№12 дәріс. ҚАУІПСІЗДІК ЖӘНЕ ДЕРЕКТЕРДІ ҚОРҒАУ

Жоспары:

1. Деректердің қауіпсіздігі мен қорғалуына кіріспе
2. Деректердің қауіптері мен осалдықтарының түрлері
3. Деректерді қорғау әдістері мен технологиялары
4. Деректер қауіпсіздігінің нормативтік актілері мен стандарттары
5. Деректерді қорғау жүйелерін енгізудің артықшылықтары мен қиындықтары
6. Деректерді қорғаудың болашағы: трендтер мен технологиялар
7. Қорытынды

Деректердің қауіпсіздігі мен қорғалуына кіріспе

Цифрландырудың қарқынды өсуі жағдайында қауіпсіздік пен деректерді қорғау кез келген көлемдегі және қызмет бағытындағы ұйымдар үшін ең басым міндеттердің біріне айналды. Деректер компаниялардың операцияларында, стратегияларды қалыптастыруда және басқарушылық шешімдер қабылдауда шешуші рөл атқарады, бұл оларды киберқылмыскерлер үшін басты мақсатқа айналдырады. Деректерді қорғау міндеті ақпараттың ағып кетуіне, рұқсатсыз кіруіне, бұзылуына немесе өзгеруіне жол бермеу және оның уәкілетті пайдаланушылар үшін қол жетімділігін қамтамасыз ету болып табылады.

Компанияның құпия ақпараты, Тұтынушы деректері, қаржылық Ақпарат және қызметкерлердің жеке деректері сияқты қорғалатын деректердің әртүрлі түрлері бар. Бұл деректердің құпиялылығын бұзу ауыр зардаптарға, соның ішінде беделдің жоғалуына, қаржылық шығындарға және құқықтық салдарға әкелуі мүмкін. Ұйымдар аутентификация, шифрлау және қол жеткізуді бақылау әдістерін қамтитын деректерді қорғаудың кешенді стратегияларын енгізуге тырысады. Еуропадағы GDPR және АҚШ-тағы HIPAA сияқты стандарттар мен ережелерді енгізу деректерді мемлекеттік деңгейде қорғаудың маңыздылығын көрсетеді және компанияларды деректердің қауіпсіздігін қамтамасыз ету үшін жауапкершілікке тартады.

Технологияның дамуымен ұйымдар бұлтты сақтау және виртуалды жұмыс орындары сияқты шешімдерді қолдана бастайды, бұл деректерді қорғаудың жаңа тәсілдерін және қосымша қауіпсіздік шараларын қолдануды талап етеді. Деректер қауіпсіздігі пайдаланушылар үшін де маңызды аспектке айналады, әсіресе цифрлық кеңістіктегі жеке ақпарат көлемінің тұрақты өсуін ескере отырып. Қызметкерлердің киберқауіптер туралы хабардарлығын арттыру, қорғаудың заманауи әдістерін қолдану және нормативтік талаптарға сай болу ұйымдарға деректердің ағып кету және ұрлану қаупімен байланысты тәуекелдерді азайтуға мүмкіндік береді.

Деректердің қауіптері мен осалдықтарының түрлері

Деректер қауіпсіздігіне төнетін қауіптердің түрлері әртүрлі және үнемі дамып отырады, бұл ұйымдарды ақпаратты қорғау тәсілдерін үнемі қайта

қарауға мәжбүр етеді. Ең жиі кездесетін қауіптердің қатарына зиянды бағдарламалар (вирустар, Трояндар, төлем бағдарламалары), фишингтік шабуылдар, DDoS шабуылдары, сондай-ақ ішкі қауіптер жатады (Сурет 1). Зиянды бағдарламалар құрылғыларға немесе компаниялар желісіне енгізілуі мүмкін, бұл деректердің тұтастығын бұзады және шабуылдаушыларға қол жетімділікті ашады. Бұл бағдарламалар көбінесе ақпаратты ұрлау, бопсалау немесе тіпті деректерді жою үшін қолданылады, бұл компанияларға үлкен зиян келтіреді.

Фишингтік шабуылдар-бұл Құпия сөздер мен несиелік карта деректері сияқты құпия ақпаратты алдау үшін пайдаланушыларды алдау әрекеттері. Шабуылдаушылар жәбірленушіні өз деректерін енгізуге мәжбүрлеу үшін жалған электрондық хаттарды немесе заңды болып көрінетін сайттарды пайдаланады. Мұндай шабуылдар әсіресе қауіпті, өйткені олар тек қызметкерлерге ғана емес, сонымен қатар клиенттерге де бағытталуы мүмкін, бұл компанияның сенімі мен беделін жоғалтуға әкеледі.

Сурет 1. Киберқауіптер мен ақпаратты қорғау құралдарының даму болжамы

DDoS шабуылдары (Distributed Denial of Service) — бұл компанияның ресурстарын шамадан тыс жүктеуге және оның қалыпты жұмысын бұзуға бағытталған шабуылдар. Мұндай шабуылдар клиенттерге қызмет көрсетуден уақытша бас тартуға және айтарлықтай шығындарға әкелуі мүмкін. Деректердің бұзылуы сияқты ішкі қауіптер де күрделі мәселе болып табылады. Көбінесе олар абайсызда да, қасақана да қызметкерлердің өздерінен келеді, мысалы, құпия ақпаратты үшінші тұлғаларға сатқысы немесе ашқысы келсе.

Бұл қауіптердің әрқайсысы мұқият талдауды және әртүрлі қорғаныс әдістерін қолдануды қажет етеді. Ықтимал осалдықтарды білу компанияларға деректерді қорғаудың дәлірек стратегияларын әзірлеуге және ағып кетулер мен шабуылдардың алдын алудың тиімді шараларын енгізуге мүмкіндік береді.

Деректерді қорғау әдістері мен технологиялары

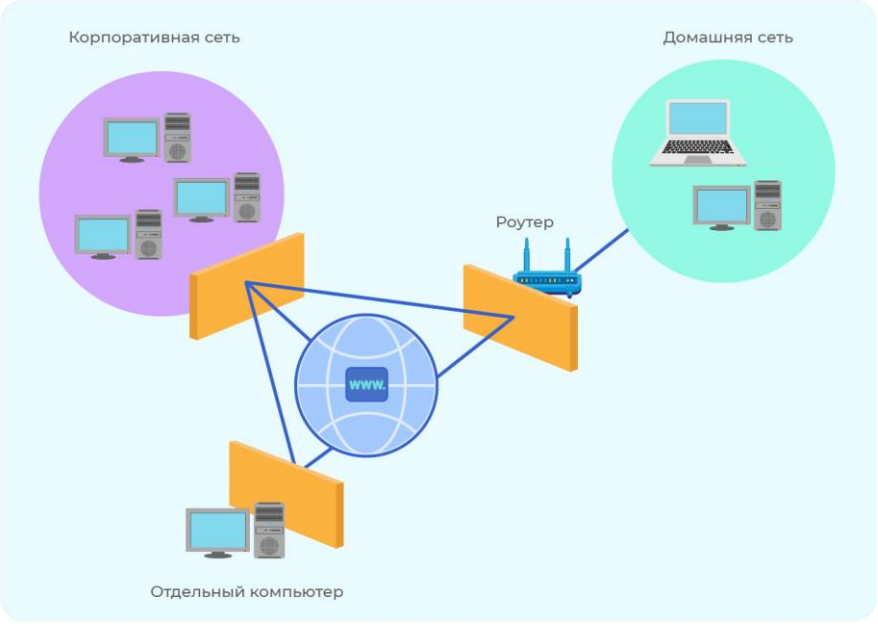
Деректерді қорғау үшін ұйымдар әртүрлі әдістер мен технологияларды пайдаланады, олардың ішінде шифрлау, аутентификация және авторизация,

брандмауэр және кіруді анықтау жүйелері (IDS) бар. Шифрлау деректерді қорғаудың негізгі әдістерінің бірі болып табылады, өйткені ол ақпаратты арнайы кілттері бар адамдар ғана оқи алатындай етіп кодтауға мүмкіндік береді. Шифрлау интернет, бұлтты сақтау және кәсіпорын серверлерінде деректерді тасымалдау кезінде қолданылады, бұл шабуылдаушылардың ақпаратты ұстап қалу қаупін айтарлықтай азайтады.

Аутентификация және авторизация деректерге қол жетімділіктің қауіпсіздігін қамтамасыз етеді, тек уәкілетті пайдаланушылар үшін кіру мүмкіндігін шектейді. Аутентификация құпия сөзді, биометриялық деректерді немесе басқа идентификаторларды енгізуді талап ету арқылы пайдаланушының түпнұсқалығын растайды, ал авторизация пайдаланушының құқықтарына байланысты деректерге қол жеткізу деңгейін анықтайды. Осы әдістердің тіркесімі рұқсат етілмеген қол жетімділікке байланысты ақпараттың ағып кету қаупін айтарлықтай азайтуға мүмкіндік береді.

Брандмауэрлер корпоративті желіні рұқсат етілмеген сыртқы қол жетімділіктен қорғауға қызмет етеді, бұл компанияның ішкі желісі мен сыртқы Интернет арасында кедергі жасайды. Брандмауэр Құрылғы мен желі арасындағы немесе екі желі арасындағы трафикті тексереді. Мысалы, корпоративтік желі және интернет(Сурет 2). Олар Ықтимал қауіпті қосылымдарды блоктайды және зиянды бағдарламалардың енуіне жол бермейді. Интрузияны анықтау жүйелері (IDS) желідегі күдікті әрекеттерді анықтауға және оқиғаларға тез жауап беруге мүмкіндік береді. IDS желілік трафикті талдайды және ауытқуларды анықтайды, бұл хакерлік әрекеттер мен шабуылдарды ерте анықтауға көмектеседі.

Бұл қауіпсіздік әдістері мен технологиялары ағып кету және кибершабуылдар қаупімен байланысты тәуекелдерді азайту арқылы жан-жақты қорғаныс жасайды. Бұл құралдарды біріктіру ұйымдарға барлық деңгейдегі деректердің қауіпсіздігін қамтамасыз ететін көп деңгейлі қорғаныс жүйесін құруға мүмкіндік береді.



Сурет 2. Брандмауэрдің жұмыс принципі

Деректер қауіпсіздігінің нормативтік актілері мен стандарттары

Деректерді қорғаудың жоғары дәрежесін қамтамасыз ету үшін компаниялар заңнамалық талаптар мен салалық стандарттарды сақтауы керек. Деректер қауіпсіздігі саласындағы ең маңызды халықаралық стандарттар ISO/IEC 27001, GDPR (деректерді қорғаудың жалпы ережесі) және HIPAA (АҚШ-тың медициналық сақтандырудың портативтілігі және есеп беру туралы Заңы) болып табылады. Бұл стандарттар мен стандарттар ақпараттық қауіпсіздікті басқаруға және жеке деректерді қорғауға қойылатын талаптарды белгілейді.

ISO/IEC 27001-ақпараттық қауіпсіздікті басқару жүйесіне (SWIB) қойылатын талаптарды анықтайтын халықаралық стандарт. Бұл стандарт ұйымдарға ақпараттық қауіпсіздік тәуекелдерін анықтауға, басқаруға және азайтуға мүмкіндік беретін құрылым құруға көмектеседі. ISO 27001 сертификатталған компаниялар деректер қауіпсіздігінің жоғары стандарттарына және ақпаратты қорғауға деген ұмтылыстарын көрсетеді.

Сурет 3. GDPR деректерді қорғау принциптері

GDPR-ЕО азаматтарының дербес деректерін өңдеу мен сақтауды реттейтін еуропалық нормативтік акт. Оның басты мақсаты — пайдаланушылардың жеке ақпаратын бақылау құқығын қорғау және олардың деректерімен жұмыс істеудің ашықтығын қамтамасыз ету. GDPR талаптарын бұзу ауыр айыппұлдарға әкелуі мүмкін, бұл компанияларды деректерді қорғау жүйелерін жақсартуға инвестиция салуға итермелейді (Сурет 3).

HIPAA Денсаулық сақтау деректерін қорғауға арналған және денсаулық сақтау ұйымдарына, денсаулық сақтау мекемелеріне және олардың АҚШ серіктестеріне таралады. Ол пациенттердің жеке ақпаратын қорғауды қамтамасыз ете отырып, құпиялылық пен қауіпсіздікке қатаң талаптар қояды. Деректердің бұзылуын болдырмау және пациенттердің жеке өмірін қорғау үшін HIPAA-ны сақтау қажет.

GDPR және HIPAA — деректерді қорғауды реттеудің жоғары стандарттарының мысалдары. Олардың талаптарын орындау киберқауіптер мен ағып кету ықтималдығын азайтып қана қоймайды, сонымен қатар компанияның сенімділігі мен құпия ақпаратты қорғау қабілетін қамтамасыз етеді. Қаржыдан денсаулық сақтауға дейінгі әртүрлі салалардағы компаниялар үшін осы стандарттарға сәйкестік тұтынушылар мен серіктестердің сенімін арттыратын және ықтимал заңды салдардан қорғайтын деректерді басқарудың маңызды аспектісіне айналады.

Осы стандарттар мен ережелерді сақтау ұйымдарға құқықтық тәуекелдерді азайтуға, деректер қауіпсіздігінің жоғары деңгейін және клиенттер мен серіктестердің сенімін қамтамасыз етуге мүмкіндік береді.

Деректерді қорғау жүйелерін енгізудің артықшылықтары мен қиындықтары

Деректерді қорғау ұйымдарға көптеген артықшылықтар береді, соның ішінде қауіпсіздік деңгейін арттыру, операциялық тәуекелдерді азайту және тұтынушылар мен серіктестердің сенімін жақсарту. Деректерді қорғаудың басты артықшылығы-ұйымды ықтимал қаржылық шығындар мен беделді тәуекелдерден қорғайтын ағып кету мен кибершабуылдардың ықтималдығын азайту. Деректерді қорғау жүйелеріне инвестиция салатын компаниялар өздерінің Ақпараттық активтері сенімді қорғалғанын біле отырып, нарықта сенімдірек жұмыс істей алады.

Дегенмен, деректерді қорғау жүйелерін енгізу қоңыраулармен де байланысты. Жоғары шығындар негізгі кедергілердің бірі болып табылады: компаниялар технологиялар мен қызметкерлерді оқытуға көп қаражат жұмсауға мәжбүр. Бұл, әсіресе, кешенді қорғауды қамтамасыз ету үшін ресурстар жетіспеуі мүмкін шағын және орта кәсіпорындарға қатысты. Сонымен қатар, қазіргі заманғы қорғаныс әдістері үнемі жаңартуды және бейімделуді қажет етеді, өйткені шабуылдаушылар үнемі бұзудың жаңа тәсілдерін табады.

Басқарудың күрделілігінің артуы компаниялар үшін де қиындық тудырады, өйткені көп деңгейлі қорғауды енгізу көп күш жұмсауды қажет етеді және ішкі процестерді қиындатуы мүмкін. Мысалы, ережелерді сақтау қосымша тексерулер мен құжаттамаға қойылатын талаптарға әкелуі мүмкін, бұл АТ бөліміне жүктемені арттырады.

Осы қиындықтарға қарамастан, деректерді қорғау жүйелерін енгізудің пайдасы айтарлықтай басым. Деректерді қорғау компанияларға тәуекелдерді азайтуға, ұзақ мерзімді қауіпсіздік пен сенімділікті қамтамасыз етуге мүмкіндік береді, бұл сайып келгенде олардың нарықтағы бәсекелестік позицияларын нығайтады.

Деректерді қорғаудың болашағы: трендтер мен технологиялар

Технологиялық прогресс деректерді қорғау тәсілдерін Өзгертуді жалғастыруда, бұл оны бейімделгіш және белсенді етеді. Деректер көлемінің ұлғаюы және ақпараттық жүйелердің күрделілігі жағдайында жасанды

интеллект (AI), Машиналық оқыту (МО), кванттық шифрлау және блокчейн сияқты технологиялар маңызды рөл атқара бастайды. Бұл технологиялар деректерді қорғаудың тиімділігін арттыруға, ықтимал қауіптерді болжауға және ақпараттың жоғары деңгейде ағып кетуіне жол бермеуге көмектеседі.

Жасанды интеллект және машиналық оқыту ауытқулар мен ықтимал қауіптерді анықтау үшін үлкен көлемдегі деректерді талдауға мүмкіндік береді. Мысалы, AI желілік трафикті талдауға және бұзу әрекеттерінен туындауы мүмкін әдеттен тыс әрекеттерді түсіруге қабілетті. Бұл деректерді қорғаудың белсенді тәсілін қамтамасыз ете отырып, оларды жүзеге асырмас бұрын қауіптерді анықтауға мүмкіндік береді. Сондай-ақ, Машиналық оқыту күдікті әрекеттерді анықтаудың дәл алгоритмдерін жасауға көмектеседі, шабуылдарды анықтау процесін жақсартады және ықтимал шабуылдардың алдын алады.

Кванттық шифрлау өзінің ерекше қасиеттеріне байланысты деректер қауіпсіздігі саласында төңкеріс жасауға уәде береді. Қуатты компьютерлерге осал болуы мүмкін классикалық шифрлау әдістерінен айырмашылығы, кванттық шифрлау кванттық физика принциптеріне негізделген, оны бұзу мүмкін емес. Бұл болашақта деректерді қорғаудағы маңызды қадам болуы мүмкін, әсіресе кванттық есептеулер қол жетімді бола бастаған жағдайда.

Блокчейн деректерді қорғау саласында да қолданылады. Бұзуға төзімділігімен танымал бұл технология ақпаратты рұқсатсыз кіруден қорғалған орталықтандырылмаған дерекқорда сақтауға мүмкіндік береді. Мысалы, блокчейн медициналық деректер мен қаржылық операцияларды қорғау үшін қолданылады, мұнда ақпараттың тұтастығын сақтау және манипуляциядан аулақ болу өте маңызды.

Назар аударатын басқа технологиялардың қатарына биометриялық аутентификация және пайдаланушылардың мінез-құлқын талдау (UBA, user Behavior Analytics) жатады. Бетті немесе саусақ ізін тану сияқты Биометрия парольдердің бұзылу қаупін азайтады, аутентификацияны қауіпсіз етеді. UBA пайдаланушылардың әрекеттеріндегі ауытқуларды анықтау үшін мінез-құлық үлгілерін пайдаланады, бұл инсайдерлік шабуыл немесе қызметкерлердің кездейсоқ қателіктері сияқты ішкі қауіптерді анықтауға көмектеседі.

Болашақтың негізгі тенденциялары сонымен қатар ұйымдарға стандарттарға сәйкес келуге және тәуекелдерді басқаруға көмектесетін сәйкестік жүйелерін дамытуды күшейтуді қамтиды. Цифрлық қауіптердің күшеюімен әлемдік үкіметтер мен реттеушілер компаниялардан деректерді қорғауға неғұрлым байыпты көзқарасты талап ете отырып, қауіпсіздіктің жаңа стандарттарын енгізуде. Бұл стандарттар ұйымдар үшін тәуекелдерді азайтып қана қоймайды, сонымен қатар клиенттердің сенімін арттырады, бұл әсіресе киберқауіптер дәуірінде маңызды.

Қорытынды

Деректерді қорғау-қауіптер мен осалдықтарды анықтаудан бастап заманауи технологияларды енгізуге және сәйкестікке дейінгі көптеген аспектілерді

қамтитын күрделі және көп қабатты тапсырма. Деректер қауіпсіздігіне кешенді көзқарас компанияларға өз ақпаратын ықтимал қауіптерден қорғауға ғана емес, сонымен қатар тұтынушылардың сенімін арттыруға, беделін жақсартуға және нарықта бәсекелестік артықшылықтар жасауға мүмкіндік береді.

AI, блокчейн және кванттық шифрлау сияқты технологиялар деректерді қорғау деңгейін жақсартуда маңызды рөл атқарады. Заманауи әдістер ұйымдарға ағып кету мен кибершабуылдармен байланысты тәуекелдерді азайтуға, сондай-ақ ресурстарды тиімдірек басқаруға мүмкіндік береді. Алайда, технологиялық аспектілерден басқа, ақпараттық қауіпсіздік мәдениетін дамыту және компанияның жоғары стандарттарға адалдығы маңызды.

Деректерді қорғау міндеттері күрделене түсуде және компаниялар жаңа қауіптер мен талаптарға сай болу үшін өз тәсілдерін үнемі бейімдеуі керек. Цифрлық технологиялардың қарқынды дамуы және киберқауіптердің артуы жағдайында деректерді қорғауды тәуекелдерді азайтуға ғана емес, сонымен қатар компанияның тұрақты өсуіне ықпал ететін бизнес үшін маңызды басымдықтардың бірі ретінде қарастыруға болады.

Бақылау сұрақтары:

1. Қауіпсиздік және деректерді қорғау дегеніміз не және оның негізгі принциптері қандай?
2. Құпиялылық, тұтастық және қолжетімділік (триадасы ЦРУ) принциптерін түсіндіріңіз.
3. Деректердің қауіпсіздігін қамтамасыз ету үшін қандай шифрлау әдістері қолданылады?
4. Аутентификация және авторизация процестерінің айырмашылықтарын түсіндіріңіз.
5. DDoS (распределенный отказ в обслуживании) шабуылдарының алдын алу үшін қандай қауіпсіздік шаралары қабылданады?

Ұсынылған әдебиеттер:

Негізгі әдебиеттер:

1. Абдрахманов, М. В. Основы защиты информации в информационных системах. М.: Юрайт, 2020.
2. Бейкер, У. Г. Защита данных и конфиденциальность. СПб.: Питер, 2021.
3. Федеральная служба по техническому и экспортному контролю. Требования к обеспечению безопасности данных. Москва: ФСТЭК, 2019.
4. European Commission. General Data Protection Regulation (GDPR). Brussels: European Union, 2018.
5. National Institute of Standards and Technology. Guide to Protecting the Confidentiality of Personally Identifiable Information. Gaithersburg: NIST, 2021.

Қосымша әдебиеттер:

6. United States Department of Health and Human Services. Health Insurance Portability and Accountability Act (HIPAA). Washington, D.C.: HHS, 1996.

7. SANS Institute. Data Security Essentials: Practical Solutions for Small and Medium Businesses. Bethesda: SANS, 2020.
8. Brown, S., & Davis, P. Data Protection and Privacy for Cloud Services. London: Routledge, 2019.
9. Choudhury, A. Data Security and Protection: Standards and Best Practices. New York: McGraw-Hill, 2018.
10. Sweeney, L. & Minor, M. "An Overview of Key Data Security Regulations and Compliance." Journal of Cyber Security, 2021.