KORPORATIV TARMOQLARNI HIMOYALASHDA VIRTUAL TARMOQ ORQALI IDPS TEXNOLOGIYASIDAN FOYDALANISH

Po'latov Doston Normurod o'g'li
Roziqov Abdug'ani Ilhomjon o'g'li
Jumaboyev Javlonbek Sherqul o'g'li
Shonazarov Sarvarbek Maqsud o'g'li

Annotatsiya

Ushbu maqola shaxsiy kompyuter, yoki korporativ tizmlarga bo'ladigan hurujlarni aniqlash va ularga qarshi chora tadbirlarining samarasini oshirish.

Kalit so'zlar: IDPS, intrusion detection, intrusion prevention, korporativtarmoq, virtual tarmoq.

Abstract

This article applies to personal computers, or corporate systems identification of future outbreaks and the effectiveness of measures against them increase

Key words: IDPS, intrusion detection, intrusion prevention, corporate network, virtual network.

Bugungi kunda hayotimizga kirib kelgan axborot texnologiyalarining jadallik bilan rivojlanishi axborotlar ahamiyatining oshish sabablaridan biri bo'lmoqda. Shaxsiy kompyuter, yoki korporativ tarmoq bo'ladimi, undagi axborot, ehtimoliy shaxs yoki guruhlar uchun sizga tahdid va xavf soluvchi omil bo'lish ehtimolligi yuzaga keladi. Ayni paytda g'arazgo'y shaxslar tomonidan kompyuter yoki, kompyuterlar tarmog'iga bo'ladigan hurujlarni aniqlash va ularni tahlil etish, ularga tegishli chora ko'rish axborot xavsizligini ta'minlashda samarali usul hisoblanadi. Taklif etilayotgan –hurujlarni aniqlash va ularga chora ko'rishda virtual tarmoqdan foydalanish usuli ko'pchilik tarmoqlarda qo'llanilsa hurujlarni aniqlash va ularga qarshi samarali chora ko'rish uchun foyda beradi.

Hozirda axborotni himoyalashning bir nechta usullari mavjud bo'lib, ushbu maqola IDPS tizmlarini qo'llashda virtual tarmoq texnologiyasidan foydalanish orqali uning samarasini oshirish masalasi keltirilgan. Hurujlarni aniqlash(Intrusion detection) –bu kompyuter tizmi yoki tarmoqdagi sodir bo'layotgan hodislarni ko'rib chiqish va ularning zaifliklarini, ya'ni u orqali tizm duch kelishi mumkin bo'lgan kompyuterning hurujlarga bo'lgan joriy siyosatini va administrator tomonidan qo'llanadigan siyosatni buzilishi ehtimollarini tahlil etish jarayonidir. Hurujlarni oldini olish(Intrusion prevention) –bu tizm Intrusion detection jarayonida aniqlangan zaifliklarni bartaraf etish jarayonidir. IDPS(Intrusion Detection and Prevention System) texnologiyasi tizmdagi mavjud zaifliklarni aniqlash, ular haqidagi ma'lumotlarni yig'ish, bartaraf etish choralarini ko'rish va tizmning axborot xavfsizligi bo'yicha administratoriga xabar qilish maqsadida foydalaniladi. Shuningdek, IDPS tizim xavfsizlik siyosatining kamchiligini aniqlash, ularga mavjud hurujlarni ko'rib chiqish va oldini olish maqsadida ham foydalaniladi. IDPS texnologiyasi bir necha xil turlari mavjud bo'lib.

Tarmoqqa asoslangan(Network-based) –tarmoq traffigi, yoki ma'lum bir tarmoq

segmenti tahlil qilish va ilovalar protokolidagi shubxali traffigni monitoring qilish.

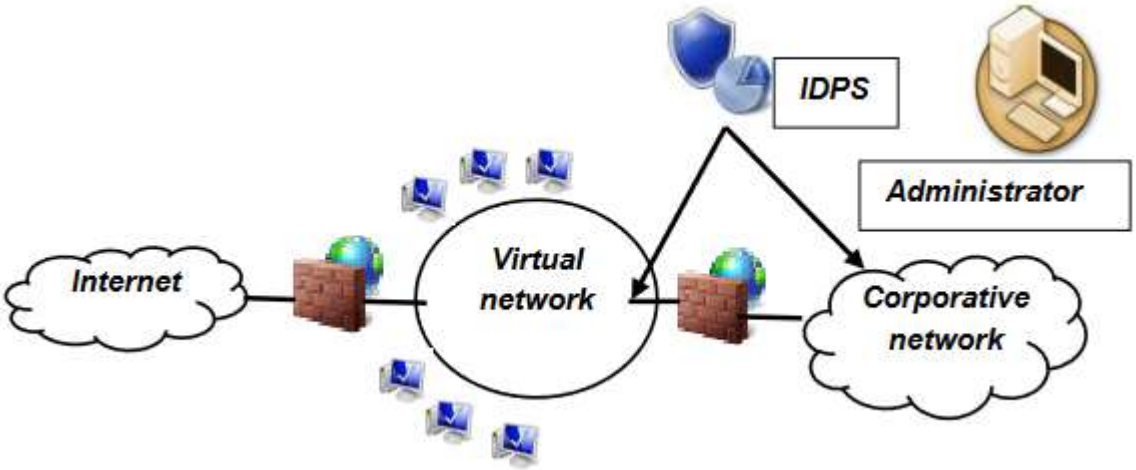
Simsiz tarmoq(Wireless) –simsiz tarmoq oqimini taxlil etish va simsiz tarmoq protokolidagi shubxali traffigni monitoring qilish.

Tarmoq tabiatini tahlil(Network behavior analysis) –tarmoq traffigidagi shubhali paketlar oqimi tabiatini tekshirish, ya'ni trafikni hujum oidligini (DoS, DDoS).

Hostga asoslangan(Host based) –yakka kompyuter uchun qo'llanadigan IDPS tizmi bo'lib undagi shubhali traffik, yoki faoliyatni aniqlash va oldini olishga qaratilgan tizmdir.

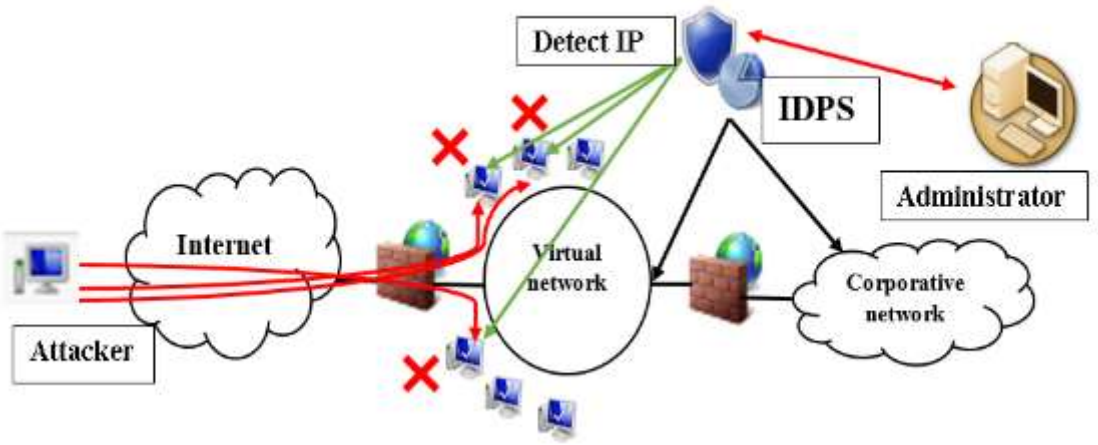
Virtual tarmoq –mantiqiy kompyuterlardan hosil qilingan tarmoq. Yuqoridagi IDPS va virtual tarmoqdan foydalanib korporativ tizmni quyidagicha shakillantirishimiz mumkin. Bu yerda qurilgan tizmning himoyasi asosan virtual tarmoqni tashkil etish orqali hosil qilinadi. Virtual tarmoqni tashkil etish kerak bo'ladigan qurilma u qadar yuqori bo'lishi esa talab etilmaydi. Aytaylik, virtual tarmoqda 10 ta kompyuter kerak bo'lsa ushbu tarmoqni hosil qilishda, 1 dona quyidagi parametrlarga ega bo'gan kompyuter kerak bo'ladi. Talab etiladigan parametrlar: VMlar xotirasini ta'minlash uchun HDD 150Gb o'lchamli xotira manbai va VMlar RAM xotirasini ta'minlash uchun RAM 10Gb xotira talab etiladi. Hosil qilingan virtual tarmoq korporativ tarmoqning kirish qismiga qo'yiladi.

Bundan maqsad, tashqaridan kiruvchi har qanday so'rov, yoki axborot paketi dastavval virtual tarmog'iga tushadi. Bu yerda, IDPS texnologiyasi har ikkala, ya'ni virtual hamda korporativ tarmoq resurslarini himoyalash orqali ularning monitoringini amalga oshiradi.



1-rasm. Tashkil etiladigan tarmoq.

Tashkil etilgan tarmoqda IDPS quyidagi ishlarni amalga oshiradi [1].
1. Tashkil etilgan tarmoqning xavfsizlik siyosati kamchiliklarini aniqlash.
2. Tizm zaifliklari haqida ma'lumotlarni taqdim qilish.
3. Kompyuter ilovalaridagi shubhali traffikni tahlil qilish, agar shubhali traffik aniqlansa traffikni vaqtincha to'xtatish va tizm administratoriga xabar berish.
4. Tarmoq traffigini monitoring qilish va chora ko'rish.
5. Administratorni yuqoridagi holatalar bo'yicha xabardor qilish va boshq.



2-rasm. Tashkil etilgan tarmoqda IDPS texnologiyasining ishlashi.

Hozirgi kundagi axborotlarni himoylash vositalarining narxlariga e’tibor qaratadigan bo’lsak ularning narxlarini qimmatligi ko’pchilik korxona va tashkilotlarda axborot xavsizligini ta’minlashga bo’lgan sarf-xarajatlarni yuqorilab ketishiga sabab bo’lib bormoqda. Ushbu taklif qilingan usul orqali esa ularga bo’lgan sarmoyani qisqartirish imkoniyatiga erishish mumkin.

Texnologik infratuzilmani va nozik ma'lumotlarni qo'riqlaydi: Siloda hech qanday tizim mavjud bo'lishi mumkin emas, ayniqsa ma'lumotlarga asoslangan biznesning hozirgi davrida. Ma'lumotlar doimiy ravishda tarmoq orqali oqadi, shuning uchun tizimga hujum qilish yoki unga kirishning eng oson yo'li haqiqiy ma'lumotlar ichida yashirishdir. Tizimning IDS qismi reaktiv bo'lib, xavfsizlik bo'yicha mutaxassislarni bunday mumkin bo'lgan hodisalar haqida ogohlantiradi. Tizimning IPS qismi proaktiv bo‘lib, xavfsizlik guruhlariga moliyaviy va obro‘ga putur yetkazishi mumkin bo‘lgan hujumlarni yumshatish imkonini beradi.

Mavjud foydalanuvchi va xavfsizlik siyosatlarini ko'rib chiqadi: Har bir xavfsizlikka asoslangan tashkilot o'z ilovalari va tizimlari uchun foydalanuvchi siyosatlari va kirish bilan bog'liq siyosatlarga ega. Ushbu siyosatlar faqat bir nechta ishonchli foydalanuvchilar guruhlari va tizimlariga muhim resurslarga kirishni ta'minlash orqali hujum maydonini sezilarli darajada kamaytiradi. Buzg'unchilikni aniqlash va oldini olish tizimlari orqali doimiy monitoring ma'murlar ushbu siyosat doirasidagi har qanday teshiklarni darhol aniqlashini ta'minlaydi. Shuningdek, u administratorlarga maksimal xavfsizlik va samaradorlikni sinab ko'rish uchun siyosatlarni o'zgartirishga imkon beradi.

Tarmoq resurslari haqida ma'lumot to'playdi: IDS-IPS shuningdek, xavfsizlik guruhiga o'z tarmoqlari orqali o'tayotgan trafikni qushning nazari bilan ko'rish imkonini beradi. Bu ularga tarmoq resurslarini kuzatib borishga yordam beradi, bu esa trafikni haddan tashqari yuklash yoki serverlardan kam foydalanish holatlarida tizimni o'zgartirish imkonini beradi.

Muvofiqlik qoidalariga rioya qilishga yordam beradi: sanoat vertikalidan qat'i nazar, barcha korxonalar iste'molchi ma'lumotlarining maxfiyligi va xavfsizligini ta'minlash uchun tobora ko'proq tartibga solinmoqda. Asosan, ushbu vakolatlarni bajarish yo'lidagi birinchi qadam bosqinlarni aniqlash va oldini olish tizimini joriy

qilishdir.

Tarmoqqa asoslangan tajovuzni oldini olish tizimi (NIPS) : Tarmoqqa asoslangan tajovuzni oldini olish tizimlari butun tarmoqlarni yoki tarmoq segmentlarini zararli trafik uchun nazorat qiladi. Bu odatda protokol faoliyatini tahlil qilish orqali amalga oshiriladi. Protokol faoliyati ma'lum hujumlar ma'lumotlar bazasiga mos keladigan bo'lsa, tegishli ma'lumotlarga kirishga ruxsat berilmaydi. NIPS odatda tarmoq chegaralarida, xavfsizlik devorlari, marshrutizatorlar va masofaviy kirish serverlari ortida joylashtiriladi.

Simsiz hujumni oldini olish tizimi (WIPS): Simsiz hujumni oldini olish tizimlari simsiz tarmoqqa maxsus protokollarni tahlil qilish orqali simsiz tarmoqlarni nazorat qiladi. WIPS tashkilotning simsiz tarmog'i doirasida qimmatli bo'lsa-da, bu tizimlar uzatishni boshqarish protokoli (TCP) kabi yuqoriroq tarmoq protokollarini tahlil qilmaydi. Simsiz kirishni oldini olish tizimlari simsiz tarmoq ichida va ruxsatsiz simsiz tarmoqlarga sezgir bo'lgan hududlarda o'rnatiladi.

Tarmoq xatti-harakatlarini tahlil qilish (NBA) tizimi : NIPS protokol faoliyatidagi og'ishlarni tahlil qilganda, tarmoq xatti-harakatlarini tahlil qilish tizimlari noodatiy trafik naqshlarini tekshirish orqali tahdidlarni aniqlaydi. Bunday naqshlar odatda siyosat buzilishi, zararli dastur tomonidan yaratilgan hujumlar yoki tarqatilgan xizmatni rad etish (DDoS) hujumlari natijasidir . NBA tizimlari tashkilotning ichki tarmoqlarida va ichki va tashqi tarmoqlar o'rtasida trafik oqadigan nuqtalarda o'rnatiladi.

Xostga asoslangan hujumni oldini olish tizimi (HIPS) : Xostga asoslangan hujumni oldini olish tizimlari qolganlardan farq qiladi, chunki ular bitta xostda joylashtirilgan. Ushbu xostlar muhim ma'lumotlarga ega muhim serverlar yoki ichki tizimlarga kirish eshigi bo'lishi mumkin bo'lgan hamma uchun ochiq serverlardir. HIPS ishlayotgan jarayonlar, tarmoq faolligi, tizim jurnallari, ilovalar faolligi va konfiguratsiya o‘zgarishlarini kuzatish orqali ushbu xostga kiruvchi va undan chiqadigan trafikni nazorat qiladi.

FOYDALANILAGAN ADABIYOTLAR:

1. Петренко С.А. “Управление информационными рисками компании” Экспресс-электроника-2002.
2. Karen S., Peter M. “Guide to Intrusion Detection and Prevention systems(IDPS)” - 2007.
3. Chang-Jiu Chen, Wei-Min Cheng, Hung-Yue Tsay va Jen-Chie Vu, "Kazi-kechiktirishga sezgir emas" Microprocessor Core Implementation for Microcontrollers, Journal Of Information Science and Engineering 25, 543-557 (2009)
4. J. H. Li, V. C. Li va K. R. Cho, “O'rnatilgan CISC tipidagi yangi asinxron quvur liniyasi arxitekturasi. kontroller - A8051, "Sxemalar va tizimlar bo'yicha 45-chi O'rta G'arb simpoziumi materiallari, jild. 2, 2002, bet. 675-678.