ISSN 2181-3187

TARMOQ XAVFSIZLIGIGA ZAMONAVIY TAHDIDLAR

Jumanova Zuxra Xolbayevna
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Nurafshon filiali assistant o‘qituvchisi
Shodimurodov Ulug’bek Akmalovich
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Nurafshon filiali talabasi
Jo‘rayev Asom Qo‘yliboy o‘g‘li
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Nurafshon filiali talabasi

ANNOTATSIYA

Ushbu maqola tarmoq xavfsizligiga zamonaviy tahdidlarni chuqur tahlil qiladi. Ransomware, phishing, DDoS hujumlari, zararli dasturlar va IoT qurilmalariga qaratilgan hujumlar kabi eng muhim tahdidlar keng qamrovli ko'rib chiqiladi. Shuningdek, bu tahdidlarga qarshi kurashish uchun tavsiya etilgan chora-tadbirlar haqida batafsil ma'lumot beriladi. Maqola zamonaviy texnologik muhitda tarmoq xavfsizligini ta'minlashning muhimligini yoritadi va bu borada eng yaxshi amaliyotlarni tavsiya qiladi.

Kalit so’zlar: *DDoS, xavfsizlik, IoT, o’zgartirish, Ransomware, SIEM, Firewalls*

KIRISH

Texnologiyalar va internetning tezkor rivojlanishi, axborot xavfsizligiga yangi tahdidlar va xatarlarni keltirib chiqarmoqda. Bugungi kunda tashkilotlar va shaxslar o'z ma'lumotlari va tarmoqlarini zararli hujumlardan himoya qilish uchun ko'proq resurslar sarflashlari kerak. Tarmoq xavfsizligi muammosi nafaqat texnik, balki iqtisodiy va ijtimoiy muammolarni ham o'z ichiga oladi.

Bugungi globallashgan dunyoda, korxonalar va davlat tashkilotlari o'zlarining biznes jarayonlarini raqamlashtirishda davom etmoqda. Bu esa tarmoqqa ulanishni va turli qurilmalar, jumladan, mobil telefonlar, noutbuklar, serverlar va IoT qurilmalarini bir tizimga ulashni talab qiladi. Shu bilan birga, tarmoqlarga kirishning ko'payishi, ular orqali sodir etiladigan kiberhujumlar sonining ham ortishiga sabab bo'lmoqda. So'nggi yillarda sodir bo'lgan yirik kiberhujumlar tufayli milliardlab dollar zarar keltirilgan va bu holat nafaqat moliyaviy yo'qotishlarga, balki kompaniyalarning obro'siga ham katta zarar yetkazgan.

ISSN 2181-3187

Shu bilan birga, kiberjinoyatchilar va davlat tomonidan qo'llab-quvvatlanadigan xakerlar ham texnologik jihatdan rivojlanmoqda. Ular yangi va murakkab usullar bilan hujumlarni amalga oshirib, himoya tizimlarini chetlab o'tishga harakat qilmoqdalar. Ransomware, phishing, DDoS hujumlari va zararli dasturlar kabi tahdidlar kiberxavfsizlik sohasida eng katta xavf sifatida qaraladi. Ushbu tahdidlar nafaqat kompaniyalar, balki shaxsiy foydalanuvchilar uchun ham katta xavf tug'diradi.

Tarmoq xavfsizligi nafaqat texnik choralar, balki xodimlarni kiberxavfsizlik bo'yicha xabardor qilish va muntazam treninglar o'tkazishni ham talab qiladi. Tashkilotlar o'z xodimlarini kiberxavfsizlik bo'yicha xabardorlikni oshirish uchun maxsus treninglar o'tkazishlari zarur. Bu, o'z navbatida, hujumlarga qarshi himoyani kuchaytiradi va foydalanuvchilarning ehtiyotsizligi sababli sodir bo'ladigan hujumlarni kamaytiradi.

Axborot xavfsizligining yana bir muhim jihati – bu tarmoqlarning uzluksiz ishlashini ta'minlashdir. Bugungi kunda kompaniyalar va tashkilotlar o'z faoliyatini raqamli infratuzilmalar orqali amalga oshiradi. Tarmoqlarning ishdan chiqishi yoki sekinlashishi esa katta iqtisodiy zarar va mijozlarning noroziligiga sabab bo'ladi. Shu bois, tarmoq xavfsizligini ta'minlash uchun uzluksiz monitoring va tezkor javob berish tizimlarini joriy etish zarur.

Ushbu maqola zamonaviy tarmoq xavfsizligiga tahdidlarni tahlil qilib, ularni oldini olish usullari haqida batafsil ma'lumot beradi. Kiberxavfsizlikning texnik, iqtisodiy va ijtimoiy jihatlarini hisobga olgan holda, zamonaviy tahdidlarga qarshi kurashish usullari va eng yaxshi amaliyotlar haqida tavsiyalar beriladi. Maqola nafaqat texnik mutaxassislar, balki keng omma uchun ham foydali bo'lishi maqsad qilingan.

TAHDIDLAR TURLARI VA ULARDAN HIMOYALANISH

Ransomware — bu kompyuter tizimlarini yoki uning ma'lumotlarini shifrlab, foydalanuvchidan ma'lum miqdorda to'lov talab qiluvchi zararli dastur. Ransomware hujumlari so'nggi yillarda juda ko'payib ketdi. Bu hujumlar odatda zararli elektron pochta qo'shimchalari yoki zararli veb-saytlar orqali amalga oshiriladi. Hujumchilar ma'lumotlarni qayta ochish uchun to'lov talab qilishadi va ko'pincha bu to'lovlar kriptovalyutalarda amalga oshiriladi, bu esa ularning izini yo'qotishga yordam beradi.

Ransomware hujumlari bir nechta yirik korporatsiyalar va tashkilotlarni nishonga olgan. Masalan, 2017 yilda WannaCry ransomware hujumi butun dunyo bo'ylab 200,000 dan ortiq kompyuter tizimini zararladi va milliardlab dollar zarar yetkazdi. Shunga o'xshash NotPetya hujumi esa ko'plab kompaniyalarning faoliyatini to'xtatdi. Ransomware hujumlarining xavfi shundan iboratki, ular nafaqat iqtisodiy zarar keltiradi, balki tizimlarni to'liq ishlamay qolishiga olib keladi.

Fishing Hujumlari: Fishing hujumlari orqali foydalanuvchilarni aldab, ularning shaxsiy va moliyaviy ma'lumotlarini olishga qaratilgan. Bu hujumlar elektron pochta, ijtimoiy tarmoqlar yoki soxta veb-saytlar orqali amalga oshiriladi. Phishing hujumlari

ISSN 2181-3187

juda ishonarli ko'rinishi mumkin va ular ko'pincha foydalanuvchilarni ularning bank hisoblari, parollari yoki boshqa shaxsiy ma'lumotlarini oshkor qilishga majbur qilish uchun ishlatiladi.

2021 yilda Google tomonidan o'rganilgan phishing hujumlari statistikasi shuni ko'rsatadiki, har kuni 240 milliondan ortiq phishing email xabarlari yuboriladi. Phishing hujumlari nafaqat shaxsiy ma'lumotlarni o'g'irlash, balki kompaniyalar tizimlariga zarar yetkazish va ularni shantaj qilish uchun ham ishlatiladi. Ushbu hujumlar ko'pincha ijtimoiy muhandislik (social engineering) usullari orqali amalga oshiriladi, bu esa ularni yanada xavfli qiladi.

DDoS Hujumlari: DDoS hujumlari (Distributed Denial of Service) hujumlari orqali hujumchilar tarmoqqa katta hajmdagi so'rovlarni yuborib, uning xizmatlarini ishdan chiqaradilar. Bu hujumlar ko'pincha kompaniyalar va davlat tashkilotlariga qaratilgan bo'lib, ular tizimlarni ishdan chiqarish yoki sekinlashtirish orqali katta zarar yetkazishi mumkin. DDoS hujumlari ko'pincha botnetlar yordamida amalga oshiriladi, ya'ni ko'p sonli kompyuterlar bir vaqtning o'zida hujumda ishtirok etadi.

2016 yilda Dyn kompaniyasiga qilingan DDoS hujumi butun internet infratuzilmasiga katta zarar yetkazdi. Bu hujum Twitter, Netflix, Reddit va boshqa yirik veb-saytlarning vaqtincha ishlamay qolishiga olib keldi. DDoS hujumlarining murakkabligi va ulkan zarar keltirishi tufayli, ular kiberjinoyatchilar tomonidan keng qo'llaniladi.

Zararlangan Dasturlar (Malware): Zararlangan dasturlar (Malware) tarmoqqa kirib, tizimni zararli faoliyat bilan ta'minlaydigan dasturlarni o'z ichiga oladi. Viruslar, trojanlar, spyware va boshqa zararli dasturlar foydalanuvchi tizimiga yashirincha kirib, ma'lumotlarni o'g'irlash yoki zarar yetkazish maqsadida ishlatiladi. Malware hujumlari ko'pincha foydalanuvchi tomonidan o'rnatilgan dasturlar orqali amalga oshiriladi.

2020 yilda zararli dastur Emotet dunyodagi eng xavfli malwarelardan biri sifatida tan olindi. Bu zararli dastur bank hisoblari, elektron pochtalar va boshqa shaxsiy ma'lumotlarni o'g'irlash uchun ishlatiladi. Emotet va shunga o'xshash zararli dasturlar tashkilotlarning operatsion faoliyatiga katta zarar yetkazishi mumkin.

IoT Qurilmalari Orqali Hujumlar: Internet of Things (IoT) qurilmalari soni oshib borayotganligi bilan birga, ular orqali amalga oshiriladigan hujumlar ham ortmoqda. Ushbu qurilmalar ko'pincha yetarlicha himoyalanmagan bo'lib, ular orqali butun tarmoqqa hujum qilish mumkin. IoT qurilmalari xavfsizlik kamchiliklari tufayli kiberhujumlar uchun oson nishonga aylanadi.

Mirai botneti 2016 yilda IoT qurilmalarini nishonga olgan yirik hujumlardan biri sifatida tanilgan. Bu botnet ko'plab IP kameralar va marshrutizatorlarni zararlab, ularni DDoS hujumlarida ishlatgan. IoT qurilmalari ko'pincha o'z vaqtida yangilanmaydi va zaifliklarni o'z ichiga oladi, bu esa ularni kiberjinoyatchilar uchun oson nishonga aylantiradi.

ISSN 2181-3187

Tarmoq Xavfsizligini Ta'minlash Yo‘llari

Yangilanish: Tizim va dasturiy ta'minot yangilanishlarini muntazam ravishda amalga oshirish. Bu yangilanishlar xavfsizlik kamchiliklarini bartaraf etishga yordam beradi va yangi tahdidlarga qarshi himoya qiladi. Masalan, Microsoft kompaniyasi muntazam ravishda Windows operatsion tizimini yangilab, xavfsizlik zaifliklarini yo'q qiladi.

Antivirus va Antimalware Dasturlaridan Foydalanish: Bu dasturlar zararli dasturlarni aniqlash va ularni olib tashlashga yordam beradi. Ularni muntazam yangilab turish zarur. Symantec va McAfee kabi antivirus kompaniyalari doimiy ravishda yangi zararli dasturlarga qarshi yangilanishlarni taqdim etadi.

Xavfsizlik Devorlari (Firewalls) va Tarmoq Filtrlash: Bu chora-tadbirlar tarmoqga kirish va chiqishni nazorat qilishga imkon beradi va zararli trafikni bloklaydi. Firewalls va IDS/IPS tizimlari tarmoq xavfsizligini oshiradi. Cisco va Palo Alto Networks kabi kompaniyalar xavfsizlik devorlarini taqdim etadi.

Shaxsiy Ma'lumotlarni Himoya Qilish: Foydalanuvchilar o'z shaxsiy ma'lumotlarini himoya qilish uchun kuchli parollar va ko'p faktorli autentifikatsiyadan foydalanishlari kerak. Shuningdek, shaxsiy ma'lumotlarni zaxira nusxalarini yaratish va ularni xavfsiz joyda saqlash muhimdir. Google Authenticator va Microsoft Authenticator kabi ko'p faktorli autentifikatsiya tizimlari bu borada yordam beradi.

Xodimlarni Xabardorlikni Oshirish: Tashkilotlar xodimlarini kiberxavfsizlik bo'yicha muntazam trening va seminarlar orqali xabardorlik darajasini oshirishlari kerak. Bu hujumlarni oldindan aniqlash va ulardan qochish imkonini beradi. IBM va SANS Institute kiberxavfsizlik bo'yicha trening va sertifikatlash dasturlarini taklif etadi.

Zaxira Nusxalari Yaratish: Ma'lumotlarni muntazam ravishda zaxira qilish va ularni xavfsiz joyda saqlash muhimdir. Bu ransomware hujumlariga qarshi samarali chora bo'lishi mumkin. Zaxira nusxalari tashkilotlarga hujumlar sodir bo'lganda ma'lumotlarni tiklash imkonini beradi.

Tarmoqlarni Segmentatsiya Qilish: Tarmoqlarni segmentatsiya qilish orqali hujumchilarning bir segmentdan boshqasiga o'tishiga to'sqinlik qilish mumkin. Bu usul katta tashkilotlar uchun samarali bo'lib, har bir segmentni alohida himoya qilish imkonini beradi.

SIEM Tizimlarini Joriy Etish: Security Information and Event Management (SIEM) tizimlari tarmoqda sodir bo'layotgan voqealarni kuzatish va tahlil qilishga imkon beradi. Splunk va QRadar kabi SIEM tizimlari xavfsizlik hodisalarini real vaqt rejimida kuzatish imkonini beradi.

XULOSA

Zamonaviy tarmoq xavfsizligi tahdidlari doimiy ravishda rivojlanmoqda va ularni oldini olish uchun chora-tadbirlarni kuchaytirish zarur. Ransomware, phishing, DDoS

ISSN 2181-3187

hujumlari, zararli dasturlar va IoT qurilmalariga qaratilgan hujumlar bugungi kunda eng katta tahdidlardan biridir. Bu tahdidlar nafaqat iqtisodiy zarar keltiradi, balki kompaniyalar va tashkilotlarning obro'sini ham katta xavf ostiga qo'yadi. Shu sababli, tarmoq xavfsizligini ta'minlash uchun bir nechta muhim choralarni amalga oshirish zarur.

Birinchidan, tizim va dasturiy ta'minotning muntazam yangilanishi va xavfsizlik yamalari (patch) kiritilishi muhimdir. Bu yangilanishlar tizimning zaif joylarini yopishga va yangi tahdidlarga qarshi samarali himoya qilishga yordam beradi. Muntazam yangilanishlar hujumchilarning mavjud zaifliklardan foydalanish imkoniyatini kamaytiradi va tizim xavfsizligini oshiradi.

Ikkinchidan, antivirus va antimalware dasturlarini o'rnatish va muntazam yangilab turish zarur. Bu dasturlar zararli dasturlarni aniqlash va ularni tizimdan olib tashlashga yordam beradi. Tizimning doimiy ravishda skanerlash va monitoring qilish, zararli faoliyatni erta bosqichda aniqlash imkonini beradi.

Uchinchidan, xavfsizlik devorlari (firewalls) va tarmoq filtrlash usullarini qo'llash kerak. Bu chora-tadbirlar tarmoqqa kirish va chiqishni nazorat qilishga imkon beradi va zararli trafikni bloklaydi. Xavfsizlik devorlari va IDS/IPS tizimlari tarmoq xavfsizligini ta'minlashda muhim rol o'ynaydi.

To'rtinchidan, foydalanuvchilar o'z shaxsiy ma'lumotlarini himoya qilish uchun kuchli parollar va ko'p faktorli autentifikatsiyadan foydalanishlari zarur. Shuningdek, shaxsiy ma'lumotlarni zaxira nusxalarini yaratish va ularni xavfsiz joyda saqlash ham muhimdir. Bu chora-tadbirlar nafaqat foydalanuvchilarni, balki butun tarmoqni himoya qilishga yordam beradi.

Beshinchidan, tashkilotlar o'z xodimlarini kiberxavfsizlik bo'yicha muntazam trening va seminarlar orqali xabardorlik darajasini oshirishlari kerak. Xodimlarning kiberxavfsizlik bo'yicha bilimlarini oshirish, hujumlarni oldindan aniqlash va ulardan qochish imkonini beradi. Xodimlarning kiberxavfsizlik borasida bilimli bo'lishi hujumchilarning ijtimoiy muhandislik usullarini qo'llashini qiyinlashtiradi.

Oltinchidan, tarmoq segmentatsiyasi va SIEM (Security Information and Event Management) tizimlarini joriy etish zarur. Tarmoqlarni segmentatsiya qilish orqali hujumchilarning bir segmentdan boshqasiga o'tishiga to'sqinlik qilish mumkin. SIEM tizimlari esa tarmoqda sodir bo'layotgan voqealarni kuzatish va tahlil qilishga imkon beradi, bu esa hujumlarni erta aniqlash va ularga tezkor javob berishni ta'minlaydi.

Yuqorida keltirilgan choralar yordamida tarmoq xavfsizligini ta'minlash va zamonaviy tahdidlarga qarshi kurashish mumkin. Ushbu chora-tadbirlar kiberxavfsizlikning samaradorligini oshirishga yordam beradi va tashkilotlar hamda shaxslarni tarmoq xavfsizligiga tahdidlardan himoya qiladi. Tarmoq xavfsizligini ta'minlash, nafaqat texnik choralarni, balki xodimlarning xabardorligini oshirish va

ISSN 2181-3187

uzluksiz monitoringni ham o'z ichiga oladi. Shu orqali tashkilotlar o'z ma'lumotlarini va tizimlarini samarali himoya qilishlari mumkin.

ADABIYOTLAR RO'YXATI

1. Symantec. "2023 Internet Security Threat Report."
2. Kaspersky. "Top 10 Cybersecurity Threats in 2023."
3. McAfee. "Understanding Ransomware and How to Protect Against It."
4. Trend Micro. "Phishing Attacks: A Growing Threat to Cybersecurity."
5. Cisco. "Defending Against DDoS Attacks."
6. IBM. "The Rise of Malware: Understanding and Preventing Attacks."
7. Palo Alto Networks. "Securing the Internet of Things (IoT)."