13-MA’RUZA. OPERATSION TIZIMLARDA XAVFSIZLIK

Reja:

- Xavfsizlik muammosi.
- Autentifikatsiya
- Dasturiy tahdidlar (hujumlar)
- Tizimli tahdidlar (hujumlar)

Xavfsizlik – bugungi kunda kundalik faoliyat va biznesning kompyuter texnologiyalariga kuchli bog'liqligi hamda tarmoq hurujlari (kiberjinoyatchilik) soni keskin ko'payib borayotganligi sababli IT sohasidagi eng dolzarb muammolardan biri hisoblanadi. Xavfsizlik, hujumlarning asosiy maqsadi sifatida operatsion tizimlar va tarmoqlar uchun juda muhimdir.

Xavfsizlik muammosi

Xavfsizlik (security) – bu tashqi hujumlardan himoyadir. Hozirgi vaqtda ma'lumotlarning yaxlitligiga, ularga bog'liq kompyuter tizimlari va kompaniyalarning sog'lig'iga, odamlarning farovonligi va shaxsiy xavfsizligiga tahdid soladigan turli xil xakerlik hujumlari soni sezilarli darajada ko'paymoqda. Hujumlardan himoya qilish uchun maxsus xavfsizlik choralari, kompyuter texnologiyalari va vositalari zarur.

Har qanday kompyuter tizimida tizimning tashqi muhitini tekshirishi va uni quyidagilardan himoya qilishi kerak bo'lgan xavfsizlik quyi tizimi bo'lishi kerak.

- Ruxsatsiz kirish
- Zararli o'zgartirish yoki buzib tashlash
- Noto'g'ri ma'lumotlarni tasodifiy kiritish.

Amaliyot shuni ko'rsatadiki, ma'lumotni zararli shikastlanishdan ko'ra, tasodifan himoya qilish osonroq.

Аутентификация

- Xavfsizlikning eng keng qo'llaniladigan usullaridan biri bu **autentifikatsiya (authentication)** – tizimga kirishda foydalanuvchilarni identifikatsiya qilish. Bunday foydalanuvchi identifikatsiyasi ko'pincha tizimga kirish uchun ro'yxatdan o'tgan foydalanuvchi **logini va paroli** orqali har bir kirish bilan bog'liq bo'lgan maxfiy kod so'zlari orqali amalga oshiriladi.

- Parollardan foydalanishning asosiy printsipi shundaki, ular sir saqlanishi kerak. Shuning uchun, xakerlarga hujum qilishning an'anaviy maqsadlaridan biri foydalanuvchidan foydalanuvchi nomi va parolini har qanday usul bilan topishdir.

Parolni tez-tez o'zgartirish. Bunday choralar harbiy yurushlar paytida ham qo'llanilgan.

Aksariyat saytlar va boshqa tizimlar (masalan, Microsoft firmasining hamkorlari sayti) foydalanuvchilardan parollarni doimiy ravishda o'zgartirishni talab qiladi (masalan, kamida uch oyda bir marta), aks holda saytga kirish uchun bloklanadi.

Murakkab parollardan foydalanish. Deyarli barcha tizimlar ro'yxatdan o'tishda foydalanuvchidan osonlikcha taxmin qilinmaydigan parollarni o'rnatishni talab qiladi: masalan, parol, qoida tariqasida, katta va kichik harflar va raqamlar, maxsus belgilarni o'z ichiga olishi va kamida 7-8 belgidan iborat bo'lishi kerak. Avtomatik aniqlanadigan parollardan foydalanish.

.

Kirish uchun yaroqsiz urinishlarni saqlash. Ko'pgina tizimlarda login va parollarni kiritishdagi barcha noto'g'ri urinishlar qayd etiladigan tizim jurnali mavjud. Odatda bunday urinishlarning aniq soni beriladi (masalan, uchta).

Parollarni shifrlash yoki kirish uchun faqat **bir marta ruxsat berilishi** mumkin, shundan so'ng foydalanuvchidan parolni o'zgartirish talab qilinadi.

Dasturiy tahdidlar (hujumlar)

Xakerlar tomonidan qo'llaniladigan tahdidlar va hujumlarning odatdagi turlarini ko'rib chiqamiz.

Troyan dasturi (Trojan Horse) – bu ba'zi foydali dasturlarni "qalbakilashtiradigan", ammo noo'rin ishga tushirilganda (zararli) atrof muhitidan foydalanadigan, masalan, maxfiy ma'lumotlarni qabul qiladigan va ishlatadigan hujum qiluvchi dastur. Troyan dasturlar bitta foydalanuvchi tomonidan yozilgan dasturlarni boshqa foydalanuvchilar tomonidan bajarilishini ta'minlash uchun tizim mexanizmlaridan foydalanadilar.

Tuzoqqa kirish (Trap Door) - xavfsizlik tekshiruvidan qochish uchun foydalanuvchi nomi yoki paroldan foydalanish.

Stek va buferdan oshib ketish (Stack and Buffer Overflow) - uning yaxlitligini buzish uchun boshqa foydalanuvchi yoki jarayonning xotirasiga kirish uchun dasturdagi xatolik (xotirasida stek yoki buferlarning to'lib qolishi).

Tizimli tahdidlar (hujumlar)

Tizimli dasturlarning zaifliklaridan **(vulnerabilities)** foydalanadigan ba'zi odatdagi hujumlarni - xatolar va kamchiliklar hujumlarni tashkil qilishga imkon beradi. Ularni quyida

ko'rib chiqamiz

Qurtlar (Черви, Worms) - bu o'z-o'zini takrorlash (ko'paytirish) mexanizmlaridan foydalanadigan zararli dasturlar. Masalan, Internet qurtlaridan biri UNIX tarmoq (masofaviy kirish) imkoniyatlari hamda **finger** va **sendmail** dasturlaridagi xatolardan foydalanadi. Uning ishlash printsipi quyidagicha: doimiy ravishda tarmoqda ishlatiladigan ba'zi bir tizim dasturlari qurtning asosiy dasturini tarqatadi.

Viruslar - bu dasturlarning va butun kompyuter tizimini ishdan chiqarish maqsadida dasturlarga kiritilgan kod bo'laklaridir. Viruslar asosan mikrokompyuter tizimlariga ta'sir qiladi. Viruslar umumiy foydalanish mumkin bo'lgan saytlardan yoki "infeksiya" bo'lgan disklardan yuklab olinadi.

Kompyuter viruslari bilan yuqtirishni oldini olish uchun kompyuterlardan foydalanganda xavfsizlik tamoyillariga rioya qilish kerak (**safe computing**) - antivirus dasturlaridan, himoya vositalaridan doimiy ravishda .exe, .doc va boshqa xotirada saqlanadigan va ochilgan har bir faylni viruslarni qidiradigan dasturlardan foydalanish lozim.

Xizmatni rad etish **(Denial of Service – DoS)** - bu serverni to'g'ri ishlashiga yo'l qo'ymaslik uchun uni sun'iy ravishda ortiqcha yuklaydigan server hujumlarining keng tarqalgan turlaridan biri. Masalan, veb-server uchun bunday hujum sun'iy ravishda bir million "GET" so'rovini yaratishi mumkin. Agar server ishonchli ishga tushirilmasa, bunday hujum ko'pincha server xotirasini to'ldirish va uni qayta yuklashga olib keladi.

Tarmoq hujumlarining turlari

Foydalanuvchilarning doim kuzatib turishlari kerak bo'lgan zamonaviy tarmoq hujumlarining ba'zi turlarini ko'rib chiqamiz.

Phishing - bu foydalanuvchining maxfiy ma'lumotlarini foydalanuvchining o'zi tomonidan aldash orqali o'g'irlashga urinish. Hatto **phishing** so'zining o'zi buzilgan so'z bilan baliq ovlash, ya'ni ushbu texnikadan foydalangan xaker haddan tashqari sodda foydalanuvchini "o'lja" sifatitida ushlaydi. Masalan, foydalanuvchini o'z xabarida uning login va parolini, kredit kartasini yoki bank hisob raqamini xavf ostiga qo'yganidan qo'rqitib, xaker foydalanuvchiga javob sifatida ba'zi maxfiy ma'lumotlarni kiritishi va yuborishi uchun harakat qiladi.

- Odatda, **phishing-xabar** (elektron pochta xabari) bank nomidan kelib chiqadi va bank veb-saytida ishlatilgan ranglar, logotiplar va boshqalarga mos kelishi uchun soxtalashtiriladi.
- Biroq, uni ochish uchun, odatda sichqoncha kursorini taqdim etilgan veb-havolaga yoki elektron pochta manziliga olib borish kifoya va manzil bankka ishora qilmasligiga ishonch hosil qiling. U butunlay begona saytga yoki elektron pochta bo'lib chiqadi.

- Shuning uchun foydalanuvchilar ehtiyot bo'lishi kerak. Agar bir xil elektron pochta manzillaridan **phishing** muntazam ravishda kelib tursa, yana bir samarali choralar elektron pochta serveridagi ushbu manzillarni qora ro'yxatga olish kerak.

Pharming - foydalanuvchini zararli veb-saytga yo'naltirish (odatda **phishing** maqsadida). zamonaviy veb-brauzerlarda phishingga qarshi dasturlari o'rnatilgan bo'lib, ular saytga kirishda avtomatik ravishda ishga tushiriladi. Garchi foydalanuvchining biroz vaqtini olsada, bunday choralar ko'plab hujumlarning oldini olishga yordam beradi.

Ma'lumotlarni buzish (**Tampering with data**)- ma'lumotlarni zararli ravishda buzish.

Axborotni kriptografiya qilish bu kabi hujumlarga qarshi kurashishning samarali chorasi hisoblanadi.

Spoofing - ma'lum bir foydalanuvchi uchun "soxta" (uning login, parol va vakolatidan zararli foydalanish). Kirish va parol foydalanuvchidan firibgarlik yo'li bilan olinadi (masalan, phishing natijasida) yoki xakerlik dasturi tomonidan "buzib kirilgan" tizim faylidan olinadi.

Imtiyozni ko'tarish (Elevation of privilege) - buzg'unchi harakatlar maqsadida vakolatlarni kengaytirishga urinish (masalan, tizim ma'muri vakolatiga). Shuning uchun har qanday kompyuter tizimidagi eng maxfiy ma'lumot bu tizim ma'murining paroli bo'lib, uni juda ehtiyotkorlik bilan himoya qilish kerak.

Ishonchli hisoblash tashabbusi (Trustworthy Computing (TWC) Initiative)

Xavfsiz va ishonchli hisoblash tashabbusi 2002 yilda Microsoft asoschisi Bill Geytsning kompaniyaning barcha xodimlariga elektron pochta orqali yuborilgan. TWC tashabbusining asosiy yo'nalishi shundan iboratki, dasturiy ta'minot tizimini ishlab chiqishda xavfsizlikni ta'minlashga dastlabki bosqichlardanoq alohida e'tibor berish kerak. Biroq, TWC tashabbusi bu bilan cheklanib qolmaydi - uning mazmuni va maqsadlari ancha kengroq bo'lib, iqtisodiy, huquqiy jihatlar va "inson omili" ni qamrab oladi.

TWC bo’yicha:

Xavfsizlik (Security):

- har qanday dasturiy ta'minot tizimida tashqi hujumlardan samarali himoya choralarini amalga oshirish va ulardan foydalanish;
- ushbu maqsadga erishishga qaratilgan dasturlarni ishlab chiqishning maxsus usullaridan foydalanish.

Axborotning maxfiyligini saqlash (Privacy):

- dasturiy ta'minot tomonidan shaxsiy va korporativ ma'lumotlardan faqat foydalanuvchining roziligi bilan va faqat o'zi uchun tushunarli bo'lgan huquqiy maqsadlarda foydalanish;
- hujum natijasida maxfiy ma'lumotlarni xakerlikdan himoya qilish.

Ishonchlilik (Reliability):

- Dasturiy ta'minot tizimlarining xatti-harakatlarining oldindan aytib berilishi, bu ma'lum bir sharoitda dasturning kutilgan to'g'ri xatti-harakatlarini ta'minlashi kerak.
- Microsoft o'zining TWC tashabbusi bilan, boshqa barcha kompaniyalar va individual dasturchilarni ushbu taklif qilingan printsiplarga rioya qilishga chaqirdi, garchi dastlab dunyoda TWC tashabbusiga nisbatan munosabat juda ehtiyotkor va hatto shubha bilan qarashgan bo'lsa ham.
- Microsoft TWCni qo'llab quvvatlash uchun universitetlarвф TWCni o'qitishni moliyalashtirdi. Shuni ta'kidlash kerakki, dunyoda universitetlarda TWC o'qitish boshlanganiga ko'p bo'lmadi. Universitetlarda ushbu masalalarga eng katta e'tibor birinchi navbatda harbiy sohalarga qaratildi.
- Universitetlarda TWC elementlarini orgatish uchun "Dasturlar va bilimlar arxitekturasi va modellari", "Operatsion tizimlar va tarmoqlar", "Java texnologiyasi", "Kompilyatorlar" degan fanlar o'qitila boshlandi.

Biznesning samaradorligi, qonuniyligi va to'g'riligi (Business Integrity) - dasturiy ta'minot mahsulotlarini qo'llab-quvvatlash guruhining samaradorligi va foydalanuvchilarning xavfsizlik masalalari bo'yicha o'z vaqtida maslahatlari; dasturiy ta'minot ishlab chiqaruvchisi - kompaniya biznesining to'g'riligi.

Microsoft o'zi 2002 yildan beri xavfsiz dasturiy ta'minotni ishlab chiqish uchun yangi hayot sikli sxemasi - **SDLC (Security Development Life Cycle)** dan foydalangan holda dasturiy ta'minotni ishlab chiqishda ish jarayonlarini butunlay qayta tashkil etdi. TWC tamoyillari Microsoft mahsulotlarining barcha yangi versiyalarida o'z aksini topgan: Internet Explorer 7 va 8, Windows Vista va boshqalar.

Dasturiy ta'minotga tahdid va hujumlarni oldindan tahlil qilish va modellashtirish va ularga qarshi choralarni ishlab chiqish zarur. Ishonchliligi va xavfsizligi nuqtai nazaridan xavfni miqdoriy baholash vositalariga ehtiyoj bor.

- Dasturiy ta'minotni sinovdan o'tkazishning maxsus turlari talab qilinadi - **security testing, fuzzy testing (fuzzing),** xakerlarning IP-manzil va kompyuter tizimining boshqa komponentlarini buzishga harakatlariga tahlid qilish.
- Xavfsizlik bo'yicha ishlanmada ishtirok etgan ekspertlarning xizmatidan foydalanish lozim.
- Microsoft xavfsiz dasturlarni baholash va ishlab chiqish, tahdid va hujumlarni baholash va hujum oqibatlarini baholash uchun bir qator oddiy xavfsizlik sxemalarni taklif qildi.

SD3C sxemasi (formulasi) xavfsiz dasturiy ta'minotni ishlab chiqishning asosiy tamoyillarini belgilaydi:

- **Secure in Design** - xavfsiz dizayn tamoyillarini qo'llash; mumkin bo'lgan hujumlarni hisobga olish; ularni aniqlash usullarini amalga oshirish;
- **Secure by Default** - standart xavfsizlik sozlamalarini qo'shish;
- **Secure in Deployment** - dasturiy ta'minotni xavfsiz tarqatish va o'rnatish;
- **Communication** - mahsulotni qo'llab-quvvatlash guruhining foydalanuvchilar bilan doimiy o'zaro aloqasini ta'minlash, xavfsizlikning aniqlangan xatolariga nisbatan mahsulotning yangi versiyalarini ishlab chiqish; xavfsizlikni sozlash bo'yicha tavsiyalar berish.

Tahdidlar va hujumlar tasnifi (STRIDE)

Microsoft **STRIDE** formulasidan foydalanib, tahdid va hujumlarni tasniflashni taklif qiladi:

- **Spoofing** - harflar: parodiya, pranking - ma'lum bir foydalanuvchi uchun "soxta"; masalan, foydalanuvchining haqiqiyligini tasdiqlaydigan operatsiyani takrorlash.
- **Tampering** - hujum uchun ma'lumotlarni ruxsatsiz o'zgartirish; masalan, yangi foydalanuvchi qo'shish uchun autentifikatsiya fayllarini o'zgartirish.
- **Repudiation** - tom ma'noda qat'iyan kelishmovchilikni, rad etishni, rad etishni anglatadi - xavfsizlik buzilishiga olib kelishi mumkin bo'lgan xatti-harakatlar tizimida qayd etilmasligi.
- Operatsion tizimda driver xavfsizlikni buzishga olib keladigan biror holatni qayd qilmasa, rad etish xavfi tug'ilishi mumkin. Masalan, fokusni o'zgartirish va rasm hajmini

kamaytirish uchun so'rovlarni qabul qilmaydigan video qurilma drayveri (bu tasvir buzilishiga olib kelishi mumkin).

- **Information disclosure** - maxfiy ma'lumotlarga ruxsatsiz kirish; Masalan: Bank mijozlarining kredit kartalari raqamlari ro'yxatini olish.
- **Denial of service** - xizmatni rad etish; masalan: xesh algoritmining kamchiliklaridan foydalanib, protsessorni haddan tashqari yuklanish ta'siriga ataylab erishish.
- **Elevation of privilege** - Imtiyozlarni oshirish (tizim ma'muri huquqlarini ruxsatsiz berish). Misol: buyruqlaringizni bajarish uchun imtiyozli dasturni ishga tushirish.

Dasturiy hujumlarni baholash

- Tashqi hujumlarni baholash uchun yana bir formula – **DREAD** tavsiya etiladi:
- **Damage** – hujum natijasida yetkazilgan zarar.
- **Reproducibility** – Hujumning takrorlanishi: u qanchalik tez-tez sodir bo'ladi va uni takrorlash mumkin.
- **Exploitability** – bu yerda: malaka (daraja); hujum uchun zarur bo'lgan tajriba va malaka (xakerning).

Hujumlarga qarshi kurash

- **Shubhali faollikni tekshirish** - masalan, ketma-ket noto'g'ri parolni kiritishga bir necha marta urinish, uni taxmin qilishga urinishni anglatishi mumkin.
- **Auditorlik jurnali (audit log)** - bunda ob'ektga kirish uchun har bir urinish vaqti, foydalanuvchisi va turi qayd qilinadi. Xavfsizlik buzilishidan qutulish va yanada samarali xavfsizlik choralarini ishlab chiqish uchun jurnaldan foydalaniladi.

Quyidagi tekshiruvlar amalga oshiriladi:

- Qisqa yoki taxmin qilish oson bo'lgan parollar;
- Turli xil foydalanuvchi nomlarini o'rnatadigan ruxsatsiz dasturlar;
- Tizim kataloglarida ruxsatsiz dasturlar;
- Kutilmagan vaqt talab qiladigan jarayonlar;
- Noto'g'ri katalog himoyasi;
- Tizim ma'lumotlari fayllarining etarli darajada himoyalanmaganligi;

- Dasturlarni qidirish yo'llaridagi xavfli elementlar (troyanlarga olib boruvchi);
- Tizim dasturlaridagi o'zgarishlar: summani tekshirish.

Xavfsizlik devori

- **Xavfsizlik devoir (Брандмауэр, firewall) –** mahalliy tarmoqni tashqi hujumlardan himoya qilish uchun tizim dasturi. Xavfsizlik devori "ishonchli" va "ishonchsiz" kompyuterlar o'rtasida joylashtirilgan - masalan, mahalliy tarmoqdagi kompyuterlar va boshqalar. Xavfsizlik devori ikki xil xavfsizlik domenlari o'rtasida tarmoqqa kirishni cheklaydi. O'rnatilgan xavfsizlik devori barcha zamonaviy operatsion tizimlarga kiritilgan va sukut bo'yicha yoqilgan. Uni o'chirmaslik qat'iyan tavsiya etiladi, bu ayniqsa Internetga kirishda juda muhimdir.
- Ishonchim komilki, Windowsning barcha foydalanuvchilari o'quvchilar orasida bir necha bor OTning kompyuteringizni buzishga urinish to'xtatilganligi haqidagi xabarga e'tibor berishdi. Buning sababi o'rnatilgan Windows xavfsizlik devori.
- Xavfsizlik devorlari odatda tarmoq paketlarini "ishonchli" va potentsial ishonchsiz IP-manzillaridan filtrlash orqali amalga oshiriladi.

Buzib kirishga urinishni aniqlash

Xavfsizlikning samarali chorasi bu kompyuter tizimlariga kirishga urinishlarni aniqlashdir. Aniqlash usullari:
Tekshirish va jurnalga yozish;

Tripwire yordamida - ba'zi fayllar va kataloglar o'zgarganligini tekshiradigan UNIX dasturlari, masalan, parollar bo'lgan fayllar;
Tizim chaqiruvlarini kuzatish.

Kriptografiya

Kriptografiya - aniq matnni shifrlangan matnga aylantirish. Kriptografiya usullari maxfiy ma'lumotlarni himoya qilish uchun keng qo'llaniladi.
Yaxshi shifrlash usullarining xususiyatlari:

- Ma'lumotlarni shifrlash va parolini hal qilish uchun vakolatli foydalanuvchilar uchun nisbatan oson usul.
- Shifrlash sxemasi maxfiy algoritmga emas, balki algoritmning shifrlash kaliti (**encryption key**) deb nomlangan maxfiy parametriga bog'liq bo'lishi kerak.
- Ruxsatsiz foydalanuvchi uchun kalitni aniqlash juda qiyin bo'lishi kerak.

Ma'lumotlarni shifrlash standarti (Data Encryption Standard - DES) texnologiyasi xavfsiz mexanizm orqali vakolatli foydalanuvchilarga taqdim etiladigan kalit asosida belgilarni almashtirish va tartiblashtirishga asoslangan. Bunday sxema faqat kalitni o'zi olish mexanizmi kabi xavfsizdir.

Boshqa keng tarqalgan kriptografiya usuli bo'lgan **ochiq kalitli kriptografiya** foydalanuvchi ikkita kalitni bilish tamoyillariga asoslanadi:

public key - ma'lumotlarni shifrlash uchun ochiq kalit.

private key - faqat foydalanuvchi biladigan va u tomonidan ma'lumotlarni parolini hal qilishda foydalanadigan shaxsiy kalit.

Ochiq kalit usuli kriptografiya usullari uchun yana bir muhim talabni o'zida mujassam etgan: usul hammaga ma'lum bo'lgan kriptografik sxemaga asoslangan bo'lishi kerak, ammo bu parol hal qilish sxemasini ochib berishni osonlashtirmaydi.

Veb-texnologiyalarda ishlatiladigan shifrlashning misoli, **SSL (Secure Socket Layer)**, shifrlangan xabarlarni rozetka orqali almashtirish uchun mo'ljallangan kriptografik protokollar oilasi. **SSL** veb-serverlar va brauzerlar o'rtasida xavfsiz aloqa uchun ishlatiladi (masalan, kredit karta raqamlarini kiritish). Mijoz serverga murojaat qilganda, server sertifikat yordamida tekshiriladi. Kompyuterlar o'rtasidagi aloqa simmetrik kalit kriptografiyasidan foydalanadi.