BUGUNGI KUNDA AXBOROT XAVFSIZLIGIGA BO`LADIGAN XUJUMLAR VA ULARNING OLDINI OLISH

Mamarajabov Husan Ergash o‘g‘li
Toshkent amaliy fanlar universiteti,
“Kompyuter injiniringi” fakulteti o`qituvchisi
E-mail: husankarimov09@gmail.com
Tel: *+998945169616*
Shukurov Dadanur Tohir o`g`li
Toshkent amaliy fanlar universiteti,
“Kompyuter injiniringi” fakulteti o`qituvchisi
E-mail: dadanur0094@gmail.com
Tel: +9989977420094
Xurramov Azizjon Baxodir o`g`li
Toshkent amaliy fanlar universiteti,
“Kompyuter injiniringi” fakulteti o`qituvchisi
E-mail: azizbekxurramov0102@gmail.com
Tel: +998907472494

Annotatsiya: Mazkur maqolada bugungi kunda axborot xavfsizligining o`rni qanchalik muhimligi, unga bo`ladigan xujumlar va uning turlari, oldini olish haqida bo`ladi.

Kalit so‘zlar: Axborot xavfsizligi, maxfiylik, butunlik,mavjudlik, dasturiy ta`minot, texnik ta`minot, antivirus dasturlari, bulutli antiviruslar, DLP texnologiyasi.

Axborot texnologiyalarining rivojlanishi va iqtisodiyotni kompyuterlashtirish munosabati bilan kompaniya faoliyatidagi eng muhim masalalardan biri axborot xavfsizligini ta’minlash hisoblanadi.

Axborot xavfsizligi - bu axborotni, shuningdek, uning eng muhim elementlarini, shu jumladan ushbu ma'lumotlarni ishlatish, saqlash va uzatish uchun mo'ljallangan tizimlar va uskunalarni saqlash va himoya qilish. Boshqacha qilib aytganda, bu axborot xavfsizligini himoya qilish uchun zarur bo'lgan texnologiyalar, standartlar va boshqaruv amaliyotlari to'plamidir.

Korxonada axborot xavfsizligi tizimlarini muvaffaqiyatli joriy etish uchun uchta asosiy tamoyilga rioya qilish kerak:

Maxfiylik. Bu korxona ma'lumotlari, aktivlari va ma'lumotlari biznes operatsiyalarining turli bosqichlarida istalmagan yoki ruxsatsiz oshkor etilishining oldini olish uchun etarli darajada himoyalanganligini ta'minlash uchun nazoratni o'rnatishni anglatadi. Axborotni saqlashda, shuningdek, uning formatidan qat'i nazar, oddiy tashkilotlar orqali o'tishda maxfiylik saqlanishi kerak.

Butunlik. Integrity korporativ ma'lumotlarning ichki va tashqi izchilligini ta'minlash bilan bog'liq bo'lgan nazorat bilan shug'ullanadi. Butunlik, shuningdek, ma'lumotlarning buzilmasligini ta'minlaydi.

Mavjudligi. Mavjudlik vakolatli shaxslar tomonidan ma'lumotlarga ishonchli va samarali kirishni ta'minlaydi. Tarmoq muhiti kerak bo'lganda ma'lumot va

ma'lumotlarga kirish uchun oldindan taxmin qilinadigan tarzda harakat qilishi kerak. Axborot mavjudligi haqida gap ketganda, tizimdagi nosozlikni tiklash muhim omil bo'lib, bunday tiklash ham ishlashga salbiy ta'sir ko'rsatmaydigan tarzda ta'minlanishi kerak.

Axborot xavfsizligini nazorat qilish

Axborot xavfsizligi tahdidlarini quyidagilarga bo'lish mumkin:

Tabiiy (inson nazorati ostida bo'lmagan kataklizmlar: yong'inlar, bo'ronlar, suv toshqini, chaqmoq urishi va boshqalar).

Sun'iy, ular ham quyidagilarga bo'linadi:

- qasddan (odamlar tomonidan ehtiyotsizlik yoki johillik tufayli sodir etilgan);
- qasddan (xakerlik hujumlari, raqobatchilarning noqonuniy harakatlari, xodimlarning qasosi va boshqalar).

Ichki (tizim ichidagi tahdid manbalari).

Tashqi (tizimdan tashqari tahdidlar manbalari)

Axborot xavfsizligi vositalari quyidagilarga bo'linadi:

Tashkiliy. Bu tashkiliy-texnik (kompyuter vositalari bilan ta'minlash, kabel tizimini o'rnatish va boshqalar) va tashkiliy-huquqiy (qonunchilik bazasi, muayyan tashkilotning nizomi) vositalarining kombinatsiyasi.

Dasturiy ta'minot. Ma'lumotni boshqarish, saqlash va himoya qilish va unga kirishga yordam beradigan dasturlar.

Texnik (apparat). Bu ma'lumotlarni kirish va oqishdan himoya qiluvchi texnik turdagi qurilmalar.

Aralash apparat va dasturiy ta'minot. Ular apparat va dasturiy ta'minot funktsiyalarini bajaradilar.

Axborot xavfsizligi vositalarining turlari:

Antivirus dasturlari kompyuter viruslari bilan kurashadigan va zararlangan fayllarni tiklaydigan dasturlardir.

Bulutli antivirus (CloudAV) bulutga asoslangan axborot xavfsizligi yechimlaridan biri bo‘lib, u himoyalangan kompyuterda engil agent dasturiy ta’minotidan foydalanadi va axborot tahlilining ko‘p qismini provayder infratuzilmasiga yuklaydi.

DLP (Data Leak Prevention) yechimlari axborotning sizib chiqishiga qarshi himoya hisoblanadi. Ma'lumotlar oqishining oldini olish (DLP) - butun dunyo bo'ylab korxonalarda yuzaga keladigan nozik ma'lumotlarning yo'qolishining oldini olishga qaratilgan texnologiyalar to'plami.

AKT xavfsizligini ta’minlashda DLP tizimini qo‘llash Axborot kommunikatsiya tizimlarini xavfsizligini ta’minlash maqsadida har xil antiviruslar, fayrvollar, radmin va shunga o‘xshash ko‘pgina dasturiy vositalar ishlab chiqilgan. Lekin bularning hech biri ichki xavfdan, ya’ni insayderlardan to‘la himoyalay olmaydi. DLP tizimi esa huddi shunday muammolarni yechishga imkon beradi. Bunda axborot xavfsizligi xodimi korxonani har tomonlama o‘rganib chiqib, unga kerak bo‘ladigan DLP tizimini tanlay olishi lozim. Dastlab DLP tizimi nima degan savolga oydinlik kiritib olsak. Data Loss Prevention yoki DLP – maxfiy axborotlarni ruxsatsiz chiqib ketishini oldini olish tizimi hisoblanadi. Ushbu tizim ma’lumotlarni kuzatib borish va korparativ tarmoqdan tashqariga uzatish uchun ruxsatsiz urinishlarni oldini olishga mo‘ljallangan. Bundan tashqari, DLP tizimi foydalanuchilarning xarakatlarini kuzatib borish, ya’ni kommunikatsiya tizimlari orqali ijtimoiy tarmoqlardan va elektron pochtalar (e-mail) dan chiqib ketayotgan ma’lumotlarni yozib borish hamda tahlil qilish jarayonlarini amalga oshiradi. DLP tizimini asosiy vazifasi – tashkilotning maxfiylik siyosatiga mosligini ta’minlashdan iborat. DLP tizimining tarkibini Symantec Data Loss Prevention (SDLP) chiziq dasturiy yechim misolida ko‘rib chiqsak. SDLP keng ko‘lamdagi yechimlari tarmoqlarda, ma’lumotlarni saqlash tizimlarida hamda korporativ tarmoqda ishlashi yoki ishlamasligidan qat’iy nazar xodimlar kompyuterlarida joylashgan konfidentsial ma’lumotlar uchun himoyani ta’minlab beradi.

Xavfsizlik siyosati tomonidan fayllarning ba’zi turlari tashqariga uzatish taqiqlangan bo‘lishi mumkin. Shu bilan birga, foydalanuvchi fayl kengaytmasini o‘zgartirganda, tizim baribir fayl turini “topishi” va kerakli choralar ko‘rishi zarur. Ko‘p yechimlarda Autonomy kompaniyasining yechimlari qo‘llaniladi. Axborotni foydalanuvchilar bo‘yicha statistik “xulq-atvor” tahlil qilish. Agar foydalanuvchi konfidentsial axborotdan foydalanish huquqiga ega bo‘lsa, shuningdek, muayyan saytlarga tashrif buyursa (web-storage, web-mail, xakerlik va h.k.), bunday holatda “xavfli guruhga” kirib qoladi va unga nisbatan xavfsizlik siyosatining qo‘shimcha cheklovlari qo‘llaniladi; Hozirgi zamon axborot texnologiyalarning rivojlanishi bilan axborotni saqlash va uzatish uchun mo‘ljallangan vositalar va qurilmalar ko‘payib bormoqda. Shuni inobatga olgan holda, davlat va xo‘jalik organlarining axborot xavfsizligini ta’minlash bo‘linmalarida maxfiy axborotlarni ruxsatsiz chiqib ketishining oldini olish hamda ma’lumotlarni kuzatib borish va ruxsatsiz urinishlarni oldini olish uchun DLP tizimidan foydalanish maqsadga muvofiq.

DLP tizimi maxfiy ma'lumotlarning sizib chiqishini oldini olishi kerakligi sababli, u ushlangan trafikda aniqlangan hujjatning maxfiylik darajasini aniqlash uchun o'rnatilgan mexanizmlarga ega. Qoida tariqasida, ikkita usul eng keng tarqalgan: maxsus hujjat belgilarini tahlil qilish va hujjat mazmunini tahlil qilish. Hozirgi vaqtda ikkinchi variant keng tarqalgan, chunki u hujjat jo'natilishidan oldin unga kiritilgan o'zgartirishlarga chidamli bo'lib, shuningdek, tizim ishlashi mumkin bo'lgan maxfiy hujjatlar sonini osongina kengaytirish imkonini beradi.

Barcha DLP tizimlarini bir qator xususiyatlarga ko'ra bir nechta asosiy sinflarga bo'lish mumkin. Maxfiy deb belgilangan ma'lumotlarni bloklash qobiliyatiga ko'ra, foydalanuvchi harakatlarini faol va passiv nazorat qiluvchi tizimlar ajralib turadi. Birinchisi uzatilgan ma'lumotni blokirovka qilishga qodir, ikkinchisi esa mos ravishda bunday qobiliyatga ega emas. Birinchi tizimlar tasodifiy ma'lumotlar sizib chiqishi bilan kurashishda ancha yaxshi, lekin shu bilan birga ular tashkilotning biznes-jarayonlarini tasodifiy to'xtatishga imkon beradi, ikkinchisi esa biznes jarayonlari uchun xavfsizdir, lekin faqat tizimli sizib chiqishi bilan kurashish uchun javob beradi.

Kriptografik tizimlar - ma'lumotni shunday o'zgartirish, uni shifrlash faqat ma'lum kodlar yoki shifrlar yordamida mumkin bo'ladi (DES - Data Encryption Standard, AES - Advanced Encryption Standard). Kriptografiya boshqa foydali ilovalar, jumladan, autentifikatsiyaning ilg'or usullari, xabarlar dayjestlari, raqamli imzolar va shifrlangan tarmoq aloqalari bilan axborot xavfsizligini ta'minlaydi.

Foydalanilgan adabiyotlar

1. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. –Т., Ўзбекистон маркаси. 2009. – 432 б.

2. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие /Под ред. М.А. Иванова. М.: НИЯУ МИФИ, 2012. – 400 с.:

3. Encyclopedia of Cryptography and Security, Edited by Henk C. A. van Tilborg. Springer Science+Business Media, Inc, 2005. –697 p.