KIBER XAVFSIZLIK VA UNING TURLARI

Andijon shahar 2-son politehnikum
Informatika va axborot fani o‘qituvchisi
Isamutdinova Xonzoda Isamutdinova

Annotatsiya

Mazkur maqolada zamonaviy axborot texnologiyalari rivojlanishi bilan birga yuzaga kelayotgan kiber tahdidlar, ularning turlari va ularga qarshi kurashish usullari yoritilgan. Keltirilgan misollar yordamida har bir tahdid turi batafsil tahlil qilingan. Shuningdek, maqolada kiber xavfsizlikni ta'minlash bo‘yicha tavsiyalar va xalqaro tajribalar keltirilgan.

Kalit so‘zlar

Kiber xavfsizlik, kiber tahdid, axborot xavfsizligi, zararli dastur, shifrlash, DDoS, phishing.

Kirish

Axborot texnologiyalari jadal rivojlanayotgan bugungi davrda, axborot resurslari ustidan nazoratni saqlab qolish va ularni himoya qilish muammolari dolzarb bo‘lib bormoqda. Kiber xavfsizlik — bu axborotni, kompyuter tizimlarini, dasturiy vositalarni va tarmoqlarni har qanday zararli ta’sirdan himoya qilish bo‘yicha kompleks choralar majmuasidir. Ushbu maqolada biz kiber xavfsizlik turlari, ularning xususiyatlari va amaliy misollar asosida ularni tahlil qilamiz.

Asosiy qism

Kiberxavfsizlik - bu tizimlar, tarmoqlar va dasturlarning raqamli hujumlardan himoya qilish uchun texnologiyalar, jarayonlar va amaliyotlardan foydalanish usuli. Kiberhujumlar ko'pincha nozik ma'lumotlar va ma'lumotlarni nishonga oladi va bu ma'lumotlarga kirish orqali kiberjinoyatchilar foydalanuvchilar va

kompaniyalardan pul undiradilar, oddiy jarayonlarni to'xtatadilar va butun saytlarni o'chirib tashlaydilar.

Samarali kiberxavfsizlik har qanday biznes uchun muhim tarkibiy qism bo'lib, kichik va o'rta tashkilotlar uchun undan ham ko'proq narsa xavf ostida, chunki ular ko'pincha bunday hujumlardan xalos bo'lish uchun resurslarga ega emaslar. Ma’lumotlarga asoslangan zamonaviy dunyomizda mavjud bo‘lgan ma’lumotlar va qurilmalar soni ortib borayotgani sababli kiberhujumlardan himoyalanish tobora qiyinlashib bormoqda.

Kiberxavfsizlik nima uchun muhim?

Kiberxavfsizlik bugungi kunda har qanday biznesning eng muhim jihatlaridan biridir. Buning sababi, hukumatlar, moliyaviy korporatsiyalar, tibbiyot kompaniyalari va deyarli har bir boshqa tashkilot kompyuterlar va qurilmalarda katta hajmdagi ma'lumotlarni to'playdi va saqlaydi. Ushbu ma'lumotlarning aksariyati intellektual mulk, moliyaviy ma'lumotlar, shaxsiy ma'lumotlar va boshqalar kabi ushbu kompaniyalar yoki jamoatchilik haqida nozik ma'lumotlarni o'z ichiga oladi. Ushbu ma'lumotlar ko'pincha tarmoqlar va qurilmalar orqali uzatiladi, ya'ni uning buzilishi uchun ko'plab imkoniyatlar mavjud.

Dunyo ko'plab keng ko'lamli kiberhujumlarga guvoh bo'ldi, bu esa ularning ma'lumotlari bilan ishlashga nisbatan ishonchsizlikning doimiy o'sishiga olib keldi. Ushbu turdagi hujumlar kompaniyalarning obro'siga ham jiddiy putur etkazadi.

Kiber xavfsizlik turlari

1. Tarmoq xavfsizligi

Tarmoq xavfsizligi — bu kompyuter tarmoqlari orqali ma’lumotlar uzatilayotgan vaqtda ularni himoyalashni ta’minlaydi. Masalan, korxonaning Wi-Fi tarmog‘iga ruxsatsiz kirishning oldini olish. Firewall, IDS/IPS tizimlari bu sohada keng qo‘llaniladi.

Tarmoq xavfsizligi – bu tarmoq orqali yuboriladigan ma'lumotlarni hackerlar, viruslar va boshqa tahdidlardan himoya qilishdir. Tasavvur qiling, sizning tarmog‘ingiz katta uyingiz va uyingizni o‘g‘rilar va jinoyatchilardan himoya qilishingiz kerak. Tarmoq xavfsizligi – bu himoya qilish uchun kerakli vositalarni qo‘llash.

Asosiy tarmoq xavfsizlik elementlari:

Firewall – Eshik oldidagi qo‘riqchi.

Misol: Sizning tarmog‘ingizga begona kirmasligi uchun Firewall tarmoqni qo‘riqlaydi.

Antivirus – Jinoyatchilarni topib chiqarish

Antivirus xuddi uyingizda ko‘zdan pana turgan o‘g‘rilarni topib, ularni tashqariga haydaydi. Agar biror zararli dastur kirsa, antivirus uni ushlaydi va yo‘q qiladi.

Shifrlash – Maxfiy yozuv

Shifrlash ma'lumotlarni maxfiy qilib, ularni faqat kerakli odam o‘qiy oladigan yozuvga aylantiradi. Xuddi shifrlangan xat kabi, uni faqat kaliti bor odam ochadi.

VPN – Maxfiy yo‘l

VPN xuddi shaxsiy tunnelga o‘xshaydi, ma'lumotlaringizni hech kim ko‘rmaydigan maxfiy yo‘l orqali yuboradi. VPN orqali kimdir sizni kuzatsa ham, ma'lumotlarni o‘qiy olmaydi.

Tarmoq xavfsizligining asosiy maqsadlari:

Maxfiylik (Confidentiality) – Ma'lumotlar faqat ruxsat etilgan foydalanuvchilar uchun ochiq bo‘lishi kerak. Bu shifrlash orqali ta'minlanadi.

Butunlik (Integrity) – Ma'lumotlar uzatilayotganda o‘zgarmasligi kerak. Hackerlar tarmoq orqali ma'lumotlarga o‘zgartirish kiritmasligi uchun xavfsizlik choralarini ko‘rish zarur.

.

Mavjudlik (Availability) – Tarmoq xizmatlari doim mavjud bo‘lishi kerak. DoS (Denial of Service) kabi hujumlardan himoya qilish orqali xizmatlarning uzluksiz ishlashi ta'minlanadi.

.

2. Ilova xavfsizligi

Ilova xavfsizligi dasturlar ichidagi xatoliklar va zaifliklar orqali kiritiladigan tahdidlarga qarshi kurashadi. Masalan, veb-saytda SQL injection zaifligi mavjud bo‘lsa, bu orqali foydalanuvchi ma’lumotlari o‘g‘irlanishi mumkin.

3. Axborot xavfsizligi

Bu tur axborotning maxfiyligi, yaxlitligi va mavjudligini ta’minlashga qaratilgan. Misol uchun, shaxsiy fayllarni parol bilan himoyalash yoki bulutli saqlashda shifrlash usullaridan foydalanish.

4. Operatsion tizim xavfsizligi

Operatsion tizimda ishlaydigan dasturlar va xizmatlar orqali tizimga zarar yetkazilishi mumkin. Masalan, Windows tizimida administrator huquqlari orqali nomaqbul dasturlar o‘rnatilishi xavfi mavjud.

5. Mobil xavfsizlik

Mobil qurilmalarda joylashgan shaxsiy ma’lumotlarni (kontaktlar, rasm, geolokatsiya) himoya qilish. Misol uchun, Android qurilmalarda noma’lum manbalardan dastur o‘rnatishni bloklash.

6. Bulutli xavfsizlik

Bulut texnologiyalaridan foydalanuvchi tashkilotlar o‘z ma’lumotlarini uchinchi tomon serverlarida saqlaydi. Bulutli xavfsizlik bu ma’lumotlar faqat ruxsat etilgan foydalanuvchilargagina ochiq bo‘lishini ta’minlaydi.

Amaliy misollar

1. 2021-yilda AQSHning Colonial Pipeline kompaniyasiga qilingan ransomware hujumi natijasida millionlab dollar zarar yetkazilgan. Bu holat sanoat tizimlarining ham kiber tahdidlarga nisbatan zaif ekanligini ko‘rsatadi.
2. O‘zbekiston Respublikasida davlat xizmatlarining ko‘plab tizimlari raqamlashtirilgani sababli, ularni himoya qilish maqsadida maxsus 'E-Xavfsizlik' markazlari tashkil etilgan.
3. O‘zbekistondagi bank mobil ilovalarida ikki bosqichli autentifikatsiya tizimlarining joriy etilishi mijozlarning hisob raqamlarini himoya qilishda muhim rol o‘ynaydi.

Xulosa

Kiber xavfsizlik — bu zamonaviy dunyoning ajralmas qismiga aylangan. Raqamli tizimlar, davlat idoralari, korxonalar va jismoniy shaxslar o‘z axborot resurslarini himoya qilish uchun doimiy ravishda yangi vosita va yondashuvlarga ehtiyoj sezmoqdalar. Tegishli xavfsizlik choralarini ko‘rish, foydalanuvchilarni ogohlikka chaqirish, tizimlarni yangilab borish va himoyalash vositalaridan foydalanish orqali tahdidlarning oldini olish mumkin.

Foydalanilgan adabiyotlar

1. Mirzaev U. 'Axborot xavfsizligi asoslari', Toshkent: Fan, 2021.
2. William Stallings. 'Network Security Essentials', Pearson Education, 2020.
3. ISO/IEC 27001: Axborot xavfsizligini boshqarish tizimi standartlari.

4. O‘zbekiston Respublikasi 'Axborot xavfsizligi to‘g‘risida'gi qonuni, 2020.

5. https://cybersecurityguide.org — Global kiber xavfsizlik bo‘yicha ma’lumotlar.