ISSN: 3030-3346

BULUTLI TIZIMLARDA ELEKTRON HUJJATLARNI HIMOYA QILISH USULLARI

Fayziyeva Dilsora Salimovna

Alfraganus universiteti, raqamli texnologiyalar kafedrasi dotsent v.b.
E-mail: dilsora.salimovna@gmail.com

KEYWORDS

bulutli texnologiyalar, hujum, autentifikatsiya, VPN.

ABSTRACT

Mazkur maqolada bulutli tizimlarda elektron hujjatlarni himoya qilish usullari batafsil yoritilgan bo'lib, bulutli xizmatlarga tahdidlarning beshta asosiy turi keltirilib, ularni bartaraf etish uchun himoya choralari ham belgilab berilgan.

Bulutli hisoblash xavfsizligi virtuallashtirilgan IP, ma'lumotlar bazalari, ilovalar, xizmatlar va bulutli hisoblash infratuzilmasini himoya qilish uchun foydalaniladigan siyosatlar, texnologiyalar, ilovalar va boshqaruv vositalarining keng to'plamini anglatadi. Bulutli tizimlarning xavfsizligini ta'minlash kompyuter xavfsizligi, tarmoq xavfsizligi va kengroq aytganda, axborot xavfsizligining bir qismidir.

Ma'lumotlarni himoya qilish bulutli hujjat tizimlari xavfsizligining eng muhim jihatlaridan biridir. Bulutli muhit xavfsizligini yaxshilash uchun korxonalar o'z ma'lumotlarini himoya qilish uchun zamonaviy texnologiyalar va ilg'or tajribalardan foydalanishlari kerak.

Bulutli xavfsizlik faqat to'g'ri xavfsizlik texnikasiga ega bo'linsa samarali bo'ladi. Bulutli EDMS arxitekturasi xavfsizlikni boshqarishda yuzaga keladigan muammolarni tan olishi kerak. Xavfsizlik boshqaruvi ushbu muammolarni xavfsizlik nazorati bilan hal qiladi. Ushbu boshqaruvlar tizimdagi har qanday zaifliklarni himoya qilish va kiberhujumlar ta'sirini kamaytirish uchun o'rnatiladi.

Bulutli xizmatlar, agar to'g'ri ta'minlansa, yuqori xavfsizlikka ega, ammo e'tiborsiz bo'lsa, ta'sir butunlay teskari bo'lishi mumkin. Yechim bulutning axborot xavfsizligi qoidalari va standartlariga muvofiqligini ta'minlashdan iborat.

O'zbekiston qonunchiligida bulutli texnologiyalarda axborot xavfsizligi tamoyilini tavsiflovchi standartlar hali mavjud emas. Natijada, bulutli xizmat ko'rsatuvchi provayderlar bozorda juda ko'p tayyor yechimlar orasidan o'zlarining ma'lumotlarni himoya qilish usullarini tanlashga majbur bo'lishadi. Lekin barcha xavfsizlik choralari bulut texnologiyasining xususiyatlarini hisobga olishi kerak.

Bulutldagi elektron hujjatlarni boshqarish tizimlarida axborot tahdidlarining asosiy turlarini quyida ko'rib chiqiladi.

E.A. Dogval o'zining ilmiy maqolasida bulutli xizmatlarga tahdidlarning beshta asosiy turini yoritgan.

1. *Dasturiy ta'minotga an'anaviy hujumlar*. Qo'llaniladigan tarmoq protokollari, operatsion tizimlar, modulli komponentlar va boshqalarning zaifligi bilan bog'liq. Bunday hujumlardan himoya qilish uchun antivirus dasturlari, xavfsizlik devori, kirishni oldini olish tizimi va boshqalar qo'llaniladi.
2. *Bulutli elementlarga funktsional hujum*. Bunday hujumlar bulutning ko'p qatlamli tabiati bilan bog'liq. Bunday kiberhujumlardan himoyalanishning asosiy vositasi tizimning eng zaif nuqtasini himoya qilishdir.

Bulutning har bir qatlami uchun funktsional hujumlardan himoya qilish uchun ularning har biri uchun maxsus himoya vositalaridan foydalanish kerak:

- proksi-server uchun - DDoS hujumlaridan himoya qilish,
- veb-server uchun - sahifa yaxlitligini nazorat qilish,
- dastur serveri uchun - dastur darajasidagi ekran.

DBMS qatlami uchun - SQL in'ektsiyalaridan himoya qilish, saqlash tizimi uchun - zaxira va kirishni boshqarish.

3. *Mijozga qaratilgan hujumlar*. Ushbu turdagi hujumlar veb-makonda juda keng tarqalgan. Bunday hujumlar bulutga asoslangan tizimlarda ham keng tarqalgan, chunki foydalanuvchilar odatda bulutga veb-brauzer orqali kirishadi. Ushbu turdagi hujumlarga saytlararo skriptlar, parollarni o'g'irlash, veb-sessiyani o'g'irlash, o'rtadagi odam hujumlari va boshqalar kiradi. Bu yerda an'anaviy tarzda foydalanuvchi autentifikatsiyasi himoya sifatida qo'llash zarur hisoblanadi, jumladan samarali ikki faktorli autentifikatsiya va o'zaro autentifikatsiya bilan shifrlangan ulanish.

4. *Virtualizatsiya vositalariga hujumlar*. Bularga gipervizorga, bulutli tugunlar o'rtasidagi o'zaro aloqada virtual mashinalarga hujumlar, shuningdek, bulutni boshqarish tizimlariga hujumlar kiradi.

Bunday tahdidlar hozirda juda kam uchraydi va bunday haqiqiy hujumlar haqida hech qanday ma'lumot yo'q. Biroq, ular bulutli virtualizatsiyaning mashhurligi tufayli kelajakda paydo bo'lishi mumkinligini yodda tutish kerak.

5. *Bulutli xizmatlar uchun murakkab tahdidlar*. Ushbu tahdidning sabablari infratuzilmani noto'g'ri nazorat qilishdir. Barcha bulutli resurslar hisoblanganligi va boshqarilmaydigan virtual mashinalar yo'qligi, keraksiz
biznes-jarayonlar ishlamayotganligi va bulut qatlamlari va elementlarining o'zaro konfiguratsiyasi buzilmasligiga kafolatlar yo'q. Ushbu turdagi tahdid bulutning yagona axborot tizimi sifatida boshqarilishi va bulutning ishlashida suiiste'mol qilish yoki boshqa buzilishlarni qidirish bilan bog'liq bo'lib, bu axborot tizimining funksionalligini saqlash uchun keraksiz xarajatlarga olib kelishi mumkin.

Ushbu turdagi tahdid yanada murakkabroq va uni himoya qilishning universal usuli yo'q - bu holda xavfsizlik usullari har bir bulut uchun alohida ishlab chiqiladi.

Shunday qilib, elektron hujjatlar bilan ishlash uchun bulut texnologiyalarida ma'lumotlar xavfsizligiga bag'ishlangan turli manbalarni tahlil qilib, elektron hujjatlar bilan ishlash uchun bulut texnologiyalarida ma'lumotlarni himoya qilishning quyidagi samarali usullarini ajratib ko'rsatish mumkin:

1. *ma'lumotlarni shifrlash*. Shifrlash axborotni himoya qilishning eng samarali usullaridan biridir. Provayder ma'lumotlar markazida joylashgan server tomonidan foydalanuvchi ma'lumotlarini shifrlashi kerak. Bulutli saqlashdan foydalanganda ma'lumotlarni shifrlashning bir necha usullari mavjud. Server tomoni shifrlash - bu tizim ikkala ma'lumotni qabul qilgandan so'ng, lekin ma'lumotlar diskka yozilishi va saqlanishidan oldin sodir bo'ladigan shifrlash va mijoz tomoni shifrlash - ma'lumotlar bulutli xotiraga yuborilishidan oldin sodir bo'ladigan shifrlash. Bunday ma'lumotlar bulutli xotiraga allaqachon shifrlangan shaklda kiradi, lekin server tomonida ham shifrlangan. Shifrlash kalitlari masalasi muhimligicha qolmoqda. Ularni bulutli serverda saqlash oqilona emas, chunki ushbu serverga kirish huquqiga ega bo'lgan har bir kishi kalitga va shuning uchun shifrlangan ma'lumotlarga kirish huquqiga ega bo'lishi mumkin. Kalitning jismoniy kiritilishi bulutli server tashqi manbaga - kalitlarni boshqarish serveriga yuboradigan so'rov bilan almashtiriladi. Bunday himoyani amalga oshirishning muhim komponenti bulutli server va kalitlarni boshqarish serverining alohida ishlashi hisoblanadi. Agar ikkalasi ham bir xil bulutli xizmat ko'rsatuvchi provayder tomonidan joylashtirilgan bo'lsa, unda barcha ma'lumotlar yana bir joyda to'planadi. Yaxshi alternativa mahalliy ma'lumotlar markazida yoki boshqa xizmat ko'rsatuvchi provayderning tashqi xizmati sifatida kalit boshqaruv serverini o'rnatishdir;

2. *ma'lumotlarni uzatish paytida himoya qilish.* Xavfsiz ma'lumotlarni qayta ishlash uchun shifrlangan uzatish zaruriy shartdir. Umumiy bulutdagi ma'lumotlarni himoya qilish uchun umumiy bulut xizmatlarini olish uchun mijoz va serverni bog'laydigan virtual xususiy tarmoq tunnelidan foydalaniladi. Virtual xususiy tarmoq tunneli xavfsiz ulanishlarni targ'ib qiladi va turli bulut manbalariga kirish uchun bitta nom va paroldan foydalanish imkonini beradi. Umumiy bulutlarda ma'lumotlarni uzatish vositasi sifatida VPN ulanishi Internet kabi umumiy resurslardan foydalanadi. Jarayon Secure Sockets Layer (SSL)

protokoliga asoslangan ikkita kalit yordamida shifrlangan kirish rejimlariga asoslangan;

3. *autentifikatsiya.* Autentifikatsiya - bu parol bilan himoyalanish. Masalan, ular tokenlardan foydalanadilar. Token - bu axborot xavfsizligini ta'minlash, shuningdek, foydalanuvchini aniqlash uchun ishlatiladigan elektron kalit. Autentifikatsiya tizimi bir martalik parollar tushunchasidan ham foydalanadi. Bunday parollar faqat bitta autentifikatsiya seansi uchun ishlatilishi mumkin va ma'lum vaqt bilan cheklanishi mumkin.

Bulutli infratuzilma o'rtasidagi asosiy farq kattaroq miqyoslilik va kengroq geografik taqsimotdir. Bir martalik parollarni olish uchun mobil gadjetlardan foydalanish birinchi o'ringa chiqmoqda. Eng oddiy holatda, bir martalik parol maxsus autentifikatsiya serveri tomonidan yaratiladi va bulut xizmatiga kirish sahifasida to'g'ri statik parolni kiritgandan so'ng foydalanuvchining mobil telefoniga SMS orqali yuboriladi.

Avtorizatsiya vaqtida provayder va identifikatsiya tizimi o‘rtasidagi shaffof o‘zaro aloqa uchun LDAP (Lightweight Directory Access Protocol) va SAML (Security Assertion Markup Language) autentifikatsiyasidan ham foydalanish tavsiya etiladi;

4. *foydalanuvchilarni izolyatsiya qilish.* Shaxsiy virtual mashina va virtual tarmoqdan foydalanish. Virtual tarmoqlar VPN (Virtual Private Network), VLAN (Virtual Local Area Network) va VPLS (Virtual Private LAN Service) kabi texnologiyalar yordamida joylashtirilishi kerak. Ko'pincha provayderlar bitta dasturiy muhitda kodni o'zgartirish orqali foydalanuvchi ma'lumotlarini bir-biridan ajratib turadilar. Ushbu yondashuv nostandart kodda ma'lumotlarga kirish imkonini beruvchi teshikni topish xavfi bilan bog'liq xavflarga ega. Kodda yuzaga kelishi mumkin bo'lgan xatolik bo'lsa, foydalanuvchi boshqa foydalanuvchining ma'lumotlariga kirish huquqiga ega bo'lishi mumkin.

Bulutli hujjatlarni qayta ishlash tizimlarida ma'lumotlarni himoya qilish haqida gapirganda, ma'lumotlarni qayta ishlash markazining o'zini eslatib o'tmaslik mumkin emas. Ma'lumotlar markazi samaradorlik va xavfsizlikni oshirish uchun bir hududda joylashgan serverlar to'plamini anglatadi.

Ma'lumotlarni qayta ishlash markazlari uchun xavfsizlik quyi tizimi quyidagi elementlarni o'z ichiga olishi kerak:

- xavfsizlik video kuzatuvi;
- xavfsizlik va yong'in signalizatsiyasi;
- kirishni boshqarish va boshqarish tizimi;
- ma'lumotlarni zaxiralash va tiklash tizimi;
- ma'lumotlarni qayta ishlash markazida axborot xavfsizligi tizimi.

Provayder nuqtai nazaridan axborot xavfsizligi texnologiyalaridan tashqari, mijoz tomonidan muammolarning oldini olish usullari ham muhimdir.

Turli adabiyotlarni tahlil qilgandan so'ng, bulut xizmatlaridan foydalanuvchilarga ularning ma'lumotlarining xavfsizligini ta'minlash bo'yicha tavsiyalar ishlab chiqish mumkin.

1. *Bulutli bozor tahlilini o'tkazish*. Korxonalarda qanday bulutli saqlash tizimlari mavjudligini, ulardan kim va qanday foydalanishini tushunish muhimdir. Siz o'z ma'lumotlaringizni faqat bozorda o'zini isbotlagan ishonchli va ishonchli kompaniyalarga ishonishingiz mumkin. Tanlashda xatolikka yo'l qo'ymaslik uchun siz bulut xizmatining obro'si, uning ishlash muddati, mijozlarning sharhlari, shuningdek, uning mashhurligi kabi muhim omillarni hisobga olishingiz kerak.

2. *Bulutli saqlash provayderi maxfiylik va xavfsizlik masalalarini qanday hal qilishini aniqlash*. Xizmat shartnomalari shartlari bulutli provayder tomonidan taqdim etiladigan umumiy himoyalarni aniqlash uchun yaxshi boshlanish nuqtasidir. Ammo bu faylni xavfsiz saqlashni ta'minlash uchun etarli emas. Bulutli xizmat ko'rsatuvchi provayderlar o'zlarining xizmat ko'rsatish shartlari va foydalanuvchi shartnomalarini tez-tez yangilab turadilar. Bu sizning maxfiyligingiz va xavfsizligingizga sezilarli ta'sir ko'rsatishi mumkin bo'lgan kichik o'zgarishlarni o'tkazib yuborishni osonlashtiradi.

Ko'pgina kelishuvlar bulutli saqlash provayderi xavfsizlikni qanday amalga oshirishi, u qanday xavfsizlik usullaridan foydalanishi va buzilish yoki buzilish holatlarida nima sodir

bo'lishi tafsilotlarini qamrab olmaydi. Natijada, provayder bilan kelajakdagi muzokaralarni osonlashtirish uchun siyosat va tartiblarni aniq belgilash muhimdir.

3. *Qanday himoya choralarini qo'llash kerakligini bilish*. Bulutda shifrlash asosiy talabdir. Bulutli saqlash provayderi shifrlashdan qanday foydalanishini, shu jumladan ma'lumotlar markazlari, serverlar va saqlash qurilmalari o'rtasida ma'lumotlarni uzatishda va shifrlash kalitlarini kim nazorat qilishini va ular ma'lum bir ma'lumotlar to'plamiga qanday qo'llanilishini bilish muhimdir.

Bulutli provayderdan foydalanadigan tashkilot tizimlarga kim kirish huquqiga ega ekanligini va DDoS hujumlaridan tortib ilovalardagi tizim xatolarigacha qanday boshqa himoyalar mavjudligini bilishi kerak;

4. *Barcha qurilmalar va tizimlarda ko'p faktorli autentifikatsiyadan foydalanish.* Ko'p faktorli autentifikatsiyadan keng foydalanish zararli dasturlarni chiqarish yoki qimmatli ma'lumotlarni o'g'irlash uchun tizim yoki ilovaga kirish xavfini sezilarli darajada kamaytiradi. Ko'p faktorli autentifikatsiya maxfiy ma'lumotlarni xakerlar, norozi xodimlar va ma'lumotlarni qasddan yoki beixtiyor xavf ostiga qo'yadigan boshqa insayderlardan himoya qilishga yordam beradi.

5. *Tahdidlar uchun audit va penetratsion testlarni o'tkazish*. Kompaniya uchinchi tomon xavfsizlik firmasi bilan hamkorlik qiladimi yoki uning ichki xodimlariga tayanadimi, ekspertlarning ta'kidlashicha, tizimning bulut xavfsizligi choralari to'g'ri ishlab chiqilganligini aniqlash uchun tahdidlarning kirib borishi testini o'tkazish kerak.

Tashkilot tizimning bulut xavfsizligi imkoniyatlarini muntazam ravishda tekshirishi kerak. Audit o'z ichiga etkazib beruvchilarning imkoniyatlarini tahlil qilishni o'z ichiga olishi kerak himoya usullari xavfsizlik shartlariga mos kelishi kerak.

Bundan tashqari, bulutdagi maxfiy ma'lumotlar va ilovalarga faqat vakolatli xodimlar kirishiga ishonch hosil qilish uchun kirish jurnallarini ko'rib chiqish kerak.

6. Ma'lumotlaringizning jismoniy himoyasini ta'minlash. Jismoniy ma'lumotlarni himoya qilish tashkilotning kompyuterlariga ruxsatsiz kirish bilan bog'liq xavflarni minimallashtirishni o'z ichiga oladi. Kelayotgan va ketayotgan mehmonlarni kuzatishdan tashqari, ofisni kalit bilan qulflash va ketishdan oldin kompyuterni qulflashni unutmaslik kerak.

Shunday qilib, elektron hujjatlar bilan ishlash uchun bulutli tizimda ma'lumotlarni himoya qilishning asosiy usullarini ko'rib chiqildi, shuningdek, bunday tizimlardan foydalanuvchilar uchun xavfsizlik choralari bo'yicha tavsiyalar ishlab chiqildi.

Aksariyat hollarda xavfsizlik muammolari tashkilotlarning bulut xizmatlaridan foydalanishiga to'sqinlik qilmasligi kerak. Bulutli xavfsizlikning eng yaxshi amaliyotlariga rioya qilish orqali ular bulutli hisoblashning barcha afzalliklaridan foydalangan holda bunday tahdidlar xavfini yanada kamaytirishi mumkin.

Katta va kichik tashkilotlar o'zlarining bulutli mahsulotlari uchun xavfsizlik tizimlarini ishlab chiqish va takomillashtirishga katta mablag' sarflaydilar. Bulutli xizmatni tanlashda siz uning barcha xususiyatlarini, ayniqsa ishonchlilik masalasini diqqat bilan o'rganishingiz kerak.

XULOSA

Hozirgi vaqtda bulutli xizmatlarda ma'lumotlarni himoya qilish usullari yangi yondashuvni talab qiladi. Himoya xizmat ko'rsatuvchi provayder va foydalanuvchining kelishilgan ishi orqali amalga oshiriladigan chora-tadbirlarning butun majmuasini o'z ichiga olishi kerak. Loyihani amalga oshirish uchun, hatto uni ishlab chiqish bosqichida ham, professional xavfsizlik mutaxassislarini jalb qilish kerak, ular yordamida tegishli dasturiy ta'minot va apparat vositalarini himoya qilish choralarini ishlab chiqish va ta'minlash, shu jumladan ishonchli shifrlash, server uskunalariga kirishni cheklash, ishonchli ishni ro'yxatga olish, guruh siyosati asosida tartibga solinadigan kirish va h.k.larni hisobga olish zarur sanaladi.

FOYDALANILGAN ADABIYOTLAR

1. S. K. G'aniev, A.A G'aniyev, Z.T. Xudoyqulov "Kiberxavfsizlik asoslari". O'quv qo'llanma. Toshkent-"Aloqachi" - 2020.
2. Александров К.С. Счет на петабайты // Машины и механизмы. 2013. № 6. С. 20-27. 2. Мурзин Ф.А., Батура Т.В., Семич Д.Ф. Облачные технологии: основные понятия, задачи и тенденции развития // Программные продукты, системы и алгоритмы. 2014. № 1. С. 2-22.
3. Берхольц К.А. Применение облачных технологий в электронном документообороте коммерческих организаций // Инновационное развитие. – 2018. № 10. С. 9-12. 4. Гладкий М.В. Безопасность приложений на платформах облачных вычислений // Труды БГТУ. 2015. № 9. С 204-207.
4. Горохов С.Н, Лобанов Е.М. Современные технологии хранения электронных документов // Вестник архивиста. 2015. № 1. С. 193-200.
5. Гусеев А.В. Перспективы облачных вычислений и информатизация учреждений здравоохранения // Медицинские информационные системы. 2011. № 2. С. 6-16.
6. енисов Д.В. Перспективы развития облачных вычислений // Прикладная информатика. 2009. № 5. С. 52-58.
7. Довгаль В.А. Облачные вычисления и анализ вопросов информационной безопасности в облаке // Вестник Адыгейского государственного университета. 2015. № 2. С. 160-166.
8. Догваль. Е.М. Методы повышения безопасности в сфере «облачных» технологий // Вестник АГУ. 2014. №4. С. 170-174.
9. . Ивонин П.В. Безопасность облака в деталях // Известия ЮФУ. 2013. № 2. С. 35-40.
10. Кодлов П.А. Проблемы безопасности облачных вычислений // Наука, техника и образование. 2016. № 12. С. 54-58.