KOMPYUTERDA KONFEDENSIAL AXBOROTLARNI SIZIB CHIQISH KANALLARINI NAZORAT QILISH

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 konfedensial axborotlar, maxfiy ma`lumotlarning sizib chiqish kanallari va ularga bo`layotgan tahdidlar, ularning oldini olish yo`llari ko`rib chiqiladi. Tahdidlar o`rganilib chiqiladi.

Kalit so‘zlar: Maxfiy ma'lumotlar manbalari (axborot tarqalishi kanallari), maxfiy ma'lumotlar xavfsizligiga tahdidlar, tahdidlar manbalari, tahdidlarni amalga oshirishning maqsadlari va usullari.

Maxfiy ma'lumotlarning chiqib ketish manbalari va kanallarining xususiyatlari.

Maxfiy ma'lumotlar - kirish Rossiya Federatsiyasi qonunchiligi bilan cheklangan hujjatlashtirilgan ma'lumotlar. Shunga ko'ra, bu ma'lumotlar kiber jinoyatchilarning qiziqish ob'ektiga aylanishi mumkin. Shu sababli, maxfiy ma'lumotlarning chiqib ketish ehtimoli minimallashtiriladigan sharoitlarni yaratish kerak.

Axborot oqish kanali - bu jarayonni tizim xavfsizligini buzadigan tarzda ma'lumotlarni uzatish imkonini beradigan aloqa kanali. Axborotning tarqalishi uch shaklda bo'lishi mumkin:

- axborotni oshkor qilish;
- texnik kanallar orqali oqish;
- ma'lumotlarga ruxsatsiz kirish.

Tizimga kirishning barcha kanallari va ma'lumotlarning chiqib ketish kanallari to'g'ridan-to'g'ri va bilvosita bo'linadi. Bilvosita kanallar deganda, ulardan foydalanish tizim komponentlari joylashgan binolarga kirishni talab qilmaydigan kanallar tushuniladi (masalan, axborot tashuvchilarni yo'qotish, masofadan tinglash, PEMI ni ushlab turish). To'g'ridan-to'g'ri kanallardan foydalanish uchun kirish kerak (bu insayderlarning harakatlari, ruxsatsiz nusxa ko'chirish va boshqalar bo'lishi mumkin).Agar raqobatchi tashkilot manfaatdor bo'lsa, shuningdek, tajovuzkorga ma'lumotlar ustidan nazoratni qo'lga kiritish imkonini beradigan shartlar mavjud bo'lsa, maxfiy ma'lumotlarning chiqib ketishi sodir bo'lishi mumkin.

Bunday holatlarning paydo bo'lishi vaziyatlarning tasodifiy tasodifi va dushmanning qasddan harakatlari tufayli mumkin. Maxfiy ma'lumotlarning asosiy manbalari quyidagilardir:

- maxfiy ma'lumotlarga ruxsat berilgan korxona xodimlari;
- maxfiy ma'lumotlarning moddiy tashuvchilari (hujjatlar, mahsulotlar);
- maxfiy ma'lumotlarni saqlash va qayta ishlash uchun texnik vositalar;
- maxfiy ma'lumotlarni uzatish uchun foydalaniladigan aloqa vositalari;
- maxfiy ma'lumotlarni o'z ichiga olgan aloqa kanallari orqali uzatiladigan xabarlar.

Maxfiy ma'lumotlarga asosiy tahdidlarga oshkor qilish, sizib chiqish va ruxsatsiz kirish kiradi. Maxfiy ma'lumotlar xavfsizligiga tahdid deganda, ma'lumotlarning tarqalishi va (yoki) ruxsat etilmagan va (yoki) ko'zda tutilmagan ta'sirlar bilan bog'liq potentsial yoki real tahdidni yaratadigan shartlar va omillar majmui tushuniladi. **Axborot xavfsizligi sohasidagi zaifliklarni tahlil qilish.** Samarali axborot xavfsizligi nafaqat korxona tarmog'idan har qanday ma'lumotlarni o'g'irlashdan himoya qilishni, balki butun biznesni moliyaviy himoya qilishni ham ta'minlaydi. Yuqori sifatli axborot xavfsizligi bilan ajralib turishni istagan korxonalar doimiy ravishda quyidagilarning oldini olish ustida ishlamoqda:

- har qanday korporativ ma'lumotlar sizib chiqishi;
- himoyalangan ma'lumotlarni masofadan tahrirlash;
- investorlar, yetkazib beruvchilar, kontragentlar va boshqalar o'rtasida ishonchni yo'qotishi mumkin bo'lgan tahdidlardan himoya darajasining o'zgarishi;

Tahdidlar bir nechta manbalarga ega bo'lishi mumkin, shuning uchun ularni o'z vaqtida tasniflash va ularni tahlil qilish sxemasini yaratish juda muhimdir. Bu korxonaning biznes-jarayonlarida yuzaga kelishi mumkin bo'lgan zaifliklarning eng keng qamrovini ta'minlaydi. Bunday tahdidlar alohida sinflarga bo'linadi.

1-sinf. Potentsial tahdid manbai bo'lishi mumkin:to'g'ridan-to'g'ri axborot tizimida (AT) AT ko'rinishida (masalan, ruxsatsiz ovoz yozish uchun qurilmalar) ***2-sinf***.AT ga ta'siri quyidagilar bo'lishi mumkin: faol tahdid (troyan, virus)passiv tahdid (tajovuzkor tomonidan maxfiy ma'lumotlarni nusxalash)

3-sinf. Amalga oshirish mumkin bo'lgan kirish usuli:

- to'g'ridan-to'g'ri (parollarni o'g'irlash)
- nostandart aloqa kanallari orqali (masalan, operatsion tizim zaifliklari)

Axborotning chiqib ketish kanallari - axborot tizimidan axborot chiqib ketish usullari va usullari; parazitar (keraksiz) axborot tashuvchilar zanjiri, ulardan biri yoki bir nechtasi (bo'lishi mumkin) huquqbuzar yoki uning maxsus jihozlari. Ular axborot xavfsizligi omili sifatida axborotni himoya qilishda katta rol o'ynaydi. Ma'lumotlarning tarqalishining barcha kanallarini bilvosita va to'g'ridan-to'g'ri ajratish mumkin. Bilvosita kanallar axborot tizimining texnik vositalariga bevosita kirishni talab qilmaydi. To'g'ridan-to'g'ri mos ravishda axborot tizimining apparat va ma'lumotlariga kirishni talab qiladi. Oqishning bilvosita kanallariga misollar:

- Saqlash vositalarini o'g'irlash yoki yo'qotish, buzilmagan axlatni tekshirish;
- Masofadan suratga olish, tinglash;
- Elektromagnit nurlanishning tutilishi.

Axborotni himoya qilish usullari.

Axborotni texnik kanallar orqali sizib chiqishidan himoya qilish konstitutsiya va qonunlar asosida amalga oshiriladi va himoya mualliflik guvohnomalari, patentlar, tovar belgilarining mavjudligi bilan ham ta'minlanadi. Rossiyada axborotlashtirish ob'ektida axborotni himoya qilish talablarini asoslash uchun himoyalangan ma'lumotlarga ta'sir qiluvchi omillarning tasnifi va ro'yxatini belgilaydigan standart mavjud. Ushbu standart faoliyatning turli sohalarida (mudofaa, iqtisod, fan va boshqa sohalarda) foydalaniladigan axborotlashtirish ob’ektlarini yaratish va ulardan foydalanish jarayonida axborot xavfsizligini tashkil etish talablariga nisbatan qo‘llaniladi.

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.
4. www.intuit.ru.
5. www.infosec.ru.
6. www.securityfocus.com.
7. http://www.cryptopro.ru/.