



**BULUTLI TEXNOLOGIYALAR ASOSIDA KORPORATIV MA'LUMOTLAR
XAVFSIZLIGINI TA'MINLASH USULLARI**

Xurramov A.B.

Xurramova M.J.

Toshkent davlat iqtisodiyot universiteti o'qituvchisi, Toshkent, O'zbekiston.

khurramov@tsue.uz

m.khurramova@tsue.uz

Annotatsiya. Mazkur tezisda zamonaviy axborot-kommunikatsiya infratuzilmasining ajralmas qismi sifatida shakllanayotgan bulutli texnologiyalar asosida korporativ ma'lumotlar xavfsizligini ta'minlash masalalari yoritilgan. Xususan, bulutli muhitda saqlanayotgan ma'lumotlarga tahdid soluvchi omillar, ularning turlari va ularni aniqlash mexanizmlari ko'rib chiqiladi. Korxonalar uchun ma'lumotlar maxfiyligini, butligini va mavjudligini kafolatlaydigan xavfsizlik texnologiyalari – shifrlash, ko'p faktorli autentifikatsiya, kirishni boshqarish siyosatlari, zaxira nusxalash va xavflarni monitoring qilish tizimlari tahlil qilinadi. Shuningdek, milliy va xalqaro axborot xavfsizligi standartlariga muvofiqlik, bulutli xizmat provayderlarining roli hamda O'zbekistondagi raqamli transformatsiya jarayonlarida bu texnologiyalarning qo'llanishi amaliy misollar bilan yoritilgan.

Kalit so'zlar: bulutli texnologiyalar, korporativ ma'lumotlar, axborot xavfsizligi, shifrlash, autentifikatsiya, zaxira nusxasi, tahdidlar, kirishni boshqarish, raqamli transformatsiya, ma'lumotlar xavfsizligi siyosati.

Kirish

Bugungi tez o'zgaruvchan raqamli makonda axborot texnologiyalari jadal rivojlanib borayotgan bir paytda, korxona va tashkilotlar o'z faoliyatida samaradorlikka erishish, xarajatlarni kamaytirish va raqobatbardoshlikni oshirish maqsadida bulutli texnologiyalar (cloud computing)dan keng foydalanmoqda. Ushbu texnologiyalar ma'lumotlarni saqlash, ularga masofadan kirish, dasturiy ta'minotdan foydalanish hamda axborot resurslarini boshqarishda qulayliklar yaratadi. Ammo bu qulayliklar bilan bir qatorda, korporativ ma'lumotlar xavfsizligini ta'minlash masalasi dolzarb muammolardan biri bo'lib qolmoqda. Ayniqsa, maxfiy va tijorat sirlarini o'zida mujassam etgan axborotlarning tahdid ostida bo'lishi korxonalar uchun jiddiy xavf tug'diradi.

Bulutli xizmatlar uch asosiy model asosida tashkil etiladi: SaaS (Software as a Service) – dasturiy ta'minotga masofaviy kirish, PaaS (Platform as a Service) – platformalar orqali dastur ishlab chiqish imkoniyati va IaaS (Infrastructure as a Service) – server, tarmoq va xotira kabi infratuzilmani ijaraga olish. Bu modellarning har biri foydalanuvchidan turli darajada xavfsizlik choralarini talab etadi.



Bulutli texnologiyalar asosida axborotni saqlash va qayta ishlash jarayonida xavfsizlik muammolari bir nechta murakkab yo'nalishlarda namoyon bo'ladi. Avvalo, identifikatsiya va autentifikatsiya jarayonlaridagi zaifliklar noto'g'ri foydalanuvchilar tomonidan ma'lumotlarga ruxsatsiz kirish holatlariga olib keladi. Bu esa korporativ ma'lumotlarning maxfiyligini jiddiy darajada xavf ostida qoldiradi. Shuningdek, axborotlarning butligi va maxfiyligi bilan bog'liq xavflar ham dolzarb hisoblanadi. Bulutli muhitda saqlanayotgan ma'lumotlarning o'zgartirilishi, buzilishi yoki uchinchi tomon tomonidan ruxsatsiz ko'rilishi ehtimoli mavjud bo'lib, bu holatlar korxona obro'siga, moliyaviy holatiga va mijozlar ishonchiga salbiy ta'sir ko'rsatadi. Bunday xavflar nafaqat tashqi tahdidlar bilan, balki ichki sabotajlar va insoniy omillar bilan ham bog'liq bo'lib, bulut xizmatlaridan foydalanuvchi xodimlar xavfsizlik siyosatiga to'liq amal qilmaganda yuzaga chiqishi mumkin.

Bundan tashqari, xizmat ko'rsatuvchi bulut provayderining ishonchliligi ham muhim omil hisoblanadi. Agar ma'lumotlar saqlanayotgan serverlar boshqa davlat hududida joylashgan bo'lsa, xalqaro huquqiy ziddiyatlar, yurisdiksiya tafovutlari va ma'lumotlarga bo'lgan egalik masalalari yuzaga kelishi mumkin. Bu holatlarda ma'lumotlar ustidan nazoratni yo'qotish xavfi oshadi. Shu bilan birga, DDoS (Distributed Denial of Service) hujumlari, zararli dasturlar va troyanlar kabi kiberxurujlar bulutli xizmatlarning to'xtab qolishi yoki butunlay ishdan chiqishiga olib kelishi mumkin. Natijada, muhim axborot resurslari vaqtincha yoki doimiy ravishda yo'qotilishi ehtimoli mavjud bo'ladi.

Yana bir muhim muammo — bu "vendor lock-in", ya'ni foydalanuvchining ma'lumotlarni bir bulut provayderidan boshqasiga o'tkaza olmasligi bilan bog'liq murakkablikdir. Texnologik mos kelmaslik, fayl formatlarining farqli bo'lishi yoki xizmat ko'rsatish shartlarining cheklanganligi sababli korxona bir provayder xizmatlariga qaram bo'lib qoladi. Bu esa raqobatbardoshlikni kamaytirib, texnologik rivojlanishga to'sqinlik qiladi.

Yuqorida sanab o'tilgan omillar shuni ko'rsatadiki, har qanday korxona bulutli texnologiyalarni joriy etishda, eng avvalo, ma'lumotlar xavfsizligini ta'minlash choralariga alohida e'tibor qaratishi lozim. Xavfsizlik siyosatini aniq belgilash, standartlarga amal qilish, zamonaviy himoya vositalarini qo'llash va xodimlar malakasini oshirish bu borada muhim ahamiyatga ega. Faqatgina kompleks yondashuv asosida tashkil etilgan xavfsizlik tizimi orqali bulutli texnologiyalardan to'liq va ishonchli foydalanish mumkin bo'ladi.

Korporativ ma'lumotlar xavfsizligini ta'minlash usullari

Zamonaviy bulutli muhitda ma'lumotlar xavfsizligini kafolatlash uchun quyidagi texnik va tashkiliy yondashuvlar samarali hisoblanadi:

1. Shifrlash (Encryption)

Ma'lumotlarni yuborishdan oldin shifrlash orqali ularning mazmunini faqat maxsus kalitga ega shaxs o'qiy oladigan shaklga keltirish lozim. Zamonaviy shifrlash algoritmlari (masalan, AES-256, RSA) yordamida ma'lumotlar xakerlar tomonidan o'g'irlangan taqdirda ham ularni yechib bo'lmaydi.





2. Ko'p faktorli autentifikatsiya (Multi-Factor Authentication)

Foydalanuvchining shaxsini tasdiqlashda bir nechta xavfsizlik bosqichlaridan foydalaniladi: parol, mobil qurilmaga yuborilgan tasdiqlash kodi, biometrik skanerlash va boshqalar. Bu, ayniqsa, yuqori darajadagi huquqga ega foydalanuvchilar uchun muhim hisoblanadi.

3. Ruxsatlarni aniqlash va rollarga asoslangan kirish (IAM)

Kompaniya ichidagi xodimlarga rollariga mos darajada cheklangan ruxsatlar berilishi kerak. Foydalanuvchilar minimal zarur axborot doirasida faoliyat yuritishi xavfsizlikni oshiradi.

4. Zaxira nusxalar va avariya tiklash strategiyasi

Ma'lumotlar muhim voqealar (server ishdan chiqishi, texnik nosozliklar) yuz berganda tezda tiklanishi uchun muntazam zaxira qilinadi. Bulutli provayderlar bu xizmatni avtomatik ravishda ta'minlaydi, biroq foydalanuvchi ularni tekshirib borishi lozim.

5. Monitoring va xavf tahlili tizimlari

Real vaqt rejimida tizim faoliyatini kuzatish, g'ayrioddiy harakatlarni aniqlash va ularga javob qaytarish uchun SIEM (Security Information and Event Management), IDS/IPS tizimlari keng qo'llaniladi. Bu texnologiyalar yordamida korxona o'zining himoya darajasini real holatda baholashi mumkin.

Axborot xavfsizligi bo'yicha standartlar va me'yorlar

Korporativ ma'lumotlar xavfsizligini ta'minlashda milliy va xalqaro standartlarga amal qilish zarur. Quyidagi me'yoriy-huquqiy hujjatlar ushbu yo'nalishda muhim o'rin tutadi:

- ISO/IEC 27001 – axborot xavfsizligini boshqarish tizimining sertifikatlash mezonlari;
- NIST SP 800-53 – AQSh Milliy Standartlar va Texnologiyalar Institutining xavfsizlik choralari to'plami;
- GDPR (General Data Protection Regulation) – Yevropa Ittifoqining shaxsiy ma'lumotlarni himoyalash reglamenti;
- O'zbekiston Respublikasining "Axborot xavfsizligi to'g'risida"gi Qonuni – milliy darajadagi xavfsizlik siyosatining asosiy hujjati;
- O'zbekiston Respublikasi Prezidentining raqamlashtirish sohasiga oid qarorlari, xususan, "Raqamli O'zbekiston – 2030" strategiyasi.

Xulosa va takliflar

Bulutli texnologiyalar raqamli transformatsiyaning asosi bo'lib, korxonalarga katta imkoniyatlar yaratmoqda. Shu bilan birga, bu texnologiyalardan foydalanish ma'lumotlar xavfsizligini ta'minlash bilan chambarchas bog'liq. Korporativ axborot xavfsizligini ishonchli darajada ta'minlash uchun quyidagilarni taklif etish mumkin:



TANQIDIY NAZAR, TAHLILIY TAFAKKUR VA INNOVATION G'OYALAR



- Bulutli xizmatlardan foydalanuvchi tashkilotlar o'z xavfsizlik siyosatlarini ishlab chiqib, doimiy ravishda yangilab borishlari zarur;
- Foydalanuvchilarning malakasini oshirish bo'yicha muntazam o'quv va treninglar tashkil etilishi;
- Shifrlash va autentifikatsiya mexanizmlaridan majburiy tarzda foydalanish;
- Faol monitoring tizimlarini joriy etish va himoya darajasini doimiy baholab borish;
- Xizmat ko'rsatuvchi bulut provayderlarining xalqaro standartlarga muvofiqligini baholab tanlash.

Umuman olganda, bulutli texnologiyalar asosida ma'lumotlar xavfsizligini ta'minlash ko'p darajali va murakkab yondashuvni talab qiladi. Bunda texnik vositalar bilan bir qatorda, inson omiliga, huquqiy me'yorlarga va strategik boshqaruvga ham alohida e'tibor qaratilishi lozim.

FOYDALANILGAN ADABIYOTLAR

1. O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi "Raqamli O'zbekiston – 2030" strategiyasini tasdiqlash to'g'risidagi PQ–6079-son Qarori: <https://lex.uz/ru/docs/-5030957>
2. ISO/IEC 27001:2013 – Information security management systems – Requirements. International Organization for Standardization, Geneva, 2013.
3. National Institute of Standards and Technology (NIST). Special Publication 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations. U.S. Department of Commerce, 2020.
4. European Union. General Data Protection Regulation (GDPR). – Regulation (EU) 2016/679 of the European Parliament and of the Council. – Brussels, 2016.
5. Stallings W. *Network Security Essentials: Applications and Standards*. – 6th ed. – Pearson Education, 2020.
6. Kaufman C., Perlman R., Speciner M. *Network Security: Private Communication in a Public World*. – 2nd ed. – Prentice Hall, 2016.
7. Хайтов М., Юсупов И. *Axborot xavfsizligi asoslari*. – Toshkent: "Fan va texnologiya", 2021. – 260 b.
8. Karimov A., Zokirov S. *Bulutli texnologiyalar va ularning amaliy qo'llanilishi*. – Toshkent: TDYU nashriyoti, 2022. – 144 b.



9. Rashid A. *Cloud Computing: Concepts, Technology & Architecture*. – Prentice Hall, 2013.

10. Li, J., Chen, X., Zhang, Q. et al. *Secure and Privacy-Preserving Data Storage in Cloud Computing: A Survey*. – *IEEE Access*, 2020. – Vol. 8. – pp. 1310–1332.

11. Wang, C., Wang, Q., Ren, K., Lou, W. *Ensuring Data Storage Security in Cloud Computing*. – *Proceedings of the 17th International Workshop on Quality of Service (IWQoS)*. – 2009.