ISSN 2181-3187

KOMPYUTER TARMOQLARIDA AXBOROT ISHONCHLIGINI TA'MINLASH

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 kompyuter tarmoqlarida axborot ishonchligini ta'minlash mavzusini o'rganadi. Axborot xavfsizligi bugungi kunda jahon miqyosida dolzarb masalalardan biridir. Maqolada axborot ishonchliligining asosiy tamoyillari, xavflar va tahdidlar, himoya choralari va texnologiyalar yoritiladi. Shuningdek, axborot xavfsizligini ta'minlashda xalqaro standartlar va me'yoriy hujjatlarning o'rni muhokama qilinadi.

Kalit so'zlar: *Axborot xavfsizligi, kompyuter tarmoqlari, ishonchlilik, tahdidlar, himoya choralari, xalqaro standartlar.*

KIRISH

Axborot texnologiyalari rivojlanishi bilan kompyuter tarmoqlarida axborot ishonchligini ta'minlash masalasi tobora dolzarblashmoqda. Axborot ishonchliligi nafaqat texnik muammolarni hal qilish, balki ijtimoiy, iqtisodiy va huquqiy omillarni ham qamrab oladi. Tarmoqlar orqali o'tadigan ma'lumotlarning ishonchliligi va xavfsizligini ta'minlash kompaniya va tashkilotlarning barqaror ishlashi uchun muhimdir. Zamonaviy axborot texnologiyalari har bir sohaga chuqur kirib borishi bilan, axborot ishonchliligi masalalari ham ortib bormoqda.

Axborot ishonchliligi uch asosiy tamoyilga tayanadi: maxfiylik, yaxlitlik va mavjudlik. Maxfiylik axborotni ruxsatsiz kirishdan himoya qilishni anglatadi. Bu degani, faqat vakolatli shaxslar axborotga kira olishlari mumkin. Yaxlitlik esa axborotning to'liqligini va to'g'riligini saqlashni nazarda tutadi. Ma'lumotlar uzatish jarayonida yoki saqlash vaqtida o'zgarmasligi kerak. Mavjudlik esa axborotga zarur vaqt va joyda kirish imkoniyatini ta'minlaydi. Axborot xizmatlarining uzluksiz ishlashi muhim, chunki xizmatlarning to'xtashi ko'pincha jiddiy zarar keltirishi mumkin.

Kompyuter tarmoqlarida axborot xavfsizligini ta'minlash nafaqat texnologik yechimlarni, balki tashkiliy va inson omillarini ham o'z ichiga oladi. Masalan, xavfsizlik siyosatlarini ishlab chiqish va amalga oshirish, xodimlarni axborot

ISSN 2181-3187

xavfsizligi bo'yicha o'qitish va ularni muntazam ravishda yangilab turish muhimdir. Shuningdek, texnik jihatdan axborot xavfsizligini ta'minlash uchun turli xil xavfsizlik texnologiyalari, shifrlash usullari va tarmoq himoya tizimlari qo'llaniladi.

Bugungi kunda axborot xavfsizligi nafaqat korporativ yoki davlat tashkilotlari uchun, balki individual foydalanuvchilar uchun ham muhimdir. Shaxsiy ma'lumotlar, moliyaviy axborotlar va boshqa sezgir ma'lumotlarning himoyasi har bir foydalanuvchi uchun dolzarb masaladir. Internet va tarmoqlar orqali amalga oshiriladigan hujumlar soni ortib borayotgani sababli, axborot xavfsizligini ta'minlash bo'yicha kompleks yondashuv zarur.

Kompaniyalar va tashkilotlar uchun axborot xavfsizligini ta'minlash nafaqat hujumlardan himoyalanish, balki ular sodir bo'lganda tezkor va samarali javob qaytarish imkoniyatini ham o'z ichiga oladi. Shu bois, xavfsizlik strategiyalari va rejalari doimiy ravishda yangilanib turishi va zamonaviy xavflarga moslashtirilishi lozim. Xulosa qilib aytganda, kompyuter tarmoqlarida axborot ishonchligini ta'minlash zamonaviy dunyoda muvaffaqiyatli faoliyat yuritish uchun zaruriy shartlardan biri hisoblanadi.

Axborot xavfsizligining asosiy tamoyillari

Axborot xavfsizligi uchta asosiy tamoyilga asoslanadi: maxfiylik, yaxlitlik va mavjudlik. Bu tamoyillar axborotning ishonchliligini ta'minlashda muhim rol o'ynaydi.

Maxfiylik: Maxfiylik tamoyili axborotga faqat ruxsat etilgan foydalanuvchilar kira olishini ta'minlashni nazarda tutadi. Bu tamoyilni amalga oshirish uchun shifrlash texnologiyalari, kirish nazorati va autentifikatsiya vositalari qo'llaniladi. Maxfiylikni ta'minlash orqali maxfiy ma'lumotlar, tijorat sirlarini himoya qilish mumkin.

Yaxlitlik: Yaxlitlik tamoyili axborotning to'g'riligi va to'liqligini saqlashni anglatadi. Bu tamoyil axborot o'zgarmasligi va ruxsatsiz o'zgartirilmasligini ta'minlaydi. Yaxlitlikni ta'minlash uchun ma'lumotlarni imzolash, hash-funksiyalar va boshqa kriptografik texnologiyalar qo'llaniladi. Shu bilan birga, zaxiralash va ma'lumotlarni tiklash jarayonlari ham yaxlitlikni saqlashda muhim ahamiyatga ega.

Mavjudlik: Mavjudlik tamoyili axborot kerakli vaqtda foydalanishga tayyor bo'lishini ta'minlashni anglatadi. Bu tamoyilni amalga oshirish uchun tarmoq resurslarining optimal ishlashi, yuqori darajadagi ishonchlilik va tarmoq infratuzilmasining bardoshligini ta'minlash zarur. Tarmoq hujumlari, xizmatlar rad etilishi (DoS hujumlari) va boshqa tahdidlarga qarshi himoya choralari ko'rilishi kerak.

Xavflar va tahdidlar. Kompyuter tarmoqlarida axborotga nisbatan turli tahdidlar mavjud bo'lib, ular quyidagi turlarga bo'linadi:

Dasturiy tahdidlar:

Viruslar: Kompyuter viruslari o'z-o'zini ko'paytiruvchi dasturlar bo'lib, ular boshqa dasturlarni zararlaydi va axborotni buzishi mumkin.

ISSN 2181-3187

Troyanlar: Troyan dasturlari foydali dastur sifatida ko'rinib, aslida zararli funksiyalarni bajaradi.

Qurtlar: Qurtlar tarmoqlar orqali tarqaluvchi dasturlar bo'lib, ular ko'pincha tarmoqqa zarar yetkazadi yoki resurslarni isrof qiladi.

Tarmoq tahdidlari:

Denial of Service (DoS): DoS hujumlari tarmoq resurslarini haddan tashqari yuklash orqali xizmatlarni ishlamay qolishiga sabab bo'ladi.

Man-in-the-middle hujumlari: Bu hujumlar axborot uzatish jarayonida vositachilik qilib, ma'lumotlarni o'g'irlash yoki o'zgartirish imkonini beradi.

Ijtimoiy muhandislik:

Fishing: Foydalanuvchilardan parollar va boshqa maxfiy ma'lumotlarni o'g'irlash uchun aldov xabarlar yuboriladi.

Spear Fishing: Maqsadli phishing hujumlari bo'lib, aniq bir tashkilot yoki shaxsga qarshi amalga oshiriladi.

Himoya choralari va texnologiyalar

Axborot xavfsizligini ta'minlash uchun quyidagi chora-tadbirlar va texnologiyalar qo'llaniladi:

Kriptografiya:

Shifrlash: Ma'lumotlarni shifrlash orqali ularning maxfiyligini saqlash. Asimmetrik va simmetrik shifrlash usullari keng qo'llaniladi.

Raqamli imzolar: Ma'lumotlarning yaxlitligi va autentifikatsiyasini ta'minlash uchun qo'llaniladi.

Tarmoqlarni monitoring qilish:

Intrusion Detection Systems (IDS): Hujumlarni erta aniqlash va oldini olish tizimlari.

Firewall: Tarmoq trafikini nazorat qilish va zararli trafikni bloklash uchun qo'llaniladi.

Dasturiy ta'minot yangilanishlari:

Patch Management: Zararli dasturlardan himoya qilish uchun doimiy yangilanishlar va xavfsizlik yamalarini o'rnatish.

Zaxiralash va ma'lumotlarni tiklash:

Backup and Recovery: Axborotning yaxlitligini ta'minlash va yo'qolgan ma'lumotlarni tiklash uchun zaxira nusxalarini yaratish.

Xalqaro standartlar va me'yoriy hujjatlar

Axborot xavfsizligini ta'minlashda xalqaro standartlar va me'yoriy hujjatlar muhim ahamiyatga ega.

Misol uchun:

ISO/IEC 27001: Axborot xavfsizligi boshqaruv tizimlari uchun xalqaro standart bo'lib, tashkilotlarga axborot xavfsizligini boshqarish bo'yicha talablarni belgilaydi. Bu

ISSN 2181-3187

standart axborot xavfsizligi siyosatlarini, jarayonlarini va nazorat choralarini ishlab chiqish va amalga oshirishda yo'l-yo'riq ko'rsatadi.

NIST SP 800-53: AQSh milliy standartlar va texnologiyalar instituti (NIST) tomonidan ishlab chiqilgan xavfsizlik va xususiylik nazoratlari. Ushbu hujjat axborot tizimlarini himoya qilish uchun zarur bo'lgan xavfsizlik choralari va amaliyotlarini tavsiya etadi.

GDPR (General Data Protection Regulation): Yevropa Ittifoqi tomonidan joriy etilgan ma'lumotlarni himoya qilish qoidalari bo'lib, u axborotning maxfiyligini saqlash va shaxsiy ma'lumotlarni himoya qilishni nazorat qiladi.

Axborot xavfsizligi strategiyalari. Axborot xavfsizligini ta'minlash uchun tashkilotlar strategik yondashuvlarni qo'llashi zarur. Bu yondashuvlar quyidagi bosqichlarni o'z ichiga oladi:

Xavflarni baholash va boshqarish: Tashkilot o'ziga tahdid solishi mumkin bo'lgan xavflarni aniqlab, ularni baholaydi va boshqarish choralarini ko'radi. Xavflarni baholash orqali tashkilot muhim resurslarini himoya qilish uchun zarur bo'lgan choralarning ustuvorligini belgilaydi.

Xodimlarni o'qitish va xabardorlikni oshirish: Axborot xavfsizligi bo'yicha xodimlarni muntazam ravishda o'qitish va ularning xabardorligini oshirish muhimdir. Xodimlar xavfsizlik siyosatlari va protseduralarini yaxshi bilishi va ularga rioya qilishi kerak.

Yordamchi infratuzilma va texnologiyalarni joriy etish: Tashkilot axborot xavfsizligini ta'minlash uchun kerakli infratuzilma va texnologiyalarni joriy etadi. Bu texnologiyalar orasida firewall, IDS/IPS tizimlari, VPN, antivirus dasturlari va boshqalar mavjud.

Doimiy monitoring va audit: Axborot xavfsizligi siyosatlari va choralari doimiy ravishda monitoring qilinishi va audit qilinishi zarur. Bu orqali xavfsizlik holati nazorat qilinadi va zarur bo'lganda tuzatishlar kiritiladi.

XULOSA

Kompyuter tarmoqlarida axborot ishonchligini ta'minlash zamonaviy dunyoda tobora muhim masalalardan biri hisoblanadi. Axborot xavfsizligi uch asosiy tamoyilga - maxfiylik, yaxlitlik va mavjudlikka asoslanib, ma'lumotlarning ishonchli va himoyalangan holda saqlanishini ta'minlaydi. Ushbu tamoyillar tashkilotlarning axborot resurslarini himoya qilishda muhim rol o'ynaydi.

Axborot xavfsizligini ta'minlash uchun tashkilotlar xavflarni baholash va boshqarish, xodimlarni muntazam ravishda o'qitish va xabardorlikni oshirish, yordamchi infratuzilma va texnologiyalarni joriy etish hamda doimiy monitoring va auditni amalga oshirishi zarur. Xavflarni baholash orqali tashkilotlar muhim resurslarini aniqlab, ularni himoya qilish uchun zarur bo'lgan choralarning

ISSN 2181-3187

ustuvorligini belgilaydi. Xodimlarning axborot xavfsizligi bo'yicha bilimlarini oshirish esa inson omili tufayli yuzaga keladigan xavflarni kamaytirishga yordam beradi.

Zamonaviy texnologiyalar va himoya vositalarining joriy etilishi axborot xavfsizligini ta'minlashda katta ahamiyatga ega. Firewall, Intrusion Detection and Prevention Systems (IDS/IPS), Virtual Private Network (VPN), antivirus dasturlari va boshqa texnologiyalar tarmoq va axborot xavfsizligini mustahkamlashga yordam beradi. Shuningdek, kriptografik texnologiyalar, ma'lumotlarni shifrlash, raqamli imzolar va hash-funksiyalar ma'lumotlarning maxfiyligini, yaxlitligini va autentifikatsiyasini ta'minlaydi.

Xalqaro standartlar va me'yoriy hujjatlar, masalan, ISO/IEC 27001 va NIST SP 800-53, axborot xavfsizligini boshqarish va nazorat qilish bo'yicha umumiy qoidalarni belgilaydi. Bu standartlar tashkilotlarga axborot xavfsizligi siyosatlarini ishlab chiqish, amalga oshirish va muntazam ravishda yangilashda yordam beradi. Ularning amal qilinishi tashkilotlarga nafaqat milliy, balki xalqaro miqyosda ham axborot xavfsizligini ta'minlashga yordam beradi.

Umuman olganda, kompyuter tarmoqlarida axborot ishonchligini ta'minlash tashkilotlarning samarali va barqaror ishlashi uchun zarur shartlardan biridir. Axborot xavfsizligi strategiyalari va choralari, xalqaro standartlarga rioya qilish va zamonaviy texnologiyalarni qo'llash orqali tashkilotlar o'z axborot resurslarini himoya qila oladi. Bu esa ularning raqobatbardoshligini oshirish, mijozlar va hamkorlar bilan ishonchli munosabatlarni saqlash va global miqyosda muvaffaqiyatli faoliyat yuritishiga xizmat qiladi.

ADABIYOTLAR RO'YXATI

1. ISO/IEC 27001:2013: Axborot xavfsizligi boshqaruv tizimlari - Talablar.

2. NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations.

3. Stallings, W. (2017). Network Security Essentials: Applications and Standards. Pearson.

4. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.

5. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

6. GDPR (General Data Protection Regulation): Yevropa Ittifoqi tomonidan joriy etilgan ma'lumotlarni himoya qilish qoidalari.