6 – TOM 6 – SON / 2023 - YIL / 15 - IYUN

AXBOROT TIZIMLARINI HIMOYALASHDA RUXSAT BERISH TA'MOYILINING QO'LLANILISHI

Seytniyazov Davronbek Bayramovich
tayanch doktorant
Atamuratova Shaxsanem Turdimuratovna
talaba
Dauletmuratova Juldiz Ayapbergenovna
talaba
Jumaniyazova Ulbosin Polatbay qizi
talaba

Axborot xavfsizligini ta'minlashning asosiy tamoyillarini axborot tizimlaridagi turli aloqa va xavfsizlikni ta'minlovchi tizimlar, umumiy texnik vositalar, aloqa kanallari, dasturiy ta'minot va ma'lumotlar bazalariga ega yagona tizim integratsiyasiga asoslangan kompleks yondashuv tashkil etadi.

Axborot tizimi keng ma'noda olib qaralganda, tizimdan foydalanuvchilarni kerakli axborot bilan ta'minlash uchun zarur bo'lgan texnik, dasturiy va tashkiliy ta'minot hamda xizmat ko'rsatish xodimlarining yig'indisi hisoblanadi.

Axborot xavfsizligi – saqlanuvchi axborotning salbiy ta'sirlardan himoyalanganlik holatidir.

Tarmoq xavfsizligi – tashkilot yoki korxonaning kompyuter tarmog'i infratuzilmasiga hamda undan foydalanishda tarmoq resurslarini ruxsatsiz foydalanishdan himoyalash bo'yicha qo'yiluvchi talablar majmuidir.

Tarmoq xavfsizligi deganda obyektning axborot infrastrukturasini (autentifikatsiyalash, mualliflash, tarmoqlararo ekran, ruxsatsiz kirishga harakatlarni aniqlash tizimlari IDS/IPS (Intrusion Detection/Prevention System – yorib kirishlarning aniqlash/oldini olish tizimlari) va boshqa usullar yordamida), tashqaridan g'arazgo'y kimsalarning kirishidan hamda tasodifiy xatolardan (DLP texnologiyasi vositasida), shuningdek ruxsatga ega bo'lgan xizmat ko'rsatuvchi xodimlarning maqsadli harakatlaridan himoya qilish tushuniladi. DLP (Data Leak Prevention) texnologiyasi – bu axborot tizimidagi konfedensial axborotlarni ruxsatsiz chiqib ketishidan dasturiy yoki dasturiy-qurilmaviy vositalarni qo'llash orqali himoya qilishning zamonaviy texnologiyasidir. Bunda chiqib ketish kanallari tarmoqli (masalan, elektron pochta) yoki lokal (tashqi axborot yig'uvchilardan foydalanib) bo'lishi mumkin.

Autentifikatsiya – foydalanuvchining axborot tizimiga kirishi uchun ruxsat berilishida, uning identifikatsiya ma'lumotlarini tekshirish jarayoni.

Mualliflash (Avtorizatsiya) – biror foydalanuvchiga ma'lum bir harakatlarni bajarish uchun huquq berish. Mualliflash autentifikatsiyadan keyin amalga oshiriladi va

foydalanuvchining qaysi resurslarga ruxsati borligini aniqlashda identifikatordan foydalaniladi. Axborot texnologiyalarida mualliflash yordamida axborot resurslari va qayta ishlash tizimlaridan foydalanishga ruxsat huquqi aniqlanadi va amalga oshiriladi.

Axborotni uzatish va qayta ishlashda autentlik – bu axborotning butunligi bo'lib, u ma'lumotlar haqiqatan ham qonuniy foydalanuvchilar tomonidan hosil qilinganligini hamda mualliflikdan bosh tortish imkoniyati yo'qligini tasdiqlaydi.

Axborotni himoya qilish – bu himoyalangan axborotni chiqib ketishi, unga noqonuniy va tasodifiy ta'sir ko'rsatishning oldini olishga yo'naltirilgan faoliyatdir.

Kompleks xavfsizlik – vujudga kelishi mumkin bo'lgan barcha turdagi tahdidlar (noqonuniy foydalanish, ma'lumotlarni tutib olish, terrorizm, yong'in, tabiiy ofatlar va h.k.)ni majburiy hisobga olib, zamon va makon (faoliyatning barcha texnologik sikllari) bo'yicha xavfsizlikni ta'minlashning majburiy bo'lgan uzluksiz jarayonini nazarda tutadi.

Kompleks yondashuv qanday shaklda qo'llanilishidan qat'iy nazar, u murakkab va turli yo'nalishdagi xususiy masalalarni, ularning o'zaro chambarchas bog'liqlikdagi yechimi bilan hal etiladi. Bunday masalalarning eng dolzarblari bo'lib, axborotlardan foydalanishni cheklash, axborotlarni texnik va kriptografik himoyalash, texnik vositalarning yondosh nurlanishlari darajasini kamaytirish, obyektlarning texnik mustahkamlanganligi, ularning qo'riqlash va tahlikadan xabardor qilish (signalizatsiya) qurilmalari bilan jihozlanganligi hisoblanadi.

Foydalanuvchilar, operatorlar, administratorlarga qurilmadan foydalanishga ruxsat berishni tashkil etishda quyidagi harakatlar amalga oshiriladi:

- ruxsat olayotgan subyektni identifikatsiyalash va autentifikasiyalash;
- qurilmani blokirovkadan chiqarish;
- ruxsat berilgan subyektning harakatlarini hisobga olish jurnalini yuritish.

Ruxsat etilgan subyektni identifikatsiyalash uchun kompyuter tizimlarida ko'p hollarda atributivli identifikatorlardan foydalaniladi. Biometrik identifikatsiyalashning oson yo'li – klaviaturada ishlash ritmi orqali aniqlashdir. Atributivli indentifikatorlar ichidan, odatda, quyidagilaridan foydalaniladi:

- parollar;
- yechib olinadigan axborot tashuvchilar;
- elektron jetonlar;
- plastik kartochkalar;
- mexanik kalitlar.

Konfidensial ma'lumotlar bilan ishlaydigan deyarli barcha kompyuterlarda foydalanuvchilarni autentifikatsiyalash parollar yordamida amalga oshiriladi.

Parol – bu simvollar (harflar, raqamlar, maxsus belgilar) kombinatsiyasi bo'lib, uni faqat parol egasi bilishi kerak. Ayrim hollarda xavfsizlik tizimi administratoriga ham ma'lum bo'ladi.

Kompyuterning zamonaviy operatsion tizimlarida paroldan foydalanish o'rnatilgan. Parol avtonom tok manbaiga ega bo'lgan maxsus xotirada saqlanadi. Parollarni taqqoslash operatsion tizim (OT) yuklangunga qadar amalga oshiriladi. Agar buzg'unchi parol saqlanayotgan xotiraning avtonom tok manbaini o'chirib qo'ya olmaganida, ushbu turdagi himoya juda samarali hisoblanar edi. Lekin, kompyuterning OT yuklanishini amalga oshirish uchun kiritiladigan foydalanuvchi parolidan tashqari, Internetda ro'yxati keltirilgan ayrim "texnologik" parollardan ham foydalanish mumkin.

Ko'pgina kompyuter tizimlarida identifikator sifatida, foydalanishga ruxsat etilgan subyektni identifikatsiyalovchi kod yozilgan yechib olinuvchi axborot tashuvchilardan foydalaniladi.

Foydalanuvchilarni identifikatsiyalashda, tasodifiy identifikasiyalash kodlarini hosil qiluvchi – elektron jetonlardan keng foydalaniladi. Jeton – bu, harflar va raqamlarning tasodifiy ketma-ketligini (so'zni) yaratuvchi qurilma. Bu so'z kompyuter tizimidagi xuddi shunday so'z bilan taxminan minutiga bir marta sinxron tarzda o'zgartirib turiladi. Natijada, faqatgina ma'lum vaqt oralig'ida va tizimga faqatgina bir marta kirish uchun foydalanishga yaraydigan, bir martalik parol ishlab chiqariladi. Boshqa bir turdagi jeton tashqi ko'rinishiga ko'ra kalkulyatorga o'xshab ketadi. Autentifikatsiyalash jarayonida kompyuter tizimi foydalanuvchi monitoriga raqamli ketma-ketlikdan iborat so'rov chiqaradi, foydalanuvchi ushbu so'rovni jeton tugmalari orqali kiritadi. Bunda jeton o'z indikatorida akslanadigan javob ketma-ketligini ishlab chiqadi va foydalanuvchi ushbu ketma-ketlikni kompyuter tizimiga kiritadi. Natijada, yana bir bor bir martalik qaytarilmaydigan parol olinadi. Jetonsiz tizimga kirishning imkoni bo'lmaydi. Jetondan foylanishdan avval unga foydalanuvchi o'zining shaxsiy parolini kiritishi lozim.

Autentifikatsiyalash jarayoni kompyuter tizimlari bilan ruxsat etilgan subyekt orasida amalga oshiriladigan muloqotni ham o'z ichiga olishi mumkin. Ruxsat etilgan subyektga bir qator savollar beriladi, olingan javoblar tahlil qilinadi va ruxsat etilgan subyektning aslligi bo'yicha yakuniy xulosa qilinadi.

Kompyuter tizimlari qurilmalaridan foydalanishga ruxsatni masofadan turib boshqarish mumkin. Masalan, lokal tarmoqlarda ishchi stansiyaning tarmoqqa ulanishini administrator ish joyidan turib blokirovka qilishi mumkin. Qurilmalardan foydalanishga ruxsat etishni tok manbaini uzib qo'yish orqali ham samarali boshqarish mumkin. Bunda ishdan boshqa vaqtlarda, tok manbai qo'riqlash xizmati tomonidan nazorat qilinadigan kommutatsiyali qurilmalar yordamida uzib qo'yiladi.

Xulosa qilib aytganda xizmat ko'rsatuvchi xodimning qurilmadan foydalanishiga ruxsat etishni tashkil etish foydalanuvchiga berilgan ruxsatdan farqlanadi. Eng avvalo, qurilma konfidensial ma'lumotlardan tozalanadi hamda axborot almashinish imkonini beruvchi aloqalar uziladi. Qurilmaga texnik xizmat ko'rsatish va uning ish qobiliyatini

tiklash mansabdor shaxs nazorati ostida amalga oshiriladi. Bunda ichki montaj va bloklarni almashtirishga bog'liq ishlarni amalga oshirilishiga jiddiy e'tibor beriladi.

FOYDALANILGAN ADABIYOTLAR:

1. Афанасьев, Алексей Алексеевич Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов. Гриф УМО МО РФ: моногр. / Афанасьев Алексей Алексеевич. - М.: Горячая линия - Телеком, 2017. - 270 с.
2. Рассел, Джесси Единая система идентификации и аутентификации / Джесси Рассел. - М.: VSD, 2016. - 717 с.
3. Васильков, А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум, 2010. - 368 с.
4. Дьяконов, Владимир Matlab. Анализ, идентификация и моделирование систем. Специальный справочник / Владимир Дьяконов , Владимир Круглов. - М.: СПб: Питер, 2002. - 448 с.