DOI: https://doi.org/10.5281/zenodo.12216717

KORPORATIV TARMOQLAR UCHUN ZAMONAVIY INTELLEKTUAL XAVFSIZLIK TAHLILLASH TIZIMLARI

Sh.B.Sayfullayev
Muhammad al-Xorazmiy nomidagi TATU

Mazkur ishda korporativ tarmoqlar uchun zamonaviy intellektual xavfsizlik tahlillash tizimlari ko'rib chiqilgan bo'lib, xavfsizlikni tahlil qilish vositalari, Internet skaneri va tizim xavfsizligi skaneri, RealSecure tizimlari tadqiq qilingan.

Kalit so'zlar: *korporativ tarmoq, intellektual, xavfsizlik, RealSecure, Internet Scanner.*

Kirish

Hozirgi vaqtda tarmoqlarning rivojlanishi va xavfsizligiga ta'sir qiluvchi, ularning murakkabligini oshiradigan va ularni boshqarishni qiyinlashtiradigan bir qancha asosiy omillar mavjud:

- bo'limlarning lokal tarmoqlarini tashkilotning yagona korporativ tarmog'iga birlashtirish;
- tashqi foydalanuvchilarni (mijozlar, mahsulot yetkazib beruvchilar va boshqalar) tashkilotning korporativ tarmog'iga ulash;
- tashkilotning korporativ tarmog'ini Internetga ulash;
- korporativ tarmoqda turli xil dasturiy va texnik vositalardan foydalanish.

Ushbu omillarning ta'siri nafaqat korxonaning korporativ tarmog'iga kirish huquqiga ega bo'lgan odamlar sonining ko'payishiga, balki tarmoq chegaralarining kengayishiga ham olib keladi. Bu esa, o'z navbatida, axborot xavfsizligiga tahdidlarning amalga oshishi potentsialining oshishiga olib keladi. Kompyuter tizimiga tahdid - bu tizim resurslariga zarar etkazishi mumkin bo'lgan potentsial hodisa, harakat, jarayon yoki hodisa. Kompyuter tizimining zaifliklaridan foydalanish orqali tahdidni amalga oshirishga olib keladigan tajovuzkor tomonidan amalga oshiriladigan har qanday harakat hujum deb ataladi. Zaiflik - bu kompyuter tizimining har qanday xarakteristikasi bo'lib, undan foydalanish tahdidni amalga oshirishga olib kelishi mumkin.

Natijada, aksariyat tashkilotlar uchun tarmoq resurslarini ruxsatsiz kirishdan himoya qilish eng dolzarb muammolardan biriga aylanib bormoqda, uning yechimi korxonaning hayotiyligini ham, uning keyingi rivojlanishini ham belgilaydi.

Tashkilotlarning axborot xavfsizligini ta’minlovchi bo‘limlarga tobora murakkablashib borayotgan tarmoq muhitida tarmoq resurslarini samarali himoya qilishni ta’minlash vazifasi yuklatilgan.

Asosiy qism

Samarali himoya faqat an’anaviy xavfsizlik xizmatlaridan (kriptografiya, autentifikatsiya, kirishni boshqarish va boshqalar) foydalanishdan iborat emas. Shuningdek, vaqti-vaqti bilan tarmoqning zaif tomonlarini tahlil qilish (audit) va doimiy ravishda (kuniga 24 soat, haftasiga 7 kun) kirishni aniqlash (monitoring) uchun korporativ tarmoq trafigini kuzatib borish kerak.

Birinchi vazifani hal qilish uchun (zaifliklarni qidirish) tarmoq zaifliklarini aniqlash va tahlil qilish va ularni bartaraf etish bo‘yicha tavsiyalar berish imkonini beruvchi vosita bo‘lishi kerak. Bunday vositalar mavjud va ular xavfsizlikni tahlil qilish vositalari deb ataladi (chet elda bu vositalar skanerlash dasturlari yoki oddiygina skanerlar deb ataladi).

Ushbu vositalardan nafaqat axborot xavfsizligi bo‘limlari, balki avtomatlashtirish bo‘limlari (tarmoq sozlamalarining to‘g‘riligini nazorat qilish uchun), shuningdek, ichki audit bo‘limlari ham foydalanishlari mumkin.

Ikkinchi vazifa (hujumlarni kuzatish) hujumni aniqlash tizimlari deb ataladigan tizimlar yordamida hal qilinadi.

Xavfsizlikni tahlil qilish vositalari. Bugungi kunda 50 dan ortiq xavfsizlikni tahlil qilish vositalari ma’lum. Ushbu vositalarning har biri o‘zining afzalliklari va kamchiliklariga ega. Ba’zilari faqat bitta operatsion tizim uchun mo‘ljallangan (odatda UNIX), boshqalari tarmoq va OT arxitekturasini juda chuqur bilishni talab qiladi (masalan, SATAN), boshqalari esa faqat bitta tarmoq zaifligini (masalan, Crack) sinab ko‘rish uchun mo‘ljallangan. Shuning uchun, har qanday maxsus xavfsizlikni tahlil qilish vositasidan foydalanishdan oldin, o‘zingizning korporativ tarmog‘ingizda ishlatiladigan dasturiy ta’minot va apparat vositalarining xususiyatlarini sinchkovlik bilan tahlil qilish va shu asosda tanlov qilish kerak.

Xorij mutaxassislarning fikricha, korporativ tarmoqlarda eng ko‘p qo‘llaniladigan operatsion tizimlar UNIX va Windows OT [7]. Bundan tashqari, OS ma’lumotlari bitta tarmoq ichida ishlatilishi mumkin. Bundan tashqari, korporativ tarmoq DOS va Windows 95/98 ish stantsiyalari va Novell Netware ishlaydigan serverlarni o‘z ichiga olishi mumkin. Xavfsizlikni tahlil qilish vositasi, agar ro‘yxatdagi barcha operatsion tizimlar bo‘lmasa, ularning aksariyatini qo‘llab-quvvatlashi kerak. Bu talab Amerikaning Internet Security Systems, Inc kompaniyasining SAFEsuite oilasiga kiruvchi tizimlar tomonidan eng yaxshi javob beradi.

SAFEsuite oilasiga 3 ta tizim kiradi:

- IP tarmog‘ini tahlil qilish tizimi. Internet skaneri;

• UNIX tizimlarining parametrlarini tahlil qilish va o‘zgartirish tizimi System Security Scanner;

• RealSecure hujumlarini tezkor aniqlash va ularga javob berish tizimi.

Internet skaneri va tizim xavfsizligi skaneri. Internet Scanner tizimi korporativ tarmoqdagi mavjud operatsion tizimlar va amaliy dasturlarda hozirda ma’lum bo‘lgan zaifliklarning paydo bo‘lishini aniqlash va kuzatish uchun mo‘ljallangan. U veb-serverlar, xavfsizlik devorlari (Firewalls), marshrutizatorlar (CISCO), UNIX OS (HP-UX, SunOS, Solaris, Linux, AIX), Windows OT da zaifliklarni aniqlash imkonini beradi. Internet Scanner, shuningdek, TCP/IP protokoli stekini qo‘llab-quvvatlaydigan operatsion tizimlarni, masalan, Windows for Workgroups, OS/2 ni sinab ko‘rish imkonini beradi.

Internet Scanner tahlil qiladigan zaifliklarga quyidagilar kiradi: veb-server va OS xizmatlari (RPC, NFS, Sendmail, FTP, CGI va boshqalar), xavfsizlik devori orqali kirish mumkin bo‘lgan xizmatlar, filtrlash qoidalari, umumiy routerlarning standart parollari, zaif parollar va boshqalar.

Internet Scanner tizimi quyidagi komponentlardan iborat:

• Veb xavfsizligi skaneri;

• Xavfsizlik devori skaneri;

• Intranet skaneri

va turli xil operatsion tizimlar va amaliy dasturlar uchun zaiflik testlari to‘plamidir.

Tahlil jarayoni juda oddiy va faqat 4 ta operatsiyani bajarishdan iborat:

1) xavfsizlikni tahlil qilish darajasini tanlash (shablonlar yordamida);

2) skanerlangan tarmoq tugunlarini tanlash;

3) tarmoq tugunlarini skanerlashning haqiqiy jarayoni;

4) hisobot yaratish.

Administrator skanerlashning tafsilotlarini (Og‘ir, O‘rta, Yengil) aniqlaydigan uchta oldindan o‘rnatilgan shablonlardan birini ishlatishi yoki o‘z shablonlarini yaratishi mumkin. Ishlatilgan barcha shablonlarni kelajakda foydalanish uchun saqlash mumkin.

Hisobotlar matn yoki HTML formatida taqdim etiladi va quyidagilarni o‘z ichiga olishi mumkin:

• topilgan zaifliklar ro‘yxati, ularning tavsifi va xavflarni baholash;

• har bir tarmoq tugunida TCP/IP arxitekturasining foydalanilgan xizmatlari va xizmatlari ro‘yxati;

• topilgan zaifliklarni bartaraf etish bo‘yicha tavsiyalar (zaifliklarni bartaraf etish uchun bajarilishi kerak bo‘lgan harakatlar tavsifi). Bundan tashqari, ko‘pgina zaifliklar uchun dasturiy ta’minotning tuzatilgan versiyalari, yamoqlar va boshqalarni o‘z ichiga

olgan Internetdagi serverlarga havolalar beriladi.

System Security Scanner tizimi korporativ tarmoqdagi UNIX tugunlarining xavfsizligini tahlil qilish va tashkilot tomonidan qabul qilingan xavfsizlik siyosatiga muvofiq ularning sozlamalarini boshqarish uchun mo‘ljallangan.

System Security Scanner tizimi ikkita asosiy quyi tizimdan iborat:

• *Tahlil quyi tizimi.*Ushbu quyi tizim ushbu OT o‘rnatilgan kompyuterda UNIX OT sozlamalarini tekshiradi va ularni maxsus ma’lumotlar bazasida saqlaydi. Ushbu ma’lumotlar bazasida, shuningdek, UNIX OS ning ma’lum zaifliklari, ma’lum xavfsizlik yamoqlari va ma’lum xakerlik naqshlari haqida ma’lumotlar mavjud. Ushbu quyi tizim bir vaqtning o‘zida bir yoki bir nechta tarmoq tugunlarida ishga tushirilishi mumkin;

Boshqaruv quyi tizimi. Ushbu quyi tizim tarmoq kompyuterlaridan birida ishlaydi va tarmoq kompyuterlarida ishlaydigan bir yoki bir nechta tahlil quyi tizimlarini boshqarish imkonini beradi, shuningdek, amalga oshirilgan tekshirish natijalari bo‘yicha hisobotlarni yaratishga imkon beradi.

Internet Scannerdan farqli o‘laroq, System Security Scanner nafaqat tizim sozlamalarini tahlil qilish, balki ularni sozlash imkonini beradi. Tizim xavfsizligi skaneri fayllarga kirish huquqlarini, tizim konfiguratsiyasini, fayl yaxlitligini, parol tizimi, foydalanuvchi va guruh ma’lumotlarini va boshqa xususiyatlarni tekshirish imkonini beradi.

Yaqin kelajakda ISS Windows NT operatsion tizimi uchun System Security Scanner versiyasini chiqarishni rejalashtirmoqda.

Bosqinlarni aniqlash tizimlari

Bugungi kunga qadar 30 dan ortiq bosqinlarni aniqlash tizimlari ma’lum. Ba’zi tizimlar, garchi real vaqtda tizim sifatida e’lon qilingan bo‘lsa-da, aslida bunday imkoniyatlarni ta’minlamaydi. Ular jurnallarni tahlil qiladilar va natijada biroz kechikish bilan reaksiyaga kirishadilar. Bundan tashqari, tajovuzni aniqlash tizimlari xavfsizlikni tahlil qilish vositalari bilan bir xil talablarga bo‘ysunadi: ko‘p platformali, foydalanish qulayligi, unumdorlikning pasayishi va boshqalar.

Bu talablarning barchasiga SAFEsuite oilasiga kiruvchi RealSecure tizimi hamda Internet Scanner va System Security Scanner tizimlari javob beradi.

RealSecure. RealSecure tizimi korporativ tarmoqning muhim tugunlariga hujumlarni (hujumlarni) aniqlash uchun mo‘ljallangan. Ushbu muammoni hal qilish uchun tizim himoyalangan tarmoq segmentiga o‘rnatiladi va tarmoq IP-trafigining doimiy monitoringini ta’minlaydi. Hujumni aniqlash real vaqt rejimida trafikning ma’lum statistik naqshlarini aniqlash va ularni ma’lumotlar bazasida saqlanadigan maxsus niqoblar bilan solishtirish, shuningdek himoyalangan tizim uchun ilgari shakllangan naqshlarning buzilishini kuzatish orqali amalga oshiriladi.

Real Secure tizimi 3 ta quyi tizimdan iborat:

• *Aniqlash quyi tizimi.* Ushbu quyi tizim tarmoq trafigini kuzatib boradi va agar hujumlar aniqlansa, ular haqida boshqaruv quyi tizimiga xabar beradi. Aniqlash quyi tizimi sizga ko‘p sonli hujumlarni aniqlash imkonini beradi (veb-serverlarga hujumlar, Java-dan foydalanish, SATAN paketi bilan tarmoqni skanerlash, SYN Flood va Ping Death hujumlari va boshqalar). Aniqlangan hujumlar soni doimiy ravishda o‘sib bormoqda.

• *Javob quyi tizimi.* Hujum aniqlanganda, ushbu tizim administrator tomonidan belgilangan harakatlarni amalga oshiradi (masalan, konsolga xabar yuborish, elektron pochta orqali, peyjerga ma’murni xabardor qilish; hujum qiluvchi tugun bilan ulanishni tugatish; maxsus skriptlarni chaqirish yoki vaziyatni boshqarish dasturlari). Korporativ tarmoqda xavfsizlik devorlaridan foydalanganda, RealSecure tizimi, hujum aniqlangan taqdirda, ushbu xavfsizlik devorlarining ba’zi sozlamalarini dinamik ravishda o‘zgartirishga imkon beradi (masalan, hujum tugunlari orqali korporativ tarmoqqa kirishni taqiqlovchi filtrlash qoidalarini o‘zgartirish).

• *Boshqaruv quyi tizimi.* Ushbu quyi tizim xavfsizlik ma’muriga turli himoyalangan segmentlarda o‘rnatilgan bir nechta aniqlash quyi tizimlarini bir joydan boshqarish imkonini beradi. Quyi tizim qulay grafik interfeysga ega.

SAFEsuite oilasiga kiruvchi boshqa tizimlar singari, RealSecure tizimi Windows NT, SunOS, Solaris, HP-UX, AIX, Linux ostida ishlaydi.

Xulosa

Yuqorida aytilganlarning barchasidan quyidagi xulosalar chiqarish mumkin:

1. Agar inson omilini hisobga olmasak, bugungi kunda tarmoqlarda xavfsizlikning eng yaxshi darajasiga faqat uzatiladigan ma’lumotlarni dinamik shifrlash orqali erishish mumkin. Bunga ixtisoslashtirilgan apparat va dasturiy ta’minotni qo‘llash orqali erishiladi, lekin ma’lumotlarni uzatish tezligiga salbiy ta’sir ko‘rsatadi.

2. Ishonchliligi yuqori bo‘lgan mavjud intellektual xavfsizlik tahlili tizimlari o‘rganilayotgan ob’yektlarning (ixtisoslashtirilgan serverlar, marshrutizatorlar va boshqa jihozlar) zaif tomonlarini aniqlash imkonini beradi. Biroq, ular ma’lum bir operatsion tizimning xavfsizligi sohasidagi ishlarning hozirgi holati bilan o‘z imkoniyatlari bilan cheklangan. Bu shuni anglatadiki, ushbu operatsion tizimning yangi versiyasi chiqarilishi bilan unda yangi xatolar ("teshiklar") paydo bo‘lishi mumkin. Va bu, o‘z navbatida, tizim xavfsizligi darajasining pasayishiga olib keladi, chunki xavfsizlik analizatorlari yangi xatolar yoki yangi operatsion tizimning u yoki bu himoyasini chetlab o‘tish usullari haqida shunchaki "bilmaydi". Bu holat kompyuter viruslari va antiviruslar bilan bog‘liq vaziyatga juda o‘xshaydi, antivirus taqqoslash

uchun imzo yo‘qligi sababli oddiygina yangi virusni taniy olmaydi. Albatta, u yoki bu xavfsizlikni tahlil qilish tizimini ishlab chiqaruvchi kompaniya bozor holatini va yangi dasturiy ta’minotni kuzatib boradi va o‘z mahsulotlarining yangilanishlari yoki yangi versiyalarini chiqaradi. Boshqacha qilib aytganda, bularning barchasi abadiy kurashga aylanadi.

Foydalanilgan adabiyotlar ro‘yxati

1. Han J. Data Mining: Concepts and Techniques / J. Han, M. Kamber // Morgan Kaufmann. – 2000.
2. Маслова Н.А. Концептуальные особенности построения интеллектуальных корпоративных систем предприятий водоснабжающей отрясли / Н.А. Маслова // Штучний інтелект. – 2006. – No 4.–С. 443-452
3. Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах / В.Ф.Шаньгин, А.В. Соколов. – Изд-во: ДМК, 2002. – 134 с.4.
4. Корнеев В.В. Базы данных: интеллектуальная обработка информации/ В.В. Корнеев, А.Ф. Гареев,С.В. Васютин, В.В. Райх. – М. : Нолидж, 2000. – 352 с.5.
5. Маслова Н.А. Информационная безопасность систем управления базами данных / Маслова Н.А. //Комп‟ютерна математика. Оптимізація обчислень : зб. наук. праць. – Київ : ІК НАН України,2001. – Т. 1. – С. 271-280.6.
6. Гончаров М. Модифицированный древовидный алгоритм Байеса для решения задачклассификации / Гончаров М. – Spellabs, 2007