тануға болады?

Фишинг-шабуылдар жүргізу кезінде электронды поштадағы хабарламаларда жиі кездесетін тіркестер мысалы:

- «Өзіңіздің тіркеулік жазбаңызды растаңыз». Компания өкілдері электронды пошта бойынша құпия сөздер, қолданушы аттарын, әлеуметтік сақтандыру нөмірлерін және басқа да жеке деректерді сұрамауы керек.
- Microsoft бірлестігінен несиелік карта жайлы ақпаратты жаңарту өтініші бар электронды пошта хабарламасын алсаңыз, жауап бермеңіз – бұл алаяқтық хабарлама.
- «Егер сіз 48 сағат ішінде жауап бермесеңіз, Сіздің тіркеулік жазбаңыз бұғатталады». Мұндай хабарламалар адамды ойланбастан жауап беруге мәжбүрлеу үшін шұғылдық сезімін тудырады.
- «Құрметті клиент!» Фишинг-хабарламалар әдетте жаппай таратылады және онда қабылдаушының аты да, тегі де болмайды.
- «Өзіңіздің тіркеулік жазбаңызға қол жеткізу үшін төмендегі сілтемені басыңыз».

Өтуді сұрайтын сілтемелерде компанияның шын аты толық немесе ішінара кездесуі мүмкін және олар әдетте жасырылған болады. Олар, ережеге сай, басқа алаяқтық веб-түйінге апарады.

Қаскүнемдер белгілі компаниялардың атын еске түсіретін, бірақ олардан аздап ерекшеленетін URL-мекен-жайларды да пайдаланады: кей әріптер қосылуы, өшірілуі немесе орындарын ауыстыруы мүмкін.

Енді тыңшы-бағдарламалар мен вирустар жайлы сөз қозғайық.

Интернет-қаскүнемдер көптеген компьютерге бір уақытта бақылау орнатып, кейін оларды зиянды әрекеттер орындайтын қуатты желі құрайтын зомби ретінде пайдалану үшін вирустарды қолдануы мүмкін.

Компьютерлік вирус – өзінің көшірмесін жасай алатын және басқа бағдарламалардың кодына, жадының жүйелік тармақтарына, жүктеу секторларына ене алатын, сонымен қатар өз көшірмелерін әртүрлі байланыс арналары арқылы тарата алатын зиянды бағдарламалық жабдықтама түрі.

Вирустың негізгі мақсаты — оның таралуы. Сонымен қатар әдетте оның қатар жүретін функциясы бағдарламалық-аппараттық кешендердің жұмысын істен шығару болып келеді. Бұл – файлдарды өшіру, тіпті, операциялық жүйені өшіру, мәліметтерді орналастыру құрылымын жарамсыз ету, қолданушы жұмысын бұғаттау және т.с.с. Вирус авторы зиянды әсерлерді бағдарламаламаса да, вирус қателіктер, операциялық жүйемен және басқа бағдарламалармен өзара әрекеттесудің ескерілмеген тұстары салдарынан компьютерлерді істен шығаруы мүмкін. Сонымен қатар вирустар ақпарат тасымалдағыштарда орын алып, жүйе ресурстарын пайдаланады.

100 000 компьютерге дейін кіретін зомби желілер жағымсыз поштаны жіберу, басқа компьютерлер мен серверлерге вирустар, шабуылдар тарату, сонымен қатар қылмыс пен алаяқтықтың басқа да түрлерін жасау үшін пайдаланылады.

Компьютерді зомбиге айналдыратын вирус біртүрлі хабарламалардың көрінуін, компьютер жұмысының баяулауын немесе оның күтпеген іс-әрекеттерін тудыруы мүмкін. Мұндай вирустар әдетте компьютерді өшірмейді. Себебі зомби желілердің жұмысы үшін оларға кіретін компьютерлер Интернетке қосылған болуы керек.

Берілген әдістің мәні ақша бопсалайтын кәдімгі бопсалау болып табылады, бірақ ол Интернет көмегімен орындалады.

1. Тосын сыйлы вирус. Қолданушы компьютеріне енген соң, бұл вирус жұмыс үстеліне машина жұмысын қалпына келтіру үшін бір жерге белгілі бір ақша сомасын жіберу керектігі жайлы хабарлама орналастырып, операциялық жүйе жұмысын бұғаттайды.

2. «Ұрланған» коммуникация құралдары. Бөгде аккаунттарды, электрондық жәшіктерді, «мессенджерлерді» бұзу. Нағыз иесіне өз құпия сөзін бұзып, ауыстырған хакерден сатып алу ұсынылады.

3. Жеке ақпараттың жариялануы. Бөгде компьютерден ұрланған материалдар әдетте құпия сөздер мен ақша шоттары жайлы мәліметтерге қарағанда құндырақ болуы мүмкін. Мысал келтірейін, А қолданушысы Б қолданушысын Интернет және басқа электрондық байланыс құралдары арқылы әрдайым қорқытады. Киберандушы қаруы электронды пошта, мессенджерлер, форумдар, чаттар, әлеуметтік желілер болады. Сонымен қатар, желі қаскүнемді анонимді түрде қалуға мүмкіндік береді. Аңдушыны арнайы құралдарсыз есептеп табу өте қиын, кей жағдайда мүмкін емес болады.

Киберандудан қалай құтылуға болады? Бастысы – желіде өзіңіз жайлы ақпаратты барынша аз қалдыру, бұлай істеу арқылы қаскүнемнің Сіздің байланыстарыңызды алу жұмысын қиындатасыз. Араласу кезінде мұқият болу керек.

КТК телеарнасы сайтының материалдары бойынша, «Informsecurity» компаниясының директоры, корпоративтік және ақпараттық қауіпсіздік саласындағы сарапшы Игорь Чернов мәліметтерді сақтау қауіпсіздігін қамтамасыз ететін жеті қорғаныс әдісін ұсынады.

1. Сенімді құпия сөздер. Компьютердің жұмыс үстеліндегі ақпаратты қорғау үшін ең алдымен тіркеу жазбасына құпия сөз құру керек. Қажет болған жағдайда Сіз өз компьютеріңізді оңай бұғаттай аласыз: іске қосу – жұмыстың аяқталуы – бұғаттау. Құрылғыны қосқан кезде құпия сөз енгізу керек. Ноутбукта қақпақты жабу кезінде бұғаттау орнатуға болады. Одан әрі қауіпсіз болу үшін BIOS немесе қатқыл дискке құпия сөз орнатуға болады. Сонымен қатар құпия сөз сенімді болуы керек, кері жағдайда оны қоюдың мәні болмайды. Арнайы генераторды пайдаланып, өзіңіздің барлық логиндеріңіз үшін әртүрлі құпия сөз орнатыңыз. Бұл әлеуметтік желілердегі аккаунттарға да, электронды пошта жәшіктеріне де қатысты. Маңызды құжаттарға да құпия сөз қоюға болады. Бастысы – кілттерді TXT, DOC, RTF файлдарда сақтамау. Дұрысы құпия сөздерді сақтауға арналған арнайы бағдарламаны пайдалану болып табылады. Ол кезде Сізге тек бір ғана құпия сөзді есте сақтау керек болады, қалғандарын тізімнен таба аласыз.

2. Өзекті антивирус. Жеке ақпараттың негізгі қатері – бұл вирустар. Трояндар, құрттар, пернетақта тыңшылары және басқа да зиянкес бағдарламалар оны өшіріп, ұрлап немесе өзгерте алады. Жеке мәліметтерді қорғау үшін антивирустық БЖ-ның брэндмауэр және фаервол функциялары бар өзекті нұсқасын пайдаланып, сондай-ақ желіде мұқият болу – файлалмасушылардан тексерілмеген файлдарды жүктемеу, күдікті сілтемелерге өтпеу және т.с.с. керек.

3. Екіфакторлы аутентификация. Бұл жүйе қолданушылар арасында әлі аса танымал емес, бірақ өз тиімділігімен ерекшеленеді. Ол тек сенімді құпия сөзді ғана емес, сонымен қатар тек қолданушыға ғана белгілі қандай да бір ақпарат немесе деректі топшылайды. Мысалы, бұл оның дауысы, саусақ ізі, смарт-карта немесе басқа нәрсе болуы мүмкін. Бастысы – аталған факторлар бөгде тұлғалар үшін қолжетімсіз болуы керек.

4. HTTPS хаттамасын пайдалану. Желіде төлем жасау кезінде сервердің мәліметтерді қауіпсіз жіберудің HTTPS хаттамасын қолдайтынына көз жеткізу керек. Мұндай жағдайда қаржылық транзакциялар жүргізу кезінде жүйе клиентке бірегей сертификат тағайындайды, содан кейін ол жіберетін барлық мәліметтер 40, 56, 128 немесе 256-биттік кілтпен кодталады. Дешифрлау тек ақырлы құрылғыларда ғана орындалады, сондықтан қаскүнемге мұндай сигналды ұстап алу ештеңе бермейді. Интернет-дүкендердің, банктердің, сондай-ақ төлем жүйелерінің (Яндекс. Ақша, Webmoney) сайттары HTTPS хаттамасын үнсіздік бойынша пайдаланады. Facebook, Google, Twitter, Вконтакте қызметтері оны аккаунт баптамаларына қосуға мүмкіндік береді. Берілген хаттаманы қолданбайтын ресурстарға аса мұқият болу керек.

5. Сымсыз желілерді қорғау. Қаскүнемдер компьютердің ішіндегілерге қорғалмаған Wi-Fi желісі арқылы да қол жеткізе алады. Мұның алдын алу үшін бағдарлауышқа WPA/WPA2 мәліметтерді шифрлау әдісін орнатып, күрделі құпия сөз құру керек. Өзіңізді Wi-Fi желісінің бұзылуынан қосылыс атын таратуды (SSID) өшіру арқылы да қорғауға болады. Мұндай жағдайда бағдарлауышқа тек желінің атын нақты білетіндер ғана қосыла алады.

6. Мәліметтерді шифрлау. Компьютердегі құнды мәліметтерді шифрлау көмегімен қорғауға болады. Free Hide Folder, Folder Lock, TrueCrypt және т.б. сияқты бағдарламалар мұны тегін орындауға мүмкіндік береді. Сонымен қатар маңызды файлдарды ZIP немесе RAR мұрағаттарына салып, оларға сенімді құпия сөз орнатып қоюға болады. Қаскүнем Сіздің компьютеріңізге енсе де, мұндай мұрағатты аша алмайды.

7. Ата-аналық бақылау жүйелері. Компьютер алдында балалар отырған кезде вирустарды қабылдап алу немесе хакерлік шабуыл нысанына айналу қатері айтарлықтай артады. Мұндай жағдайда өзіңізді ата-аналық бақылау жүйесі көмегімен қорғауыңызға болады: ол баланың компьютер алдындағы уақытын реттеуге, белгілі бір бағдарламалар мен сайттарға кіруге тыйым салуға, БЖ орнату мүмкіндігін бұғаттауға жағдай жасайды. Сондай-ақ бала үшін құқықтары шектеулі жеке тіркеулік жазба құруға болады.

Желідегі ақпараттардың қауіпсідігін сақтаудың тағы бір жаңа, танымал құралы **блокчейн технологиясы** болып табылады. Тұжырымдамалы түрде Блокчейннің жаңа технологиясын 2013 жылы Виталий Бутырин сипаттады, оның жарыққа шығуына көптеген танымал программистер, соның ішінде биткоинның виртуалды ақшаларын жасау алдында тұрғандары да көмектесті. Бүгінде **криптвалюта онымен байланысты биткоинді терминдерін** интернеттен көптеп кездестіруге болады. Идеяны іске асырудың сәті тек 2015 жылы ғана түсті.

Блокчейн технологиясы, капиталдануы осынша қысқа мерзім ішінде 1 миллиардқа жуық АҚШ долларын құраған криптовалюталық эфириуммен шектелмейді. Блокчейннің ашық кодының (құпия сөзінің) негізінде бірнеше стартаптар, яғни компаниялар жұмыс жасайды, солардың ішіндегі ең танымал ДАО инвестициялық қоры. Ресейдегі орталық банкінің өзі ақпараттар алмасу үшін өз негізінде блокчейн технологиясын қолданатын платформа әзірлеу үстінде. Блокчейнде жұмыс жасайтын алғашқы және белгілі қосымша қолданба биткоин болып табылады, бірақ эфир әрі қарай жүріп жатыр, ол барлық сандармен өрнектеуге болатындарға жарамды. Бұл криптовалютадағы операциялар транзакция деп аталады. Транзакциядағы сома тізбегі «Ақылды» келісімшарт деп аталады.

Американдық «Economist» баспасының сарапшылары блокчейн технологиясының пайда болуы қаржы қарым-қатынасында жаңа дәуір тудырды деп есептейді. Мұнан былай эфириум

криптовалютасы жекеленген дербес «Ақылды» келісімшарттарға бөлінетін бағдарламаланған, үлестірілген желіге айналады. Бірыңғай орталықтың болмауы, кодтың ерекешелігі құпия мәліметтерді алаяқтардан сенімді түрде қорғайды. Эфириум технологиясы келешекте бірте-бірте біртұтас болып бірігетін корпоративтік желілердің, бағдарламалардың пайда болуына мүмкіндік туғызады. Келешекте эфириум бүкіл дүниежүзілік біртұтас валютаға айналуы мүмкін. Көріп отырғанымыздай эфириумнің болашағы зор.

2019 жылы Қазақстанның қаржы саласында блокчейн технологияларын қолданатын болады. Осылай деп Қазақстан Республикасының Премьер-Министрінің орынбасары Ерболат Досаев Қазақстан Республикасының Қаржы Министрлігінің кеңейтілген алқасында хабарлады. «Әрі қарай егер де түпкілігі ойдағыдай өтетін болса, онда 2019 жылы блокчейн технологияларын практикаға ендіріп және қолдануға кірігу үшін барлық қажетті жағдайларды жасаймыз деп үміттенеміз», – деді Ерболат Досаев. Бақыт Тұрлыханұлы Сұлтанов Елбасымен кездесуінде бұл жөнінде: «Біз 2018 жылдың тамызында алғашқы қадамды жасаймыз», – деді. Оның айтуынша бұл технологияны бірінші болып Қаржы Министрлігі енгізеді деп атап өтті.

Блокчейннің келесі артықшылықтарын пайдалану көзделеді:

- Әлеуметтік салдары: егер де ақпарат алмасу айқын және оны жасыру немесе қолдан жасау мүмкін емес болса, онда сыбайлас жемқорлық өткеннің еншісінде қалады.
- Кез келген нысанның іс-әрекеті өшіруге және өзгертуге болмайтын сандық түрде сақталып қалдырылады.

Бұл технология мемлекеттік секторда да, сол сияқты өндірісте де, заттар ғаламторында және өзге салаларда да қолданыс табады деп ойлаймыз. Деректер қорғанысы жоғарылай түседі деген сенімдеміз.

Өкінішке орай, жүз пайыз тиімділікпен ерекшеленетін мәліметтерді қорғаудың әмбебап әдісі жоқ. Сарапшылар өзіңізді хакерлерден барынша қорғау үшін белгілі бір әдістерді құрамдастыра пайдалануға және ең маңызды ақпараттардың резервтік көшірмесін мерзімді түрде жасап тұруға кеңес береді.