Sulaymonov Zafarjon Raxmonberdiyevich va Umurzaqov Bahrom Burxonovich
UNIVERSITY OF MENAGEMENT AND FUTURE TECHNOLOGIES
2-bosqich Magistrlari

SULAYMONOV Zafarjon Rakhmonberdiyevich and UMURZAKOV Bahrom Burkhonovich
2nd-year Master's Students of the University of Management and Future Technologies

MA'LUMOTLAR BAZASIDA KIBER XAVFSIZLIK TUSHUNCHASI

Annotatsiya: Ushbu maqolada ma'lumotlar bazasida axborot xavfsizlikgini ta'minlash va kiberxavfsizligi tushunchasi tahlili keltirilgan.

Kalit so'zlar: Kiberjinoyatchilik tushunchasi,ma'lumotlar bazasi, kiberxavfsizlik, ma'lumotlar bazasini ta'minlash, kiber makon tushunchasi

CONCEPT OF CYBER SECURITY IN DATABASES

Abstract: This article provides information security in the database and an analysis of the concept of cyber security is presented.

Keywords: Concept of cybercrime, database, cyber security, database security, concept of cyberspace.

Axborot xavfsizligi tushunchasi kundan kunga glaballashib bormoqda, ayniqsa kundan-kunga axborot xurujlari va kiberjinoyatlar sonining ortib borishi xavfsizlik tushunchasining qanchalik glabal ekanligini ko'rsatmoqda. Axborot turli shakilda va turli saqlovchilarda saqlanishi mumkin, - bu axborotni saqlashning yangi texnologiyalarini ishlab chiqishni talab qiladi. Axborotni ma'lumotlar bazasida himoylash murakkab va texnologik jarayondir.

Kiberjinoyatchilikning, bizga ma'lum bo'lgan virusli dasturlarni tarqatish, parollarni buzib kirish, kredit karta va boshqa bank rekvizitlaridagi mablag'larni o'zlashtirish talon-toroj qilish, shuningdek, internet orqali qonunga zid axborotlar, xususan, bo'hton, ma'naviy buzuq ma'lumotlarni tarqatish bilan bashariyat hayotiga katta xavf solayotganidan ko'z yuma olmaymiz.

"Kiberjinoyatchilik" tushunchasi - axborot-kommunikatsiya texnologiyalari vositalaridan foydalangan holda, virtual tarmoqda dahshat solish, virus va boshqa zararli dasturlar, qonunga zid axborotlar tayyorlash va tarqatish, elektron xatlarni ommaviy tarqatish (spam), xakkerlik hujumi, veb-saytlarga noqonuniy kirish,

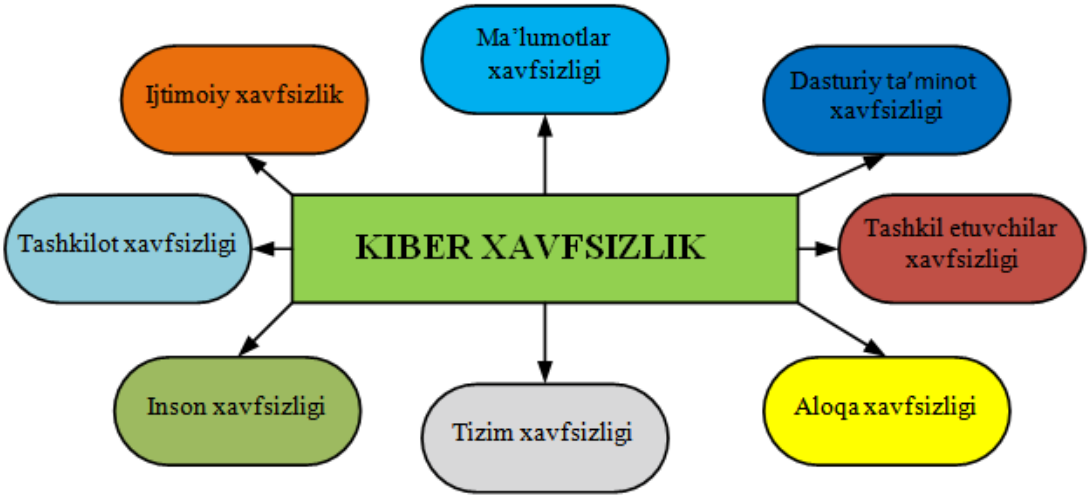
firibgarlik, ma’lumotlar butunligi va mualliflik huquqini buzish, kredit kartochkalari raqami hamda bank rekvizitlarini o‘g‘irlash *(fishing va farming)* va boshqa turli huquqbuzarliklar bilan izohlanadi.

Ma’lumotlar bazasi xavfsizligi deganda – ma’lumotlar bazasining maxfiyligi, yaxlitligi va mavjudligini o‘rnatish va saqlash uchun mo‘ljallangan vositalar, boshqaruv vositalari va chora-tadbirlar majmuasi tushuniladi.

Axborotni ma’lumotlar bazasida xavfsizligi quyidagilarni hal qilishi va himoya qilishi quyidagilardan iborat:

- Ma’lumotlar bazasidagi ma’lumotlar;
- ma’lumotlar bazasini boshqarish tizimi (DBMS);
- har qanday bog‘liq ilovalar;
- jismoniy ma’lumotlar bazasi serveri *va/yoki* virtual ma’lumotlar bazasi serveri va asosiy uskuna;
- ma’lumotlar bazasiga kirish uchun foydalaniladigan hisoblash *va/yoki* tarmoq infratuzilmasi.

Ma’lumotlar bazasi xavfsizligi axborot xavfsizligi texnologiyalari va amaliyotlarining barcha jihatlarini o‘z ichiga olgan murakkab va qiyin ishdir. Bundan tashqari, bu ma’lumotlar bazasidan foydalanishga to‘g‘ri kelmaydi. *Ma’lumotlar bazasi qanchalik qulay va foydalanish mumkin bo‘lsa,* u xavfsizlik tahdidlariga nisbatan zaifroq bo‘ladi, ma’lumotlar bazasi tahdidlarga qanchalik daxlsiz bo‘lsa, unga kirish va undan foydalanish shunchalik qiyin bo‘ladi.



1-rasm. Kiberxavfsizlikning bilim sohalari.

Kundan-kunga takomillashib ketayotgan kiberjinoyatchilikka qarshi kiberxavfsizlikni ta’minlashda quyidagi asosiy talablarni bajarish orqali ulardan himoyalanish, ya’ni kiberxavfsizlikni ta’minlashimiz mumkin:

- xodimlarga axborot xavfsizligi asoslarini o‘rgatish;
- foydalanayotgan dasturiy mahsulotlarning zaifliklarini doimiy sinovdan o‘tkazish;
- ishonchli antivirus dasturidan foydalanish;
- litsenziyalangan rasmiy dasturlardan foydalanish;
- axborot tizimlarini himoyalashda ko‘p faktorli autentifikatsiyadan foydalanish;
- parollardan foydalanishda kuchli parolni saqlash siyosatiga rioya qilish;
- muntazam ravishda kompyuter qattiq disklaridagi ma’lumotlarni shifrlash.

Ko‘pgina dasturiy ta’minotning noto‘g‘ri konfiguratsiyasi - zaifliklar yoki ehtiyotsizlik yoki noto‘g‘ri foydalanish shakllari buzilishlarga olib kelishi mumkin.

Quyida ma’lumotlar bazasi xavfsizligi hujumlarining eng keng tarqalgan turlari yoki sabablari va ularning sabablari keltirilgan:

- Ichki tahdidlar;
- **Insayder tahdid**- bu ma’lumotlar bazasiga imtiyozli kirish huquqiga ega bo‘lgan uchta manbadan birining xavfsizlikka tahdididir;
- zarar yetkazmoqchi bo‘lgan yomon niyatli insayder;

- ma’lumotlar bazasini hujumga qarshi himoyasiz qiladigan xatolarga yo‘l qo‘yadigan beparvo insayder;

- **Infiltrator**-bu qandaydir tarzda fishing kabi sxema orqali yoki hisob ma’lumotlari, ma’lumotlar bazasiga kirish orqali hisob ma’lumotlarini oladigan begona shaxs;

ma’lumotlar bazasiga xos tahdid bo‘lib, ular veb-ilovalar yoki HTTP sarlavhalari tomonidan xizmat ko‘rsatadigan ma’lumotlar bazasi so‘rovlariga o‘zboshimchalik bilan SQL yoki SQL bo‘lmagan hujum satrlarini kiritishni o‘z ichiga oladi. Xavfsiz veb-ilovalarni kodlash amaliyotiga rioya qilmaydigan va muntazam zaiflik sinovlarini o‘tkazadigan tashkilotlar ushbu hujumlarga ochiq.

Ma’lumotlar bazasi xavfsizligi axborot xavfsizligi texnologiyalari va amaliyotlarining barcha jihatlarini o‘z ichiga olgan murakkab va qiyin ishdir. Bundan tashqari, bu ma’lumotlar bazasidan foydalanishga to‘g‘ri kelmaydi. Ma’lumotlar bazasi qanchalik qulay va foydalanish mumkin bo‘lsa, u xavfsizlik tahdidlariga nisbatan zaifroq bo‘ladi, *ma’lumotlar bazasi tahdidlarga qanchalik daxlsiz bo‘lsa,* unga kirish va undan foydalanish shunchalik qiyin bo‘ladi.

Ruxsatlarni boshqarish - axborot tizimlari va axborot texnologiyalarining barcha resurslaridan foydalanishni tartibga solish orqali himoyalash usuli. Bunday usullar, axborotga bo‘lgan barcha ruxsat etilmagan kirish imkoniyatlarini bartaraf eta olishi lozim. Ruxsatlarni boshqarish quyidagi himoya funksiyalarini o‘z ichiga qamrab oladi:

foydalanuvchilarni, xodimlarni va tizim resurslarini identifikatsiyalash (har bir ob’ektga shahsiy identifikator berish);

ob’ekt yoki sub’ektlarni ularga berilgan identifikator orqali tanib olish (haqiyiyligini ta’minlash);

foydalanish huquqiga egaligini tekshirish;

himoyalangan resurslarga bo‘lgan murojaatlarni ro‘yhatga olish;

ruxsat etilmagan kirishlarga urinish harakatlari bo‘lgan vaqtda sezish (signalli ogohlantirish, tizimni o‘chirish, tizim ishini to‘htatib qo‘yish, so‘rovlarga javob bermaslik).

Identifikatsiya va autentifikatsiya

Identifikatsiya va autentifikatsiyani xavfsizlikning muhim dasturiy-texnik vositasi deb hisoblash mumkin, modomiki qolgan servislar sub’ektlarning o‘zigagina mo‘ljallangan. Identifikatsiya va autentifikatsiya - bu korxonaning axborot maydoniga kirishning, boshlang‘ich himoya chizig‘idar.

Identifikatsiya va autentifikatsiya protsedurasining birgalikda bajarilishini **avtorizatsiya protsedurasi** deb qabul qilingan**.**

Identifikatsiya sub'ektlarga (foydalanuvchilarga, jarayonlarga, ma'lum bir foydalanuvchi nomidan harakat qiluvchilarga) o'zini kimligini ma'lum qilish imkonini beradi. Autentifikatsiya orqali ikkinchi tomonni aslida kim ekanligini bilish imkonini beradi. Ba'zan "autentifikatsiya" iborasining sinonimi sifatida "haqiqiyligini tekshirish" iborasi ishlatiladi.

Autentifikatsiya ikki hil bo'ladi, bir tomonlama (odatda klient haqiqiyligini serverga isbotlaydi) va ikki tomonlama (ikki tomon ham bir birini haqiqiyligini isbotlaydi) bo'ladi. Bir tomonlama autentifikatsiya protsedurasiga misol qilib foydalanuvchilarning tizimga kirish holatini keltirish mumkin.

Ochiq tarmoq muhitida tomonlar o'rtasidagi identifikatsiyalash, autentifikatsiyalashda ishonchli marshrut mavjud emas. Tarmoqlarda passiv va aktiv bo'lgan tinglashlardan, ya'ni ma'lumotlarni **ushlab qolish**, **o'zgartirish** va **qayta ishlashdan** himoyalashni ta'minlash zarur hisoblanadi.

Zamonaviy identifikatsiya va autentifikatsi vositalari, tarmoqqa markazlashtirilgan holda kirish konsepsiyasini qo'llashi kerak. Tarmoqga markazlashtirilgan holda kirish - bu, birinchi o'rinda foydalanuvchilarga qulaylik yaratish talabi hisoblanadi. Agar korporativ tarmoqda ko'plab axborot servislar, murojatlarni bir-biridan mustaqil ravishda amalga oshirsa, u holda identifikatsiya va autentifikatsiyalash juda qiyin kechadi.

Kompyuter tizimlarida autentifikatsiya usullaridan biri, foydalanuvchi identifikatorini kiritish orqali, oddiy nom bilan aytganda login (inglizcha - foydalanuvchining ro'yhatga olinuvchi nomi) va parol - qandaydir maxfiy ma'lumot hisoblanadi. Ishonchli parol va login juftligi maxsus ma'lumotlar bazasida saqlanadi.

Rivojlanayotgan IT muhiti ma'lumotlar bazalarini tahdidlarga nisbatan sezgirroq qiladi. Ma'lumotlar bazalariga hujumlarning yangi turlariga olib kelishi mumkin bo'lgan yoki yangi mudofaa choralarini talab qilishi mumkin bo'lgan tendentsiyalar:

O'sib borayotgan ma'lumotlar hajmi - saqlash, ma'lumotlarni yig'ish va qayta ishlash deyarli barcha tashkilotlarda eksponent ravishda o'sib bormoqda. Har qanday ma'lumotlar xavfsizligi amaliyoti yoki vositalari uzoq va yaqin kelajakdagi talablarni qondirish uchun yuqori darajada kengaytirilishi kerak.

Tarqalgan infratuzilma - tarmoq muhitlari murakkablashib bormoqda, ayniqsa korxonalar ish yuklarini gibrid bulut yoki ko'p bulutli arxitekturaga o'tkazar ekan, bu xavfsizlik yechimlarini joylashtirish, boshqarish va tanlashni qiyinlashtiradi.

Borgan sari qat'iy tartibga soluvchi talablar - butun dunyo bo‘ylab tartibga solishga muvofiqlik landshafti murakkablashib bormoqda, shuning uchun barcha mandatlarga rioya qilish yanada qiyinlashmoqda.

Kiberxavfsizlik bo‘yicha ko‘nikmalar yetishmasligi - global kiberxavfsizlik bo‘yicha malakali mutaxassislarning etishmasligi va tashkilotlar xavfsizlik rollarini to‘ldirishda qiynalmoqda. Bu muhim infratuzilmani, jumladan ma'lumotlar bazalarini himoya qilishni qiyinlashtirishi mumkin.

Xulosa

Bugungi kunda mamlakatimizda joriy etilayotgan zamonaviy raqamli texnologiyalar, fuqarolarimizga qator qulayliklar va imkoniyatlar eshigini ochmoqda.

Shu o‘rinda ma'lumotlar bazasida kiber xavfsizlik, kiberterrorizm va uning jamiyat hayotiga solayotgan xavfining ko‘lami ham oshib borayotganini ta'kidlash joiz. Kiberterroristik harakat (kiber hujum)-kompyuterlar va axborot kommunikatsiya vositalari yordamida amalga oshirilgan, odamlarning hayoti va sog‘lig‘iga bevosita xavf tug‘diradigan yoki potensial xavf tug‘dirishi mumkin bo‘lgan, moddiy ob'ektlarga katta zarar yetkazishi yoki shunga olib kelishi mumkin bo‘lgan, ijtimoiy xavfli oqibatlarning boshlanishi yoki maqsadi bo‘lgan siyosiy sababdir. Zamonaviy terrorchilar uchun kibermakondan foydalanishning jozibadorligi kiberhujumni amalga oshirish katta moliyaviy xarajatlarni talab qilmasligi bilan bog‘liq. Kiberxavfsizlikni ta'minlash, sodir etilishi mumkin bo‘lgan kiberjinoyatlarning oldini olish va unga qarshi kurashish masalasi hisoblanadi.

Foydalanilgan adabiyotlar ro‘yxati.

1. O‘zbekiston Respublikasi Prezidentining “Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to‘g‘risida”gi qarori.

2. O‘zbekiston Respublikasi Axborotlashtirish va telekommunikatsiyalar sohasida nazorat bo‘yicha davlat inspeksiyasi to‘g‘risidagi nizom.

3. Kessler, Gari “Kriptografiyaga umumiy nuqta” (2006-yil 17-noyabr).

4. А. Соколов, О. Степанюк. Зашита от компьютерного терроризма. Справочное пособие. БХВ-Петербург. Арлит, 2002 г.

5. А.А. Петров. Компьютерная безопасность. Криптографические методи зашиты. М.: ДМК Пресс, 2000 г.

6. “Axborot texnologiyasi, Axborotlarni kriptografik muhofazasi, Ma’lumotlarni shifrlash algoritmi” Toshkent.