ОӘЖ 004.056.53

БҰЛТТЫҚ СЕРВИСТЕРДІҢ ҚАУІПСІЗДІГІ

Аманбаева Айжан Жанатовна
amanbaeva.aizhana@mail.ru
Л.Н.Гумилев атындағы ЕҰУ ақпараттық технологиялар факультетінің
7М06111-Ақпараттық қауіпсіздіктің әдістері мен технологиялары білім беру бағдарламасы
бойынша 2-курс магистранты, Нұр-Сұлтан, Қазақстан
Ғылыми жетекші – Разахова Бибигүл Шамшановна

Бұлттық сервистер мен өнімдер төрт негізгі деңгейдің инфрақұрылымына негізделген: аппараттық (физикалық бөліктер, яғни серверлер мен желілік компоненттер), программалық жасақтама (мысалы, операциялық жүйелер), виртуализация ресурстары (есептеу ресурстарын біріктіру және бөлісу) және қосымшалар (мысалы, Salesforce.com және Google Apps). Сервис

әзірлеушісі бұлттық тұтынушы да, бұлт провайдері де пайдалану үшін бұлттық қосымшалар мен сервистерді жасайды, жариялайды және бақылайды [1].

McAfee 2020 жылы жүргізген зерттеуге сәйкес, бұлттық қауіпсіздік қатерлері мен кибершабуылдардың саны артып келеді. 2020 жылдың қаңтарынан сәуіріне дейін бұлттық шоттарға шабуылдар саны 630% - ға өсті. Бұл жағдайда резонанстық бұзылулардың көпшілігі провайдер емес, пайдаланушының қателігінен болады.

Бұлтты енгізудің басынан бастап ұйымдар өз қызметкерлері үшін провайдердің жауапкершілік саласы қай жерде аяқталатынын анықтауы керек. Тапсырыс берушілер қызметкерлердің бұлтпен және онымен байланысты кез-келген құралдармен және қызметтермен жұмыс істеуге мұқият дайындалғандығына көз жеткізуі керек.

Сарапшылардың бағалауы бойынша, 2022 жылға дейін бұлт қауіпсіздігінің кем дегенде 95% - ы клиенттердің қателіктерінен болады. Сондықтан бұлттағы бірлескен жауапкершілік моделінің айналасындағы шатасуды жою бұрынғыдан да маңызды [2].

Бұлттық провайдерлер қауіпсіздікті жақсарту үшін үнемі инновациялық шешімдерге қаражат салады. Бірақ клиенттер артта қалмауы керек. Орналастыру түрлеріне байланысты жауапкершілікте айқын айырмашылықтар болса да, негізгі стратегия өзгеріссіз қалады: клиенттер үшін құрылғылар арасындағы өзара әрекеттесуді визуализациялау, нақты уақыт режимінде қауіпсіздіктің ықтимал қауіптерін анықтау және оларды уақытында жою маңызды.

Интернет-сервистердің негізгі осалдығы тек қана парольдік аутентификацияны пайдалану және ұмытылған аутентификациялық деректерді — логиндер мен парольдерді (ең алдымен — электрондық пошта арқылы) қалпына келтірудің әбден сенімді емес тәсілдерін қолдану болып табылады. Егер пайдаланушы бұлттық қызмет провайдеріне сенбесе немесе бұлттағы қосымша ақпаратты қорғауды қамтамасыз еткісі келсе, онда ол бұлттағы деректерді шифрлауды қолдана алады. Қорғаудың бұл әдісі, егер пайдаланушы бұлттағы ақпаратты өңдеуді жоспарламаса (мысалы, фотосуретті немесе мәтінді өңдеу), тек деректерді бастапқы түрінде сақтап, жіберсе ғана мүмкін болады. Бұл жағдайда криптографиялық кілттерді бөлу және басқарудағы қиындықтарды (әсіресе ірі ұйымдар үшін) және мобильділіктің жоғалуын ескеру қажет (деректерге қол жеткізу үшін пайдаланушының құрылғысында қауіпсіз түрде сақталатын нақты криптографиялық кілт болуы керек және техникалық немесе технологиялық проблемалар туындауы мүмкін) [3].

Құпия ақпаратты, оның ішінде жеке деректерді сақтау үшін бұлттық сервистерді пайдалануды азайту немесе оларды криптографиялық қорғаудың тұрақты әдісімен шифрланған түрде орналастырған жөн. Пайдаланушылар көбінесе жеке құжаттарды іздеу қызметтері индекстейтін бұлтты қоймаларға уақытша сақтауға орналастырады, бұл оларды зиянкестер үшін қол жетімді етеді. Ақпаратты криптографиялық қорғаудың көптеген ақысыз құралдары бар: PGP, парольмен және файл атауларын шифрлайтын RAR мұрағаттары. Соңғысы - ең қолайлы нұсқа, бүкіл әлем бойынша миллиондаған пайдаланушылар мұрағаттарды пайдаланады, сондықтан барлық адамдар арасында, тіпті парольмен де ақпаратты бөлу өте қиын болады [4].

Пайдаланушы деректерді қандай бұлтты сақтау керек екенін өзі шешеді. Сонымен қатар, ол әр түрлі бұлттық сервистердің қауіпсіздік рейтингін мұқият зерделеуі керек. Мысалы, бірінші кестеде TopTenReview материалдары мен Falcongaze аналитикалық орталығының зерттеулеріне негізделген бұлтты деректер қоймаларының қауіпсіздік рейтингі көрсетілген.

Кесте 1. TopTenReview материалдары мен Falcongaze аналитикалық орталығының зерттеулеріне негізделген бұлтты деректерді сақтау қауіпсіздігінің рейтингі.

		Шифрлау деңгейі	SSH	Жеке шифрлау кілті	Екі деңгейлі аутентификация

1	IDrive	256-бит AES	256-бит	Ия	Жоқ
2	Google Drive	128-бит AES	256-бит	Жоқ	Ия
3	SpiderOakONE	256-бит AES	256-бит	Ия	Жоқ
4	iCloud Drive	128-бит AES	128-бит	Жоқ	Ия
5	Dropbox	256-бит AES	128-бит	Жоқ	Ия
6	Yandex.Диск	256-бит AES	128-бит	Жоқ	Ия

Бұл мақалада ең танымал бес қызмет қарастырылған: Dropbox, Яндекс.Диск, Google Drive, iCloud, OneDrive. Көптеген бәсекелестер сияқты, Dropbox клиенттердің деректерін сервер жағында шифрлайды, бірақ программаның клиенттік бөлігінде шифрлаудан бас тартады. Сондай-ақ, компанияның серверлерінен файлдарды ағынмен жіберу әрдайым шифрланбайды. Осылайша, файлдарды серверге жүктеу және жүктеу кезінде деректердің бұзылуы мүмкін. Сонымен қатар, Dropbox-та қауіпсіздік оқиғаларының әсерлі тарихы бар. Мысалы, 2016 жылы деректер базасын сату жағдайы-68 млн пайдаланушы туралы 5 Гб жазба. Оқиға туралы ақпарат баспасөзге түскеннен кейін, Dropbox деректердің ағып жатқанын мойындады, бірақ пайдаланушылардың есептік жазбаларына заңсыз кірудің іздері табылған жоқ деп мәлімдеді. Жоғарыда аталған мәселелерге байланысты Dropbox - бұл ең сенімді емес қызмет. Негізгі нұсқадан басқа, Dropbox-та бизнес үшін деректер жоспары бар. Ол деректерді беру кезінде және қосымшаларда қосымша шифрлауды, шифрланған блоктар түрінде мазмұнды файлдарды сақтауды, сондай-ақ метадеректер мен деректер блоктарын бөлек сақтауды қамтамасыз етеді [5].

Ең танымал отандық сақтау қызметтерінің бірі - Яндекс.Диск Dropbox-қа қарағанда біршама сенімді. Оған Яндекстің басқа қызметтерімен интеграция енгізілген, сонымен қатар пин-кодты, QR-кодты және TouchID-ті қолдана отырып, екі факторлы аутентификация бар. Жүктеу кезінде файлдар вирустарға тексеріліп, деректер шифрланған арна арқылы жіберіледі. Бұлтты қызметке қатысты мәселелер де болды. Мысалы, күлкілі қате 2013 жылы табылды. Клиентті жаңарту немесе жою кезінде, Яндекс.Диск Windows жүйелік қалталарын түбірлік каталогқа дейін жойды. Өтемақы ретінде компания пайдаланушыларға 200 Гб тұрақты емес нұсқасын ұсынды.

Келесі бұлттық сервис - Google Drive. Онда екі факторлы аутентификация бар, есептік жазбаны қалпына келтіру құпия сұрақ арқылы жүзеге асырылады, қызметтің өзі пайдаланушы ойлап тапқан парольді сенімділік үшін тексереді және оңай бұзылатын парольдерді пайдалануға рұқсат бермейді. Деректер беру кезінде шифрланады, бұл жүктеу кезінде олардың бұзылуын болдырмайды, бірақ сервердегі деректерді шифрлау үшін үшінші тарап бағдарламалары қажет болады. Google Drive-да файлдарды қорғаудың жоғары деңгейін қамтамасыз етуге мүмкіндік беретін бизнес-аккаунттардың нұсқасы бар. Онда, мысалы, жарнаманы көрсету үшін берілетін ақпаратты талдау жоқ және бірыңғай кіру жүйесі, электрондық поштаны қорғау ережелері, мысалы, TLS протоколын мәжбүрлеп қосу, сондай-ақ IRM және DLP технологиялары бар. Алайда, 2018 жылдың шілдесінде болған жағдай болды. Файлдарды "бөлісу" арқылы пайдаланушылар "сілтеме арқылы қол жеткізуді" деген сілтемені таңдады, бұл құжат тек мекен-жаймен бөліскен әріптестерде ашылады деп сенді. Алайда, іздеу жүйелері мұндай файлдарды индекстей алатындығы белгілі болды.

Apple техникасын пайдаланушылар үшін iCloud Drive бұлттық сақтау орны бар. Бұл сервиске байланысты бұлттық сақтау тарихындағы ең үлкен жанжалдардың бірі болды. 2014 жылы iCloud-та аккаунттардың жаппай бұзылуы болды, нәтижесінде көптеген пайдаланушылардың жеке деректері желіге қосылды. 2016 жылы тағы бір көрнекі жағдай болды - "Iphone табу" функциясы арқылы 40 миллион шотты ұрлау, оларды кейіннен бұғаттау және ақшаны бопсалау үшін пайдалану. Осы оқиғалардан кейін, Apple қызмет қауіпсіздігін жақсартуға байсалды кірісті - қазір iCloud Drive-дағы деректер беру кезінде де, серверде де шифрланады, пароль сенімділікке тексеріледі, екі факторлы аутентификация бар. Жоғарыда айтылғандарды ескере отырып, Apple бұлтты сақтау осы кезеңде өте сенімді болып табылады [6].

Кеңсе өнімдерінің танымалдылығының арқасында Microsoft осы OneDrive компаниясының бұлттық сервисіне ие болды. Өнімнің негізгі нұсқасы клиент пен сервер арасында берілетін деректерді шифрлауды, сондай-ақ екі факторлы авторизацияны қамтамасыз етеді; сонымен қатар, Microsoft тіркелгісінің паролі сенімділікке тексеріледі. OneDrive бизнес нұсқасы жақсартылған қауіпсіздік мүмкіндіктеріне ие. Онда "деректер орталығының физикалық қауіпсіздігі, желілік қауіпсіздік, қол жетімділік қауіпсіздігі, қосымшалар мен деректер қауіпсіздігі"қамтамасыз етіледі. Бизнес нұсқасында қолданылатын сақтау түрлері-шифрланған мазмұнды сақтау, мазмұн дерекқоры және кілт қоймасы — физикалық түрде бөлінген, сондықтан олардың кез-келгені бұзылған кезде ақпаратты бұзуға болмайды. Мұның бәрі OneDrive-ны қарастырылған қоймалардың ішіндегі ең қауіпсіз етеді. Алайда, OneDrive-да сақталған деректер Microsoft тарапынан бақыланады. Microsoft корпорациясының мінез-құлық кодексін бұзды деп күдіктенген кез-келген мазмұн жойылады және есептік жазба бұғатталуы мүмкін. Бұл ұстаным OneDrive-да сақталған деректердің құпиялылығына күмән тудырды. Компания ішкі қауіпсіздіктің қатаң саясаты бар деп мәлімдегенімен, тексеру арнайы бағдарламалық алгоритмдер арқылы жүзеге асырылады [7].

Сонымен, жоғарыда келтірілген мәліметтер бойынша бұлттық сақтаудың негізгі мәселелерін бөліп көрсетуге болады:

- Деректерді сақтау және қайта жіберу қауіпсіздігі "бұлтпен" жұмыс істеу кезінде, әсіресе құпия және жеке деректерге қатысты негізгі мәселелердің бірі болып табылады. Мысалы, провайдер клиенттің деректерін (егер олар парольмен қорғалмаса) көре алады, олар провайдердің қорғаныс жүйелерін бұзған хакерлердің қолына түсуі мүмкін.
- "Бұлтта" деректердің сенімділігі, уақтылы алынуы және қол жетімділігі көптеген аралық параметрлерге байланысты, мысалы: клиенттен "бұлтқа" жолдағы деректерді беру арналары, соңғы мильдің сенімділігі, клиенттің интернет-провайдерінің жұмыс сапасы, қазіргі уақытта "бұлттың" қол жетімділігі. Егер онлайн сақтауды ұсынатын компанияның өзі жойылса, клиент барлық деректерін жоғалтуы мүмкін.
- "Бұлттағы" деректермен жұмыс істеудің жалпы өнімділігі жергілікті деректердің көшірмелерімен жұмыс істегенге қарағанда төмен болуы мүмкін.
- Қосымша мүмкіндіктер үшін абоненттік төлем (деректерді сақтаудың жоғарылауы, үлкен файлдарды жіберу және т.б.). Бұлтты сақтаудың көптеген кемшіліктері бар, бірақ сонымен бірге артықшылықтар аз емес. Жеке деректерге "бұлттарға" сену-бұл әр пайдаланушы үшін жеке мәселе. Бұл қызметтерді ұсынатын компаниялар жыл сайын өз қоймаларының қауіпсіздігін арттыруға тырысады. Олар жаңа пайдаланушыларға қызығушылық танытады, ал олар өз кезегінде құпиялылықты қажет етеді, сондықтан жеке деректерді қорғау дәрежесі артады [8].

Қолданылған әдебиеттер тізімі

1. Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2012). A survey on security issues and solutions at different layers of Cloud computing. The Journal of Supercomputing, Vol. 63, Issue 2, pp. 561–592.

2. Разделение ответственности за обеспечение безопасности в облаке защиты [Электронды ресурс]. — URL: https://www.cloud4y.ru/blog/razdelenie-otvetstvennosti-za-obespechenie-bezopasnosti-v-oblake/
3. Kuyoro S. O., Ibikunle, F., and Awodele, O. (2011). Cloud Computing Security Issues and Challenges. International Journal of Computer Networks (IJCN), Vol. 3, Issue 5, pp. 247-255.
4. Gonzalez, N., Miers, C., Redígolo, F., Simplício, M., Carvalho, T., Näslund, M., and Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 2012 1:11. DOI: 10.1186/2192-113X-1-11
5. Ramachandran, M. (2015). Software security requirements management as an emerging cloud computing service. International Journal of Information Management, Vol. 36, Issue 4, pp. 580-590
6. M. Carroll, et al., "Secure Virtualization: Benefits, Risks and Controls," presented at the CLOSER 2011: The 1st International Conference on Cloud Computing and Services Science, Noordwijkerhout, The Netherlands, 2011.
7. Sharma, R. & Trivedi, R. K. (2014). Literature review: Cloud Computing –Security Issues, Solution and Technologies. International Journal of Engineering Research, Vol. 3, Issue 4, pp. 221-225.
8. Heiser J. What you need to know about cloud computing security and compliance, Gartner, Research, ID Number: G00168345, 2009.