ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

4. Verizon Data Breach Investigations Report, 2021. URL: https://enterprise.verizon.com/resources/reports/dbir/
5. S. L. Pfleeger. Security in Computing. - Prentice Hall, 2006. - 845 с. - ISBN 978-0132390774.
6. What is Vulnerability Management? // Tenable, URL: https://www.tenable.com/solutions/vulnerability-management
7. R. Cellan-Jones. Massive ransomware infection hits computer in 99 countries // BBC News. 2017. URL: https://www.bbc.com/news/technology-39901382
8. D. Lee. Apple rushes to fix major password bug // BBC News, 2017. URL: https://www.bbc.com/news/technology-42161823

ӘОЖ 004

БҰЛТТЫ ҚОЙМАДАҒЫ ҚАУІПСІЗДІК: БҰЛТТАҒЫ ДЕРЕКТЕР МЕН ҚОЛДАНБАЛАРДЫ ҚАУІПСІЗ САҚТАУ

Исабай Темірлан Бақытбекұлы
isabayev14@mail.ru
Ақпараттық қауіпсіздік жүйелері мамандығының Л.Н.Гумилев атындағы ЕҰУ студенті, Астана, Қазақстан
Ғылыми жетекші – Е.Қайупов

Бұлтты қойма - бұл деректерді жергілікті құрылғыда сақтаудың орнына провайдердің серверлерінде қашықтағы жерде сақтауға мүмкіндік беретін қызмет болып табылады. Бұлтты қойма пайдаланушыға желіге қосылған кез келген құрылғы арқылы деректерді интернет арқылы сақтауға, синхрондауға және бөлісуге мүмкіндік береді. Бұлтты қойманың әртүрлі түрлері Google Drive, Dropbox, OneDrive, iCloud және тағы басқалары болады. Бұлтты қойманың басты артықшылықтары:

- кез-келген құрылғыдан және интернетке қол жетімді әлемнің кез-келген нүктесінен деректерге қол жеткізу мүмкіндігі;
- деректерді бірнеше құрылғылар арасында синхрондау мүмкіндігі;
- құжаттар мен жобаларды басқа пайдаланушылармен бірлесіп жұмыс істеудің ыңғайлы тәсілі;
- жергілікті құрылғы істен шыққан жағдайда деректерді жоғалтудан қорғау;
- деректердің автоматты сақтық көшірмесі;

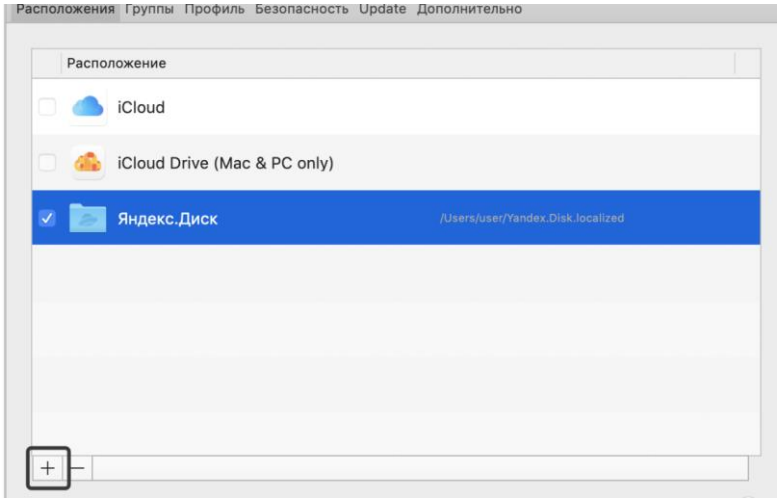
Сондай-ақ, бұлтты қоймада деректер қашықтан сақталады. Бұлтты қойманы пайдаланудың кемшіліктері:

- деректерге қол жеткізу үшін интернетке кіру қажеттілігі;
- бұлтты қоймаға рұқсатсыз кіру жағдайында деректердің бұзылуы және құпиялылықтың бұзылу қаупі;
- бұлтты қойма провайдерінің серверіне кіру проблемалары туындаған жағдайда деректерге қол жеткізуді шектеуж
- деректерді қорғауды шектеулі бақылау, өйткені бұлтты қойма провайдерінің міндеті;
- деректерді сақтаудың үлкен көлемі қажет болған жағдайда бұлтты қойма пайдаланудың жоғары құны.

Бұлтты қойма қауіпсіздігі - бұлтты есептеу жүйелерін қорғауға арналған киберқауіпсіздік бөлімі. Бұған барлық желілік инфрақұрылым нысандарында, онлайн қолданбалар мен платформаларда құпиялылық пен деректерді қорғау кіреді. Бұлтқа негізделген провайдерлер де, жеке тұлғалар, шағын және орта бизнес немесе корпорациялар болсын, пайдаланушылар да атсалысуы керек болып табылады. Бұлтты қойма қызметтері тұрақты Интернет байланысы бар серверлерде орналастырылады. Сондықтан бұлтта сақталған жеке деректердің қол

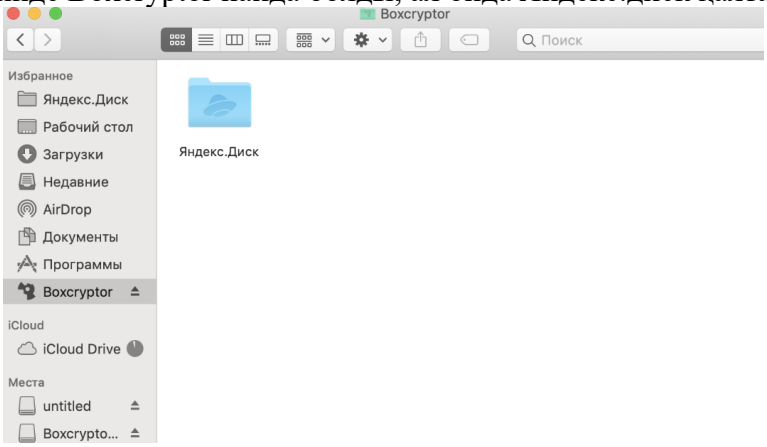
сұғылмаушылығын қамтамасыз ету олардың мүддесі үшін, жеткізушілер пайдаланушылардың сеніміне арқа сүйейді. Дегенмен, бұлттық қойманың қауіпсіздігі пайдаланушылардың қолында деуге болады. Сенімді қорғаныс үшін екі тараптың да өз жауапкершіліктерін түсінулері өте маңызды болып табылады. Бұлтты қойманы пайдалану кезінде сақталған деректердің қауіпсіздігін қамтамасыз ету маңызды. Өйткені, шабуылдаушылар мен киберқылмыскерлер бұлт қоймасында деректеріңізге рұқсатсыз қол жеткізуге тырысуы мүмкін. Бұлтты сақтаудың қауіпсіздігін қамтамасыз ету үшін пайдаланушылар қабылдай алатын әртүрлі қауіпсіздік шаралары бар. Бұл шаралар күшті құпия сөздерді және екі факторлы аутентификацияны пайдалануды, деректердің сақтық көшірмесін жасауды, қауіпсіздікті тексеруді және үнемі жаңартуды, желі қауіпсіздігін қамтамасыз етуді, тек қажетті пайдаланушыларға қол жеткізуді шектеп және тиісті кіру құқықтарын реттеуді қамтиды.Олардың орындалу ретін практикалық негізде көрсететін түрлері де бар. Олар:

Деректерді шифрлау - рұқсатсыз кіруден қорғауға көмектеседі. Шифрлауға көмектесетін құралдар, мысалы,VeraCrypt, Mega, Boxcryptor деген секілді түрлері бар. Шифрлау үшін мысалы, Boxcryptor -ды қолданайық. Ол TrueCrypt-ке ұқсас шифрлауды қолданады, құрылғыдағы деректерді шифрлайды, содан кейін оны шифрланған түрде бұлтқа жібереді. Бұлтта сенімді шифрланған файлдар жатыр, сондықтан үшінші тараптың бұлтына кіру, мейлі ол шабуылдаушы болсын немесе ресми сұрау арқылы деректерді алған құқық қорғау органдарының өкілі болсын, оған файл мазмұнына қол жеткізуге мүмкіндік бермейді.



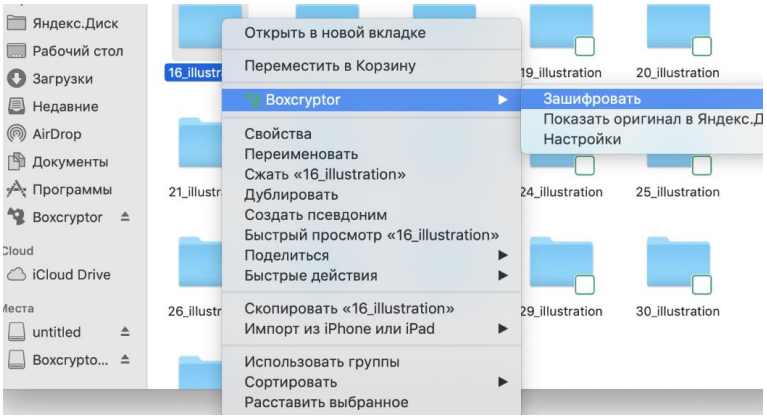
Сурет 1.Boxcryptor – ды қолдану барысының алғашқы қадамы – шифрлау дискін таңдау.

Дискілер тізімінде Boxcryptor пайда болды, ал онда Яндекс.диск қалтасы бар.



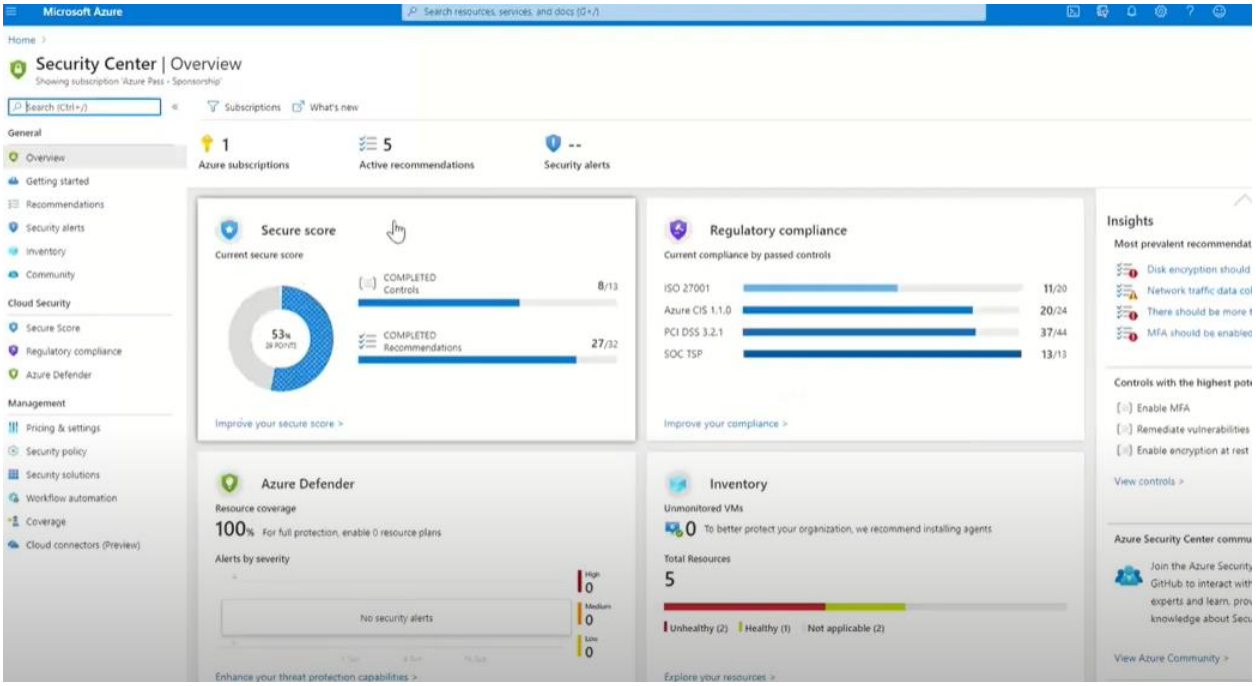
Сурет 2. Boxcryptor – ды қолдану барысының келесі қадамы.

Бұлттағы қалталар мен файлдарды шифрлау қажет болады.



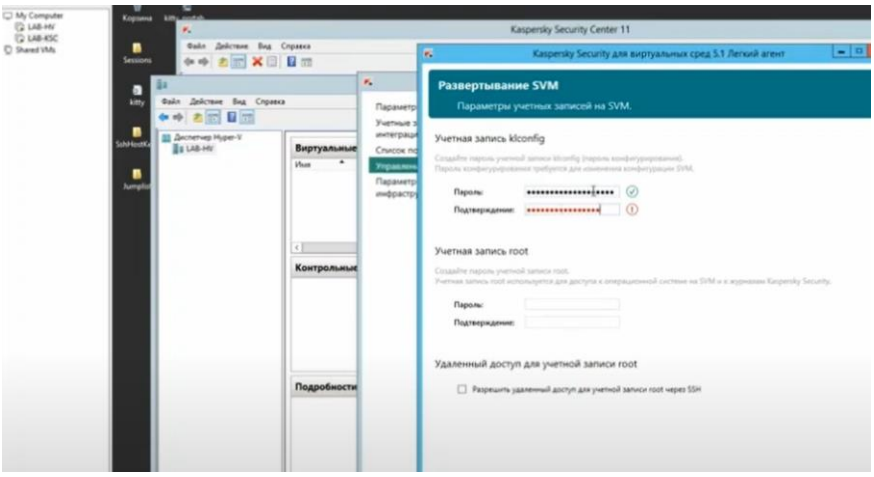
Сурет 3. Boxcryptor – ды қолданудағы шифрлау соңғы қадамы.

Қауіпсіздік мониторингін қолдану арқылы, біздің бақылауымыздан тыс әрекеттерді және ықтимал қауіпсіздік қауіптерін бақылау үшін бұлттағы деректер мен қолданбалардың қауіпсіздігін бақылап және тексере аламыз. Солардың бірі, Microsoft Azure Security Center – ол бұлт ресурстарының қауіпсіздігін бақылауды, қауіптерді анықтауды және алдын алуды және осалдықтарды басқаруды қамтамасыз ететін Microsoft Azure қауіпсіздік қызметі, жоғары деңгейлі қауіпсіздік көмегін ұсына алады.



Сурет 4. Microsoft Azure қауіпсіздікті бақылау орталығы

Виртуалды ортада деректерді бұлтты қорғауға арналған шешімдер: Trend Micro Deep Security,Виртуалды және бұлтты орталарға арналған Kaspersky Security,ESET Virtualization Security,Vgate қауіпсіздік коды,CASB –Cloud access security broker,ForcepointCASB,Palo Alto Aperture деген сияқты түрлерін атап өтуге болады. Мысалы, Виртуалды және бұлтты орталарға арналған Kaspersky Security-бұл виртуалдандырылған инфрақұрылымдарды (серверлер, деректер орталықтары және жұмыс үстелі компьютерлері) зиянды кодтан қорғау жүйесі. Сонымен қатар, виртуалды орталарға арналған Kaspersky Security стандартты операцияларды орындауды жеңілдететін және қорғаныс мәселелерін бірден көрінетін бірыңғай басқару консолінен физикалық серверлерді, виртуалды машиналарды және мобильді құрылғыларды қоса алғанда, көптеген құрылғылардың қауіпсіздігін басқаруға мүмкіндік береді. Бұл жерде виртуалды машинада параметрлер бойынша жұмыс жасау негізі көрсетліген.



Сурет 5.Виртуалды машинада Kaspersky Security – ді жүйелеу процесі

Сонымен қатар, ақпаратты ұрлаудан немесе тыңдаудан қорғау үшін бұлқа қауіпсіз қосылу қажет болады. Ол үшін VPN және SSL сияқты қауіпсіз арналар арқылы қосылған кезде, егер мекен-жай "http://" орнына "https://" деп басталса, бұл SSL қосылымының белсенді екенін білдіреді. Сенімді бұлттық қызмет провайдерлерін пайдалану да деректерді қорғаудың жоғары деңгейін қамтамасыз етеді және ISO 27001, SOC 2 және тағы да басқа, сияқты қауіпсіздік сертификаты бар жақсы қауіпсіздік беделі бар бұлттық қызмет провайдерлерін таңдау өте маңызды болып табылады.

Қорытынды

Бұлтты қоймаданың қауіпсіздігін маңызға ала отыра, бұлттағы деректер мен қолданбаларды қалай қауіпсіз сақтауға болатындығы жайлы әртүрлі тәсілдері зерттелді және мән беретін дүниелер көрсетіліп өтті. Бұлтты қойманы пайдалану барысында, қауіпсіздікті тексеріп отыру және қорғау барсында жасауды талап ететін қадамдар аталып өтілді, ықтимал осалдықтарды анықтауға көмектесетін қол жетімді құралдарды қолдана отырып, қауіптердің алдын алу жолдары баян етілді. Осы қауіпсіздік шараларын сақтау бұлтты сақтауды шабуылдаушылардан және қылмыскерлерден қорғауға және деректеріңіздің сақталуын қамтамасыз етуге көмектеседі.

Қолданылған әдебиеттер тізімі

1. "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" by Tim Mather, Subra Kumaraswamy, and Shahed Latif, 106 с.

2. "Cloud Security: A Comprehensive Guide to Secure Cloud Computing" by Ronald L. Krutz and Russell Dean Vines, 1 с.,153 с.

3. Kaspersky Security Cloud | Адаптивная защита | Лаборатория Касперского

4. Azure Monitor — современные средства наблюдаемости | Microsoft Azure

ӘОЖ 004.896

ЖАСАНДЫ ИНТЕЛЛЕКТТІҢ ДАМУ ҚАРҚЫНЫНА ОРАЙ ҚАТЕРЛЕРІН ЕСКЕРУ

Искаков Ерасыл Кайратович
Iskakovk2016@gmail.com
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің, ақпарттық жүйелер кафедрасының 1-курс студенті, Астана, Қазақстан
Ғылыми жетекшісі –Таберхан Роман

Осыдан миллиондаған жыл бұрын Homo Sapiens, яғни саналы адам тарих сахнасына эволюция сатысымен көтерілген болатын, бірақ одан арғы эволюциялық өсуі өте ақырын