Қазақстан Білім және Ғылым министрлігі
Қарағанды Техникалық унтверситеті

Ақпараттық технология және
қауіпсіздік кафедрасы

Тақырыбы:Дерекқорында ақпаратты қорғаудың ерекшеліктері.

Дайындаған:Битемиров Асылхан

Сиб-19-1

Қабылдаған:Тайлак Бибигуль

Кіріспе

Дерекқор

Дерекқорды қорғау тұжырымдамасы

Дерекқорды қорғау әдістері мен ерекшеліктері

Қорытынды

Пайдаланылған әдебиеттер

Кіріспе

Қазіргі жағдайда кез-келген ұйымның қызметі ақпараттың үлкен көлемімен жұмыс істеумен байланысты, оған қол жетімділіктің кең ауқымы бар.соңғы уақытта ақпараттың маңыздылығының артуының салдары деректердің құпиялылығына, тұтастығына және қол жетімділігіне қойылатын жоғары талаптар болды. Мұндай жағдайларда ұйымның бір ғана қызметкерінің зиянды немесе жай ғана біліксіз әрекеттері тұтастай алғанда ұйымға түзетілмейтін зиян келтіруі мүмкін. Бұл тіпті құнды ақпаратты ұрлау туралы болмауы мүмкін. Маңызды ақпарат ресурсына қол жетімділікті ұзақ уақыт бойы кез-келген тәсілмен бұғаттау жеткілікті. Деректер базасын басқару жүйелері (ДҚБЖ), әсіресе реляциялық ДҚБЖ және сараптамалық жүйелер (ЭЖ) деректерді сақтау, өңдеу және ұсыну саласындағы басым құралға айналды. ДҚБЖ (ЭС) жұмысындағы кез-келген сәтсіздік, деректерге уақытша қол жетімділіктің жоғалуымен бірге, кәсіпорынның бәсекелестік қабілетіне бірден әсер етеді. Сондықтан, деректерді рұқсатсыз кіруден, рұқсатсыз модификациядан немесе оларды жай бұзудан қорғау кез-келген ақпараттық жүйені жобалаудағы басым міндеттердің бірі болып табылады.

Дерекқор

Дерекқор, деректер базасы (франц. base, грек. basis – негіз) – ұзақ мерзімге сақтауға (әдетте, компьютердің жадында), өңдеуге және күнделікті қолдануға арналған деректердің (мәліметтердің) реттелген жиынтығы.

Деректер базасы келісілген жүйе бойынша бөлінген белгілі бір мәліметтердің қоймасы болып табылады және ақпараттың барлық көлемінің тәртібін сақтау мақсатында құрылады. Деректер қоймасының түрлері мен мазмұны ұйымның ерекшелігіне байланысты. Сақтаудың кез-келген форматында ақпарат қауіпсіздік жүйелерінің алуан түрлілігіне сәйкес көптеген құралдар арқылы бұзудан қорғалуы керек. Сонымен қатар, басқа адамдардың мәліметтер базасына енгізу құралдары қатердің алдын-алу құралдарына қарағанда тезірек жетілдіріледі.

Сақтаудан басқа, қазіргі заманғы архивтер есептерді уақтылы жасауға және олардың мазмұнын талдауға мүмкіндік береді. Пайдаланушы ыңғайлылығы үшін көптеген жүйелер Windows жүйесіне бейімделген.

Деректер базасын бұзу мәліметтерді бүлдіру мақсатында да, санкцияланбаған қол жеткізу үшін де жүргізілуі мүмкін. Екі аспект те өте жағымсыз және бірқатар салдарға әкеледі.

Қауіпсіздіктің қаупі, тұжырымдамасы

Қауіпсіздіктің қаупі дегеніміз ақпаратқа зиян келтіруді (бұрмалауды немесе жоюды), ақпараттық ресурстарды ұрлауды, соның ішінде маркетинг мақсатын көздейтін кірудің барлық әдістері деп түсінеміз. Кездейсоқ та, қасақана қорқыту да мүмкін.

Кездейсоқ ақаулар деп пайдаланушыға тәуелді емес техникалық ақаулар - қателіктер, компьютерлердің немесе ақпарат құралдарының зақымдануы, табиғи апаттар түсініледі. Байқаусыз қателіктер, әдетте, бағдарламаны орындау процесінің бұзылуымен байланысты және көбінесе қызметкерлердің кінәсінен болады.

Қасақана қауіп-қатерлер көбінесе сыртқы кіру көздерімен жүзеге асырылады, яғни олар ұйымға - ақпарат көзіне қатысы жоқ. Мұндай «мамандарды» бағдарламалық жасақтама да, ол өңдейтін ақпарат та қызықтыруы мүмкін. Оның үстіне ресурстарды бөлудің мақсаттары әртүрлі болуы мүмкін: банктік кірістен бастап бүкіл кәсіпорынды диверсия мен кемсітуге дейін, содан кейін жұмыс процесін бұзуға дейін.

Мәліметтер қорын қорғау тұжырымдамасы

Деректер қорының қауіпсіздігіне келетін болсақ, деректердің қауіпсіздігін қамтамасыз етуге арналған екі негізгі тәсілді атап өткен жөн:

1.Мәліметтерді таңдамалы басқару. Бір элементке қатысты әр түрлі мердігерлерге әр түрлі күштер берілуі мүмкін жеткілікті икемді әдіс.

2. Мәліметтерді міндетті түрде басқару. Бұл әдіс қарама-қарсы іс-қимыл схемасына ие, яғни мәліметтер қоры және барлық кітапхана объектілері құпиялылық деңгейлеріне сәйкес таратылады, бұл сәйкесінше қол жетімділік деңгейі немесе одан жоғары қолданушыларға көруге және өзгертуге рұқсат етіледі. Құпиялылықтың барлық құрылымын бұзбау үшін әдіс жоғары дәрежелі жіктелімге ие субъектінің төменгі құпия санаттарына мәліметтерді енгізуіне мүмкіндік бермейді.

Іс-әрекеттердің белгілі бір жүйесі кәсіпорын ақпаратының және оларды сақтау құралдарының тұтастығы мен құпиялылығын қамтамасыз етуге бағытталған, бұл ақпаратпен рұқсат етілмеген манипуляцияларды болдырмайды. Егер репозитарийге қол жеткізу қолжетімділік құқығын көп сатылы тексеру арқылы жүзеге асырылса және сонымен бірге бағдарламалық жасақтама құралдарының жеткілікті жиынтығы болса, қорғаныс сенімді болады.

Бастапқы сенімділік критерийлері:

• Деректердің қауіпсіздігі саясаты. Ықтимал қауіптерді бақылауға және оларды жою құралын табуға бағытталған. Белгілі бір ұйымға тән репозиторийдің мазмұнын пайдалану ережелері мен ережелерін қамтиды. Қауіпсіздік саясатын қайта қарау негізінде жүйені қорғауды ұйымдастырудың жеке тетіктері анықталды.

• Деректердің сенімділігі. Таңдалған бағдарламалық құралдардың негіздемесін болжайды. Бұл санат белгілі бір жүйенің қауіпсіздік саясатын жүргізетін механизмдерді қамтиды.

Қауіпсіздікті басқару жүйесінің есептеу бөлігі контрагенттердің қорғалатын деректермен белгілі бір операцияларға жіберілуін бақылайды. Субъектімен байланысқан кезде бақылау функциялары оған рұқсат етілген әрекеттерді корреляциялайды.

Сақтау қауіпсіздігінің ең көп тараған мәселесі - компьютерге рұқсатсыз таратылған қол жетімділік, сондықтан жеке жұмыс орнын қорғау - бұл мақаланың бөлек маңызды аспектісі. Айтпақшы, дербес компьютердің бастапқы мақсаты ақпаратты қорғау процесіне емес, жеке пайдалануға бағытталған. Мұндай қауіптің қаупі компьютерлік мазмұн үшін келесі себептерге байланысты артады:

Сақтанудың жолдары

Егер сіз кең аудиторияға арналмаған дерекқорды сақтау үшін компьютерді қолдансаңыз, оны қорғау және қауіпсіздігі үшін жақсартылған бағдарламалық жасақтама туралы қамқорлық жасауыңыз керек. Іс-шаралар жұмыс орнын физикалық қорғауды қамтуы керек. Бұл объектілерді анықтаудың заманауи жүйелері: құлыптар, инфрақызыл, лазерлік, қозғалысқа жауап беретін ультрадыбыстық жүйелер, теледидарлық бақылау жүйелері, жақындық датчиктері бар кабельдік жүйелер арқылы әр пайдаланушыны сәйкестендіруді білдіреді. Барлық қолайлы құралдар рұқсат етілмеген зиянкестердің пайдаланушының жұмыс орнына кіру ықтималдығын азайтады.

Ақпаратты аппараттық қорғау шараларына:

• қол жетімділікті және деректер элементтерімен әрекеттерді басқару. Қауіпсіздікке жауапты адамдарға жедел жауап алу үшін кіру әрекеттерін тіркеу жүйесі дереу ескертуі керек;

• уақытында архивтеу;

• жүйеге барлық қоңыраулардың жазбаларын жүргізу;

• лайықты сапалы бағдарламалық жасақтама және қауіп-қатерді азайту құралдары. Бұл жүйеге кіру әрекеттерін және уақытша шешімдерден аулақ болуды білдіреді.

Дерекқорды қорғаудың негізгі ережелері

Қорғаудың тексерілген екі әдісі бар:

1. Құпия сөзді қорғау. Ең қарапайым, бірақ сонымен бірге сенімсіз әдіс, әсіресе шифрланбаған құпия сөзді қолдансаңыз, өйткені есептеу жүйесі бірдей парольдері бар басқа пайдаланушыны көрмейді. Сондай-ақ, кемшілік - парольді есте сақтау немесе оны жеке ортаға (қағазға немесе телефонға) бекіту қажеттілігі, бұл өте ыңғайлы емес, өйткені шабуылдаушылар оңай есте сақталатын тіркестерді есептей алады чит парағында жазылған ақпаратты ашуға болады. Жүйеге кіру үшін әрқайсысы әртүрлі дәрежедегі қуат беретін бірнеше құпия сөзді орнатқан жөн.

2. Пайдаланушының идентификациясы. Рұқсат алуға талпыныс дереу аутентификация үдерісімен бірге жүретін жеткілікті күрделі және сенімді тәсіл, яғни кіріс фигураларын қоспағанда.

Компанияның негізгі ресурстарын қорғауға арналған ұсыныстар:

1. Көшіруді болдырмау үшін мәліметтер базасы үшінші тарап компьютерінде сәтсіздікке ұшырау үшін жабдыққа орындалатын кодты байланыстырумен қамтамасыз етілген.

2. Бағдарламалық жасақтаманы зерттеуге жол бермеу үшін оқу процесін баяулататын немесе жоққа шығаратын механизмдер қолданылады. Сонымен қатар, сіз қауіпсіздік жүйесін белгілі бір кіру әрекеттерінен кейін, яғни дұрыс емес пароль енгізгеннен кейін, одан әрі қосылу әрекеттері бұғатталатын етіп бағдарламалай аласыз. Кейбір жағдайларда жүйенің өзін-өзі жою нұсқасын жасаған жөн.

3. Файл сипаттамаларының бірін салыстыру арқылы мәліметтердің рұқсат етілмеген өзгертілуін болдырмауға болады. Файлдарды модификациялауды басқару бағдарламасы өзгертілген файл мен мәліметтер базасы ұсынған түпнұсқа файл арасындағы айырмашылықты анықтаған кезде дабыл қағады.

4. Сіз файлдарды жойылудан қорғау функциясы бар бағдарламаны әзірлеу немесе сатып алу арқылы ғана деректерді жоюдан қорғай аласыз, өйткені, өкінішке орай, мұндай ресурстар MS DOS және Windows амалдық жүйелерінде қарастырылмаған.

5. Қарап шығудың алдын алудың танымал және сенімді әдісі - деректерді шифрлау. Крекинг процесі шифрлау кілтін таңдаумен қиындатады, бұл жеткілікті дамыған бағдарламалық жасақтама құралдарына қарамастан, іс жүзінде мүмкін емес.

6. Компьютерлік жүйенің ақауларын азайту үшін деректерді резервтік көшіру практикасы белсенді қолданылады. Сонымен қатар, процедураның әртүрлі деңгейлерінде резервтеуді енгізу әртүрлі тапсырмаларды орындайды. Бұл жабдықтың артық болуы (компьютерлер, жергілікті құрылғылар немесе схемалар) болуы мүмкін. Жүйенің бірнеше элементтері бірден бір функцияны орындайтын кездегі функционалды резервтеу. Ұқсас схема негізгі элемент бұзылып, оны резервтікке ауыстырған кезде іске қосылады. Ақпараттық резервтеу репозиторийдің маңызды фрагменттерін сақтауға бағытталған және оларды мерзімді мұрағаттау арқылы жүзеге асырылады. Айтпақшы, құжаттар ғана емес, бағдарламалар да архивтеліп, көшірілуі керек.

Қорғау әдістері

• Құпия сөзден қорғау. Қатынау кодын мәліметтер базасын басқару жүйесінің әкімшісі тағайындайды және шифрлау арқылы шифрланған түрде сақталады, бұл шифрды ашу мүмкіндігін жоққа шығарады. Бұл әдісті таңдағанда мәліметтер кітапханасына пароль қажет емес.

• Шифрды ашу үшін пароль. Шифрлаудан қорғау 100% қауіпсіз әдіс болып саналмайды, өйткені деректердің шифрын шешуге болады. Сондықтан, осы әдісті таңдап, сіз әлі де шифрды «құпия сөзбен» қорғағаныңыз жөн.

• Бағдарламалардың бастапқы нұсқаларын шифрлау орындалатын амалдардың ретін жасыруға мүмкіндік береді.

Кіру құқығын белгілеу мүмкіндігі туралы ұмытпаңыз. Бұл құпия заттарға қажетсіз қол жетімділік қаупін едәуір азайтады.

Мәліметтер кітапханаларына қол жеткізу құқықтары келесі режимдерде жұмыс істей алады:

• деректерді қарау мүмкіндігі;
• редакциялау мүмкіндігі;
• ақпаратты қосу арқылы кестені кеңейту мүмкіндігі;
• деректерді қосу және жою мүмкіндігі;
• аталған барлық әрекеттерді орындау мүмкіндігі.

Деректер қорының қауіпсіздігін сақтауға арналған қосымша құралдар, ол жанама болып саналса да, оны қолданған жөн:

• Мазмұнды бақылау. Толтыру кезінде механикалық қате болған жағдайда, редакцияланған өрістің түріне сәйкес келмейтін мән енгізуге болады. Жағдай мәнді басқару функциясы арқылы сақталады, кірісті блоктайды және қате туралы сигнал береді.

• Сақталған процедураларды жобалау. Мәліметтердің шектеулерін орнату арқылы өңделген элементтердің мағыналық мағынасын терең бақылау үшін ақпараттың сенімділігін арттырудың техникалық құралдары қолданылады. Бұған валидацияны басқарудың жетілдірілген түрі - сақталған процедуралардың дизайны кіреді. Бұл кестелер мәліметтерімен алгоритмі кейбір әрекеттерді орындауға мүмкіндік беретін бағдарламалар.

• Мәліметтер қайшылығын шешуге арналған құрылғылар. Олар барлық заманауи бағдарламалық жасақтамаларда ұсынылған және мәліметтер архиві бірдей болса да, бірнеше пайдаланушылардың бір объектіні параллель редакциялау мәселесін шешеді. Алайда, қақтығыстарды болдырмау үшін құлыптау жүйелері жиі енгізіледі.

Пайданылған әдебиеттер тізімі

1. Дейт, К., Дж. Введение в системы баз данных. 6-е изд. – К.; М., СПб.: «Вильямс», 2000. – 848с.

2. Хомоненко А.Д., Цыганков В.М., Мальцев М.Г. Базы данных: Учебник для высших учебных заведений/Под ред. проф. А.Д. Хомоненко. – СПб.: КОРОНА принт, 2002. – 672с.

3. В.В. Корнеев, А.Ф. Гареев, С.В. Васютин, В.В. Райх Базы данных. Интеллектуальная обработка информации. – М.: Нолидж, 2001.- 496с.