ЛЕКЦИЯ 8. КИБЕРҚАУІПСІЗДІК

Ақпараттық қауіпсіздіктің қатерлері және олардың жіктелуі. Киберқауіпсіздік индустриясы. Киберқауіпсіздік және Интернетті басқару. Зиянды бағдарламалар. Ақпаратты қорғаудың шаралары мен құралдары. Ақпараттық қауіпсіздік саласындағы стандарттар мен спецификациялар. Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы реттеуші құқықтық қатынастар заңнамасы. Электрондық цифрлық қолтаңба. Шифрлау.

8.1. Ақпараттық қауіпсіздікті қамтамасыз ету

Ақпараттық қауіпсіздікті қамтамасыз етудің ең маңызды құраушысы қауіпті анықтау және оның жіктелуі болып табылады. Ақпараттық қауіпсіздікке қауіп төндіруші - қорғалған ақпаратқа қауіпті тудыратын қандай да бір факторлар мен жағдайлардың жиынтығы.

Ақпараттық жүйелер мен электрондық желілер «өнеркәсіптік автоматика және бақылау жүйелері» деген жалпы атауға ие. Өнеркәсіптік автоматика мен бақылау жүйелерінің қауіпсіздігі деп штаттық және жоспарланған жұмысқа заңсыз енуді немесе қасақана араласуды, не болмаса қорғалатын ақпаратқа қолжетімділікті болдырмауды айтады. Киберқауіпсіздік компьютерлерге, желілерге, операциялық жүйелерге, қосымшаларға және өнеркәсіптік автоматика мен бақылау жүйесінің басқа да конфигурацияланатын бағдарлама құрамдастарына қолданылады.

Киберқауіпсіздік бағдарламалардың, желілер мен мәліметтердің біртұтастығын кибер шабуылдардан (цифрлық шабуылдардан) қорғау технологияларының, әдістемелер мен процестердің жиынтығын білдіреді.

Киберқауіпсіздік қауіптің үш түрімен күреседі.

- Киберқылмыс-бұл бір немесе бірнеше шабуылдаушылар жүйеге оның жұмысын бұзу немесе қаржылық пайда алу үшін шабуыл жасау мақсатында ұйымдастырған әрекеттер.
- Кибершабуыл-бұл негізінен саяси сипаттағы ақпарат жинауға бағытталған әрекеттер.
- Кибертерроризм-қорқыныш немесе үрей тудыру мақсатында электрондық жүйелерді тұрақсыздандыруға бағытталған әрекеттер.

Құқық бұзушылар құпия ақпаратты заңсыз көшіріп алу немесе редакциялау (жою немесе түрін өзгерту) мақсатымен (рұқсат етілмеген) кибершабуыл жасайды. Оны, негізінен, адамдардан (ақпараттық жүйелерді пайдаланушылардан) қаржыны ұрлау немесе ұйымдағы өндірістік немесе жұмыстық процестерді бұзу, тіпті мемлекеттік құпияларды ұрлау мақсатында жүзеге асырады.

Қазіргі кезде көптеген ұйымдар мен үкіметтік мекемелерде жұмысқа қажетті барлық ақпаратты, сондай-ақ қызметкерлердің, пайдаланушылардың және т.б. жеке мәліметтерін жинау, сақтау және өңдеу жолға қойылған. Ал бұл ақпаратты қорғауды талап етеді, өйткені ақпарат құпия болуы керек. Осы ақпараттардың жоғалуы немесе ұрлануы адамдар, ұйымдар және тіпті мемлекет үшін де кері салдарға әкелуі мүмкін.

Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны») Қазақстанның әлемнің ең дамыған 30 мемлекетінің қатарына ену бойынша «Қазақстан 2050» стратегиясының тәсілдерін ескере отырып, Қазақстан Республикасы Президентінің «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» атты Жолдауына сәйкес әзірленді.

Ақпаратты қауіпсіздік үшін қауіп төндірушіні, қорғау объектісін анықтау қажет. Себебі ақпарат - бұл кандай да бір дерек. Мысалы, құпия ақпаратты тасымалдаушылар - құжаттар, ақпаратты өндеу мен сақтаудың техникалық құралдары немесе адамдар болуы мүмкін.

Ақпараттық қауіпсіздік - ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қорғау. Құпиялылық - ол тіркелген пайдаланушыға ғана ақпараттық ресурспен колжетімді. Тұтастылық - ол ақпаратты жіберу немесе сактау үрдісінде өзгермеуі. Қолжетімділік - ол уакыттың әрбір сәтінде тіркелген пайдаланушыға ақпараттық деректерді алу және пайдалану мүмкіндігін анықтайтын ақпараттық ресурстардың қасиеті.

Ақпараттың қауіпсіздігі - сакталатын ақпаратты жағымсыз әсерден корғау жағдайы. Ақпараттық қауіпсіздіктің классикалық үлгісі ақпараттың қауіпсіздігі үшін маңызды үш белгіні қамтамасыз етуге негізделеді: құпиялылық, тұтастық және қолжетімділік. Ақпараттық қауіпсіздіктің

классикалық үлгісі ақпараттың қауіпсіздігі үшін маңызды үш белгіні қамтамасыз етуге негізделеді: құпиялылық, тұтастық және қолжетімділік. Ақпараттың құпиялығы онымен өзінің иесі белгілеген катаң шектелген адамдар тобы ғана таныса алады дегенді білдіреді. Егер ақпаратқа қолжетімділікті уәкілеттілігі жоқ адам алатын болса, рұқсат етілмеген қолжетімділікке немесе құпиялықтың бұзылуына жол беріледі. Желілік қауіпсіздік - бұл орындауға рұқсат етілмеген қолжетімділіктен желілік ресурстарды корғауды қамтамасыз ететін өндірістің компьютерлік желілерінін инфрақұрылымына және саясаткердің онымен жүмысына ұсынылатын талаптардың жиынтығы.

Заң немесе иесі қорғайтын ақпараттың кейбір түрлері үшін құпиялық ең маңызды белгілерінің (қызметтік акпарат, заңмен қорғалатын құпиялар түрлері, қолжетімділігі шектеулі жеке деректер, мысалы, банктің клиенттері, кредиторлары туралы мәліметтер, салықтық деректер, медицина мекемелеріндегі емделушілердің Денсаулық жағдайы туралы мәліметтері және т.б.) бірі болып табылады.

Ақпараттың тұтастығы ақпараттың (деректердің) бұрмаланбаған түрде сақталу қабілеті. Ақпараттың заңсыз және иесі көздемеген өзгеруі (оператор қатесінің немесе уәкілеттілігі жоқ адамның қасақана іс-әрекетінің нәтижесінде) тұтастықтың бұзылуына алып келеді.

Әсіресе аса маңызды ақпараттық-коммуникациялық инфрақұрылым объектілерінің жұмыс істеуімен байланысты деректердің тұтастығы ерекше маңызды (мысалы: әуе қозғалысын, электрмен және энергиямен автоматтандырылған жүйелері және т.б.) жабдықтауды басқарудың

Ақпараттың қолжетімділігі - ақпараттық жүйенің тиісті уәкілеттіктері бар субъектілерге ақпаратқа дер кезінде бөгетсіз руксат беру қабілеті мен анықталады.

Ақпаратты жою немесе бұғаттау (қателіктің немесе қасақана іс-әрекеттің нәтижесінде) қолжетімділіктің жойылуына алып келеді.

Қолжетімділік ақпараттық-коммуникациялық қызметтерді беру (теміржол және авиациялық билеттерді сатудың, банктік қызметтердің ақпараттық жүйелері, интернетте енімдерді интернет- ресурстармен және электрондық БАҚ-пен тарату) жолымен клиенттерге қызмет көрсетуге бағытталған ақпараттық жүйе.

Уәкілетті пайдаланушы белгілі бір қызметтерге (көбінесе желілік) рұқсат ала алмайтын жағдайды қызмет көрсетуден бас тарту деп атайды.

Әлеуметтік желілердегі қауіпсіз қарым-қатынастың ережелері. Бүгінде қоғам мүшелері әлеуметтік желілерсіз өз өмірін елестете алмайды. Күн өткен сайын Вконтакте, Одноклассники, Фэйсбук, Твиттер т.б. сияқты әлеуметтік желілерді пайдаланушылар саны артып келеді. Әлеуметтік желілердің көмегімен адамдар бір- бірімен қарым-қатынас жасайды, мәліметтер, фотосуреттер және т.б. алмасады. Мұндай ресурстар неғұрлым танымал бола бастаған сайын, алаяқтар да соғұрлым оларға көбірек қызығушылық танытуда. Осыған байланысты оларды пайдалану қауіпті бола туседі.

Әлеуметтік желілерді пайдалану кезіндегі қауіптіліктер:

1. Жеке ақпаратты (оның ішінде, басқа адамдарға тиістілерін де) жария ету. Бұған тіпті мәліметтердің одан әрі таралуына себепші болатын дос-жаранға жіберген хабарламалар да жатады. Жеке ақпаратты қорғау саласындағы құқықбұзушылықтар тізбегі осылай құрылады.

2. Қауіпті танысулар. Кейбіреулер кәмелетке толмағандармен хат алмасу арқылы азғыруды жүзеге асырса, кейбіреулер жеке кездесуге алдап көндіреді.

3. Қылмыскерлердің назарын аудару. Балалар мен жасөспірімдердің өз өміріндегі барлық оқиғаны әлеуметтік желілерде жария етуі. Тек бір ғана статус пен фотосуреттер бойынша бала мен оның отбасы мүшелерінің қай жерде болатынын, баланың қашан жалғыз қалатынын, қай кезде пәтердің қараусыз қалатынын білуге болады.

4. Жұмыс іздеу, музыка, бейнежазба және т.б. мәліметтерді көшіріп алуға мүмкіндік береді-мыс дейтін қосымшалардың қауіпсіздігіне сенімді болмасаң, оларды орнатудың қажеті жоқ. Көбіне олар орнату кезінде жеке акаунттан логин мен пароль сұратады. Бұл хакерлерге жеке ақпаратқа қолжетімділікті алу мүмкіндігін береді.

5. Басқа компьютерлерден, тіпті ол досыңның компьютері болса да, әлеуметтік желілердегі жеке аккаунттарды ашпау. Өйткені онда сенің аккаунтың туралы мәліметтерді жіберетін вирус болуы мүмкін.

6. Достардан жіберілген тәрізді көрінетін хабарламалар жиі кездеседі, бірақ оларды достарыңның аккаунттарын бұза алған алдаяқтардың жіберуі мүмкін. Егер хабарлама күмәнді болып көрінсе, досыңмен тікелей немесе телефон арқылы жеке байланысып, бұл хабарламаның шынымен досыңнан келгендігіне көз жеткізу қажет.

7. Әлеуметтік желілерге өзің туралы ақпаратты орналастыру кезінде абай болған жөн. Алаяқтар көбіне құпия сұраққа жауап беруді өтінетін «Парольді ұмыттыңыз ба?» батырмасын пайдалана отырып, аккаунттарды бұзады.

8. Әлеуметтік желіге кіру кезінде тек браузердің мекенжай жолын немесе қосымшасын пайдалану керек. Интернеттегі күмәнді сілтеме бойынша әлеуметтік желіге өту жағдайында жеке мәліметтерді ұрлау үшін пайдаланылатын сайтқа түсу тәуекелі туындайды.

9. Өз достарыңның мекенжайларын құпияда ұстау үшін әлеуметтік желілерге электрондық поштадағы мекенжайлар кітапшасының сканерленуіне мүмкіндік бермеу керек.

10. Достарыңа кімдерді қосу керек екендігін қадағалап отыру қажет. Алаяқтар көбіне осындай жолмен қарым-қатынастың тар шеңбері үшін қолжетімді мәліметтерді білуге тырысады.

11. Өз жұмыс орнында әлеуметтік желілерді пайдаланбауға тырысу. Әлеуметтік желі вирустарды немесе тыңшылық бағдарламаларды таратудың көзіне айналуы, олар құпия мәліметтердің жоғалуына әкелуі мүмкін.

Wi - Fi желілерін қауіпсіз пайдалану ережелері. Қазіргі кезде кез келген жерде (қала, ауыл немесе жай ғана көше, қоғамдық орын, мекеме,

вокзал) интернетке қолжетімді тегін қоғамдық Wi-Fi нүктелері бар. Өркениеттің бұл игілігінің арқасында желіде тұрақты қалуға, керекті жұмысты орындауға, әлеуметтік медиа-империяны басқаруға, жаңалықтар мен оқиғалардан хабардар болып отыруға болады. Алайда жоғарыда айтылғандай, жалпыға ортақ қолжетімді Wi-Fi нүктелерімен жұмыс істеу онлайн қауіпсіздікке айтарлықтай қатер төндіруі мүмкін. Мұндай қатерден қауіпсіз өту ушін мынадай негізгі іс - шараларды қабылдау қажет:

«Wi-Fi желісін пайдалану туралы келісімді» мұқият оқып шығу, стандартты тіркеуден өту. Бұл келісімде нақ кандай мәліметтердің ұсынылуы тиіс екендігі, бұл меліметтердің қандай пайдаланылатыны және қай жерде сақталатыны туралы мәліметтер болады.

Веб-сайттар мен қосымшалар үшін қорғалған жалғастыруларды пайдалану. Бұл хакерлердің құпия ақпаратты ұрлауынан қорғайды.

Бейресми дүкендерден қандай да бір косымшаны жүктемеу және орнатпау, сондай-ақ антивирустық бағдарламалық қамсыздандыруды қосқанда, жүйелік бағдарламалық қамтымның жаңартылғандығына көз жеткізу.

Жалпыға қолжетімді желілердің үйлердегі немесе жұмыс орындарындағы желілерге қарағанда, қаскүнемдердің ықпалына көбірек ұшырайтынын есте сақтаған жөн.

Банкілік ақпаратты енгізу немесе өте маңызды веб сервиске жедел кіру қажет болған жағдайда қауіпсіздеу балу үшін, балама ретінде қоғамдық «Wi-Fi» нүктесін емес, ұтқыр интернетті пайдаланған дұрыс.

Зиянды ПО

Атау өзі туралы айтады. Зиянды бағдарламалық жасақтама-киберқылмыскерлердің ең көп таралған құралы. Олар оны пайдаланушының компьютерін және ондағы деректерді зақымдау немесе оны өшіру үшін өздері жасайды. Зиянды бағдарлама көбінесе зиянсыз файлдар немесе пошта тіркемелері түрінде таратылады. Киберқылмыскерлер оны саяси себептермен шабуыл жасау немесе шабуыл жасау үшін пайдаланады.Зиянды бағдарлама әр түрлі болуы мүмкін, мұнда кейбір жалпы түрлер бар:

Вирустар-файлдарды зиянды кодпен жұқтыратын бағдарламалар. Компьютер жүйесінде тарату үшін олар өздерін көшіреді.

Трояншы– вредоносы жасырынатын астында масканы жариялы БОЙЫНША. Киберқылмыскерлер қолданушыларды троянды компьютерге жүктеуге мәжбүр етеді, содан кейін деректерді жинайды немесе бұлдіреді.

Жарнамалық бағдарлама-зиянды бағдарлама таратылуы мүмкін жарнамалық бағдарламалар.

Ботнеттер-киберқылмыскерлер өз мақсаттары үшін пайдаланатын зиянды

БҚ-мен зарарланған компьютерлер желісі.

SQL инъекциясы.Кибершабуылдың бұл түрі мәліметтер базасынан ақпаратты ұрлау үшін қолданылады. Киберқылмыскерлер зиянды кодты дерекқорды басқару тілінде (SQL) тарату үшін деректерге негізделген қосымшаларда осалдықтарды пайдаланады.

Фишинг.Мақсаты пайдаланушының құпия ақпаратын (мысалы, банк карталарының деректері немесе парольдер) алдау болып табылатын Фишинг – шабуылдар. Көбінесе мұндай шабуылдар кезінде қылмыскерлер зардап шеккендерге ресми ұйым ретінде көрінетін электрондық хаттар жібереді.

Man-in-the-Middle шабуылдары ("ортадағы адам") Бұл шабуыл, оның барысында киберқылмыскер деректерді беру кезінде ұстап алады – ол тізбектегі аралық буынға айналады, ал зардап шеккендер бұл туралы Тіпті білмейді. Егер сіз, мысалы, қорғалмаған Wi-Fi желісіне қосылсаңыз, сізге осындай шабуыл жасалуы мүмкін.

DoS-шабуылдар ("қызмет көрсетуден бас тарту" түріндегі шабуылдар)

Киберқылмыскерлер шабуыл объектісінің желілері мен серверлеріне артық жүктеме жасайды, соның салдарынан жүйе қалыпты жұмысын тоқтатады және оны пайдалану мүмкін болмайды. Мәселен, шабуылдаушылар, мысалы, инфрақұрылымның маңызды компоненттерін зақымдауы және ұйымның қызметін доғаруы мүмкін.

Киберқауіпсіздік түрлері

Шифрлау.Оны дұрыс қолданған кезде шифрлау (және бопсалау бағдарламаларының бөлігі емес) сіздің қауіпсіздігіңізді қамтамасыз етудің тамаша тәсілі болып табылады. Шифрлауды қолданатын бағдарлама немесе қызмет сіздің хабарламаларыңызды немесе файлдарыңызды қабылдайды және оларды бастапқы ақпаратты оқуға мүмкіндік бермейтін кодқа айналдырады. Бұл дегеніміз, шабуылдаушы сіздің байланысыңызға араласса да, ол ештеңе көрмейді. Шифрлау-бұл файлдарды жіберу үшін кез-келген қызметті пайдалану кезінде назар аудару керек деректерді қорғаудың сенімді әдісі.

VPN.VPN әртүрлі мақсаттарда қолданылады, мысалы, желіге қашықтан қол жеткізуді қамтамасыз ету үшін, сонымен қатар кибершабуылдардан жақсы қорғайды. VPN қызметтері Сіздің IP-мекен-жайыңызды, яғни желідегі бірегей идентификатор ретінде қызмет ететін және сіздің үй мекен-жайыңызға ұқсас мекенжайды жасырады. Егер сіз оны жасырсаңыз, алаяқтар сіздің орналасқан жеріңізді немесе желіңізді таба алмайды. Мысалы, Сіз Америка Құрама Штаттарында бола аласыз, ал VPN сіздің IP-мекен-жайыңызды еуропалық мекен-жайға жасыра алады.

Аутентификация.Бұл қарапайым технология. Аутентификация сіз өзіңіз берген адам екеніңізді тексеруге мүмкіндік береді, сондықтан шабуылдаушылар сіздің есептік жазбаңызға кіре алмайды. Әдетте тексеру үшін тек пароль қолданылады, бірақ қазір көптеген қызметтер екі сатылы тексеруді талап етеді және бұл туралы толық келісу керек. Екі сатылы аутентификация қосымша қорғауды қамтамасыз етеді, және бұл көбінесе кіру үшін сізге электрондық пошта немесе телефон арқылы жіберілген кодты енгізу керек дегенді білдіреді, хакердің барлық осы арналарға кіруі екіталай.

Қорғаудың бұл әдісі жалпы файлдар немесе кіріс хаттар сияқты онлайн режимінде деректерді сақтау үшін қолданылады. Аутентификацияның тағы бір шешімі-SSO немесе бірыңғай кіру технологиясы. Бұл шешім бір рет кіруге және бірнеше қосымшаларға қол жеткізуге мүмкіндік береді. Бұл әдіс бірнеше есептік жазбаны алаяқтықтың ең қысқа жолы болып көрінуі мүмкін, бірақ олай емес. Егер сіз бірыңғай кіру технологиясын қолдансаңыз, сізге бірегей логин және әр есептік жазба үшін өте күрделі пароль қажет емес. Тиісінше, құпия деректердің саны және оларды ұрлау ықтималдығы азаяды.

SIEM.Ақпараттық қауіпсіздік және қауіпсіздік оқиғаларын басқару жүйесі (SIEM) — бұл нақты уақыт режимінде жұмыс істейтін қорғаныс құралы. SIEM шешімдері бағдарламалық жасақтама немесе қызметтер түрінде қол жетімді. Компанияның қызметін бақылау арқылы олар кез-келген бұзушылықтар туралы бірден ескертеді және проблемалардың алдын алады. Пайдаланылған бағдарламаға немесе қызметке байланысты SIEM сәйкестік туралы есептер шығаруға көмектеседі және апаттан кейін ақпараттық жүйенің жұмысын қалпына келтіруге көмектеседі.

Антивирус және брандмауэр.Бұл қарапайым қорғаныс құралдарын өзіңіз орната аласыз және олар барлық ноутбуктер мен мобильді құрылғылар үшін қажет. Брандмауэрден қорғау және антивирустар зиянды бағдарламаларды тоқтатуға көмектеседі, тіпті егер сіз "жүктеу" түймесін бассаңыз да; киберқауіпсіздік қауіптерін анықтап, оларды дереу алып тастаңыз немесе қауіпсіз қалтаға жылжытыңыз.

Бақылау сұрақтары:

1. «Ақпараттық қауіпсіздік» түсінігіне анықтама беріңіз.
2. Акпарат қауіпсіздігіне кауіпті калай түсінесіз?
3. Акларат қауіпсіздігіне кандай кауіптер мәлім?
4. Киберқауіпсіздік термині нені білдіреді?
5. Әлеуметтік желілерді пайдаланудың қандай қауіптілігі бар?
6. Әлеуметтік желілерді пайдалану кезінде алдын ала сақтанудың қандай іс-шараларын қабылдау керек?
7. Оқу орындарына Wi-Fi керек пе? Оны қолдану қауіпсіз бе? Оның зиянды сәулелерінен қалай қорғануға болады?

8. Wi-Fi желілерін қауіпсіз пайдалану ережелері туралы әңгімелеңдер.