TARMOQ SATHIDA MA'LUMOTLARNI HIMOYALASH

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 tezisda tarmoq sathida ma'lumotlarni himoyalash muhimligi va usullari ko'rib chiqiladi. Tarmoq xavfsizligini ta'minlash uchun zamonaviy texnologiyalar va himoya usullarining roli muhokama qilinadi. Tezkor o'zgarib turuvchi kiber tahdidlarga qarshi samarali himoya choralarini qo'llashning dolzarbligi tahlil qilinadi.

Kalit so'zlar: tarmoq xavfsizligi, ma'lumotlarni himoyalash, kiber xavfsizlik, firewalls, IDS, IPS, VPN, shifrlash, kiber tahdidlar, zamonaviy texnologiyalar.

Tarmoq xavfsizligi bugungi kunda eng muhim masalalardan biridir. Global tarmoqlar orqali o'tayotgan ma'lumotlarning soni va hajmi kundan-kunga oshib bormoqda, shu sababli ularni himoyalash ehtiyoji ham kuchaymoqda. Ma'lumotlar xavfsizligini ta'minlashda tarmoq sathida qo'llaniladigan turli xil texnologiyalar va usullar mavjud. Ushbu tezisda tarmoq xavfsizligi bo'yicha asosiy kontseptsiya va himoya usullari ko'rib chiqiladi.

Tarmoq xavfsizligi muammosi nafaqat yirik korporatsiyalar, balki kichik bizneslar va hatto shaxsiy foydalanuvchilar uchun ham dolzarbdir. Internetning keng tarqalishi bilan birga, tarmoq orqali uzatiladigan ma'lumotlarning xavfsizligi ham muhim ahamiyat kasb etmoqda. Ma'lumotlarning maxfiyligi, butunligi va mavjudligini ta'minlash uchun tarmoq xavfsizligini ta'minlash muhimdir.

Kiberxavfsizlikning asosiy elementlari orasida kirish nazorati, autentifikatsiya, shifrlash, zararli dasturlardan himoya qilish, tarmoq monitoringi va xavfsizlik hodisalarini boshqarish kiradi. Bu elementlar birgalikda ishlaganda tarmoq xavfsizligini ta'minlashda samarali natijalar beradi. Ushbu tezisda biz tarmoq xavfsizligini ta'minlashda asosiy usullar va texnologiyalarni batafsil ko'rib chiqamiz.

Tarmoq xavfsizligi asoslari:

Tarmoq xavfsizligi – bu tarmoq infratuzilmasini, shu jumladan kompyuterlarni, serverlarni va tarmoqdagi boshqa qurilmalarni xavfsizlik xavf-xatarlaridan himoya qilishga qaratilgan choralar majmui. Asosiy maqsad ma'lumotlarning butunligini, maxfiyligini va mavjudligini ta'minlashdan iborat. Tarmoq xavfsizligining asosiy tamoyillari kirish nazorati, autentifikatsiya, ma'lumotlarni shifrlash va monitoringdan iborat.

Kirish nazorati orqali tarmoqqa kirish ruxsatiga ega bo‘lmagan foydalanuvchilarni bloklash mumkin. Autentifikatsiya foydalanuvchilarning shaxsini tasdiqlashni o‘z ichiga oladi. Shifrlash ma'lumotlarni o‘qilmas holga keltiradi, shunda faqat ruxsat etilgan shaxslar ularni o‘qiy oladi. Monitoring esa tarmoq faoliyatini kuzatib, nomaqbul faoliyatlarni aniqlashga yordam beradi.

Tarmoq sathidagi tahdidlar:

Tarmoq xavfsizligiga tahdid soluvchi asosiy omillar quyidagilardan iborat:

Xakerlik hujumlari: Tarmoqga kirib, maxfiy ma'lumotlarni o‘g‘irlash yoki yo‘q qilish maqsadida amalga oshiriladigan noqonuniy kirishlar. Xakerlar tarmoq infratuzilmasiga kirish uchun turli xil usullarni qo‘llaydilar, masalan, parollarni buzish, fishing hujumlari yoki zararli dasturlar orqali.

DDoS hujumlari: Tarmoq resurslarini haddan tashqari yuklab, xizmat ko‘rsatishni to‘xtatishga qaratilgan hujumlar. DDoS hujumlari tarmoqning ishlash qobiliyatini pasaytiradi yoki butunlay to‘xtatadi, bu esa kompaniyalar uchun katta zarar keltirishi mumkin.

Zararli dasturlar: Tarmoqqa kirib, zarar yetkazishga qaratilgan viruslar, trojanlar va boshqa zararli dasturlar. Zararli dasturlar tarmoq resurslarini buzishi, ma'lumotlarni o‘g‘irlashi yoki yo‘q qilishi mumkin.

Himoya usullari:

Firewalls: Firewalls tarmoqni kirish va chiqish trafikini nazorat qilish orqali himoya qiladi. Ular ruxsat etilgan va taqiqlangan trafikni aniqlab, tarmoq xavfsizligini ta'minlaydi. Zamonaviy firewalls tarmoqning turli qatlamlarida ishlaydi va trafikni chuqur tahlil qiladi. Ular kirish nuqtalarini nazorat qilib, shubhali faoliyatlarni aniqlaydi va bloklaydi.

Intrusion Detection Systems (IDS) va Intrusion Prevention Systems (IPS): IDS va IPS tizimlari tarmoqdagi zararli faoliyatni aniqlash va oldini olish uchun ishlatiladi. IDS zararli faoliyatni aniqlaydi va administratorlarga xabar beradi, IPS esa avtomatik ravishda chora ko‘radi. IDS tizimlari passiv bo‘lib, faqat xabar beradi, IPS tizimlari esa faol bo‘lib, zararli trafikni to‘sadi va tarmoqni himoya qiladi.

Virtual Private Network (VPN): PN tarmoq orqali uzatiladigan ma'lumotlarni shifrlash orqali himoya qiladi. Bu usul yordamida ma'lumotlar maxfiyligi va butunligi ta'minlanadi. VPN foydalanuvchilarga xavfsiz kanallar orqali tarmoq resurslariga kirish imkonini beradi va ularni kiber tahdidlardan himoya qiladi.

Shifrlash: Ma'lumotlarni shifrlash orqali ularni faqat ruxsat etilgan foydalanuvchilar o‘qiy oladigan holatda uzatish mumkin. Shifrlash algoritmlari ma'lumotlarning maxfiyligini ta'minlaydi. Zamonaviy shifrlash usullari, masalan, AES va RSA algoritmlari, ma'lumotlarning yuqori darajada himoyalanganligini ta'minlaydi.

Tarmoq xavfsizligi texnologiyalari:

Hozirgi kunda tarmoq xavfsizligini ta'minlashda qo‘llaniladigan zamonaviy texnologiyalar orasida Machine Learning (ML) va Artificial Intelligence (AI) asosida ishlaydigan tizimlar ham mavjud. Bu texnologiyalar tarmoqdagi normal va anormal faoliyatni ajratib, xavfsizlikni oshirishga yordam beradi. ML va AI tizimlari katta miqdordagi tarmoq ma'lumotlarini tahlil qilib, zararli faoliyatlarni aniqlash va oldini olish uchun foydalaniladi.

ML va AI asosidagi tizimlar tarmoq xavfsizligini ta'minlashda o‘ziga xos afzalliklarga ega. Ular o‘z-o‘zini o‘rgatish qobiliyatiga ega bo‘lib, yangi tahdidlarga moslasha oladi va tarmoqni himoya qilishda samaradorligini oshiradi. Bunday tizimlar tarmoq faoliyatini doimiy ravishda monitoring qilib, nomaqbul faoliyatlarni tezda aniqlaydi va chora ko‘radi.

Tarmoq xavfsizligi bugungi kunda axborot texnologiyalari sohasida eng muhim masalalardan biri bo‘lib, turli xil xavf-xatarlardan himoyalanish uchun samarali usullarni qo‘llashni talab etadi. Firewalls, IDS/IPS tizimlari, VPN va shifrlash kabi texnologiyalar tarmoq xavfsizligini ta'minlashda katta ahamiyatga ega. Ushbu texnologiyalar birgalikda ishlaganda, tarmoqdagi barcha darajalarda xavfsizlikni ta'minlashga yordam beradi.

Kiber tahdidlarga qarshi kurashda zamonaviy texnologiyalar, xususan, ML va AI asosida ishlaydigan tizimlardan foydalanish dolzarb bo‘lib qolmoqda. Ushbu texnologiyalar yordamida tarmoq xavfsizligini ta'minlash yanada samarali bo‘lib, yangi tahdidlarga tezda moslasha olish qobiliyati bilan ajralib turadi. Tezisda tarmoq xavfsizligining asosiy kontseptlari va himoya usullari yoritilgan bo‘lib, bu sohadagi muammolarni hal etishga qaratilgan amaliy tavsiyalar berilgan.

Tarmoq xavfsizligi muammolarini hal qilish uchun samarali strategiyalarni ishlab chiqish va zamonaviy texnologiyalardan foydalanish zarur. Tarmoq xavfsizligini ta'minlash orqali foydalanuvchilar va tashkilotlar o‘z ma'lumotlarini himoya qilish va kiber tahdidlardan saqlanish imkoniyatiga ega bo‘ladi.

ADABIYOTLAR RO‘YXATI

1. Xasanov A. "Kompyuter xavfsizligi va tarmoq himoyasi", Toshkent, 2020.
2. Karimov B. "Axborot xavfsizligi asoslari", Toshkent, 2019.
3. Rashidov I. "Tarmoq xavfsizligi: nazariya va amaliyot", Toshkent, 2018.
4. Stallings W. "Network Security Essentials", Prentice Hall, 2017.
5. Tanenbaum A.S. "Computer Networks", Pearson, 2016.

5-SHO'BA.
UZLUKSIZ TA'LIMDA O'QUV JARAYONINI TASHKIL ETISHNING MUAMMOLARI VA ISTIQBOLLARI