ISSN 3060-4567

KOMPYUTER TARMOQLARI XAVFSIZLIGINI TA'MINLASHDA ADMINISTRATORNING ROLI

Toshkent viloyati, Bo‘stonliq tumani, 1-son politexnikum

Abduvaliyev Abdujamol Abdurasul o‘g‘li

fan: Kompyuter tarmoqlari va administratorlash

Elektron pochta manzili: fmswerance@gmail.com

Telefon raqami: +998 95 750 45 95

Annotatsiya: *Kompyuter tarmoqlari xavfsizligi zamonaviy axborot texnologiyalari sohasida eng dolzarb masalalardan biridir. Tarmoqlarning murakkablashishi va raqamli transformatsiya jarayonlarining kengayishi kiberxavfsizlikka bo‘lgan ehtiyojni yanada oshirdi. Tarmoq administratorining roli tizimning xavfsizligini ta’minlash, ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini kafolatlashda markaziy ahamiyatga ega. Ushbu maqolada tarmoq administratorining asosiy vazifalari, xavfsizlikni ta’minlashda qo‘llaniladigan texnologiyalar, zamonaviy kiberxavfsizlik tahdidlariga qarshi kurash usullari va strategik yondashuvlari keng yoritiladi. Shuningdek, maqolada profilaktik choralar, avtomatlashtirilgan tizimlardan foydalanish, xodimlarning kiberxavfsizlik bo‘yicha bilimlarini oshirish va xavfsizlik hodisalariga javob berish jarayonlari tahlil qilinadi. Ushbu tadqiqot kiberxavfsizlik sohasida faoliyat yurituvchi mutaxassislar, tashkilot rahbarlari va axborot texnologiyalari sohasida ta’lim oluvchi talabalar uchun qimmatli manba bo‘lib xizmat qilishi kutilmoqda.*

Kalit so‘zlar: *kompyuter tarmoqlari, xavfsizlik, tarmoq administratori, kiberxavfsizlik, kiber tahdidlar, profilaktik choralar, avtomatlashtirish, ma’lumotlar maxfiyligi, tizim monitoringi, xavfsizlik devori, zaxira nusxalash, sun’iy intellekt, incident boshqaruvi.*

Kirish

Kompyuter tarmoqlari zamonaviy dunyoda axborot almashinuvining asosiy vositasi sifatida xizmat qiladi. Ular tashkilotlarning biznes jarayonlarini

avtomatlashtirish, ma’lumotlarni tezkor uzatish va global miqyosda aloqa o‘rnatish imkonini beradi. Banklar, sog‘liqni saqlash muassasalari, davlat idoralari, ta’lim muassasalari va xususiy sektor korxonalari o‘z faoliyatida tarmoqlarga tayanadi. Biroq, tarmoqlarning kengayishi va ularning murakkablashishi kiberxavfsizlik tahdidlarining ortishiga olib keldi. Xakerlik hujumlari, zararli dasturlar, ma’lumotlarni o‘g‘irlash, fidya dasturlari va boshqa kiberjinoyatlar tashkilotlar uchun jiddiy xavf tug‘diradi. Bunday sharoitda tarmoq xavfsizligini ta’minlash tashkilotning moliyaviy barqarorligi, obro‘si va hatto qonuniy mas'uliyati nuqtai nazaridan muhim ahamiyatga ega.

Tarmoq administratori tarmoq xavfsizligini ta’minlashda asosiy rol o‘ynaydi. U tarmoq infratuzilmasini boshqaradi, xavfsizlik choralarini joriy etadi, tahdidlarni aniqlaydi va ularga javob beradi. Administratorning vazifalari nafaqat texnik bilimlarni, balki strategik fikrlash, tezkor qaror qabul qilish va xodimlar bilan hamkorlik qilish qobiliyatini talab qiladi. So‘nggi yillarda kiberxavfsizlik sohasida sun’iy intellekt, mashinaviy o‘qitish va avtomatlashtirilgan tizimlar keng joriy etilmoqda. Biroq, bu texnologiyalar administratorning tajribasi va professional yondashuvini to‘liq almashtira olmaydi. Ushbu maqola tarmoq administratorining xavfsizlikni ta’minlashdagi mas'uliyatini, qo‘llaniladigan texnologiyalarni, zamonaviy tahdidlarga qarshi kurash usullarini va kelajakdagi istiqbollarini chuqur tahlil qilishga qaratilgan. Maqola kiberxavfsizlik sohasida ishlaydigan mutaxassislar, tashkilot rahbarlari va axborot texnologiyalari sohasida ta’lim oluvchilar uchun foydali manba bo‘lib xizmat qiladi.

Tarmoq xavfsizligining asosiy jihatlari

Tarmoq xavfsizligining ahamiyati va tamoyillari

Kompyuter tarmoqlari xavfsizligi ma’lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashga qaratilgan. Ushbu uchta tamoyil kiberxavfsizlikning asosini tashkil qiladi:

- **Maxfiylik**: Maxfiy ma’lumotlar faqat ruxsat berilgan shaxslar uchun ochiq bo‘lishi kerak. Masalan, bank mijozlarining moliyaviy ma’lumotlari yoki shaxsiy tibbiy yozuvlar ruxsatsiz shaxslar uchun yopiq bo‘lishi zarur.

- **Yaxlitlik**: Ma’lumotlar o‘zgartirilmasligi yoki buzilmasligi kerak. Agar ma’lumotlar xakerlar tomonidan manipulyatsiya qilinsa, bu tashkilotning qaror qabul qilish jarayonlariga yoki mijozlar ishonchiga putur yetkazadi.
- **Mavjudlik**: Tarmoq va ma’lumotlar foydalanuvchilar uchun doimiy ravishda ochiq bo‘lishi kerak. Masalan, DDoS (Distributed Denial of Service) hujumlari tarmoqning mavjudligiga xavf tug‘diradi va xizmatlarning uzilishiga olib keladi.

Tarmoq xavfsizligining ahamiyati zamonaviy dunyoda tobora ortib bormoqda. Tashkilotlar raqamli texnologiyalarga ko‘proq tayanmoqda, bu esa maxfiy ma’lumotlarni himoya qilishni dolzarb vazifaga aylantiradi. Xavfsizlik buzilishi moliyaviy yo‘qotishlar, mijozlar ishonchining yo‘qolishi, qonuniy jarimalar va obro‘ga putur yetkazishi mumkin. Masalan, 2023 yilda dunyo bo‘ylab yirik kompaniyalar kiberhujumlar tufayli milliardlab dollar yo‘qotgan, bu esa tarmoq xavfsizligiga sarmoya kiritish zarurligini ko‘rsatadi. Tarmoq administratori ushbu tamoyillarni amalda ta’minlash uchun tizimli yondashuvni qo‘llaydi va tashkilotning xavfsizlik strategiyasini shakllantirishda muhim rol o‘ynaydi.

Zamonaviy kiberxavfsizlik tahdidlari va ularning xususiyatlari

Kiberxavfsizlik tahdidlari doimo rivojlanmoqda va tarmoq administratorlari uchun yangi sinovlar yaratmoqda. Zamonaviy tahdidlar xilma-xil bo‘lib, quyidagi asosiy turlarni o‘z ichiga oladi:

- **Xakerlik hujumlari**: Ma’lumotlarni o‘g‘irlash, tizimni buzish yoki xizmatdan chiqarish maqsadida amalga oshiriladigan hujumlar. Masalan, SQL injeksiyasi yoki parolni o‘g‘irlash usullari orqali maxfiy ma’lumotlarga kirish mumkin.
- **Zararli dasturlar**: Viruslar, troyanlar, fidya dasturlari (ransomware), qurtlar va boshqa zararli dasturiy ta’minotlar tarmoqqa jiddiy xavf tug‘diradi. Fidya dasturlari ma’lumotlarni shifrlab, ularni qaytarish evaziga pul talab qiladi.
- **Fishing hujumlari**: Foydalanuvchilarni aldash orqali maxfiy ma’lumotlarni o‘g‘irlash. Masalan, soxta elektron pochta xabarlari orqali foydalanuvchilar bank kartasi ma’lumotlarini kiritishga majburlanadi.

- **Ichki tahdidlar**: Tashkilot xodimlari tomonidan qasddan yoki tasodifan yuzaga keladigan xavfsizlik buzilishlari. Masalan, xodim tasodifan maxfiy ma’lumotlarni ochiq joylashtirishi yoki zararli havolani bosishi mumkin.
- **Noma’lum zaifliklar (zero-day exploits)**: Dasturiy ta’minotdagi noma’lum xatolar xakerlar tomonidan foydalaniladi. Bunday zaifliklar aniqlanmaguncha tizim xavf ostida qoladi.
- **IoT (Internet of Things) tahdidlari**: Aqlli qurilmalar (masalan, kameralar, sensorlar) tarmoqqa ulanganda ular zaif nuqta sifatida ishlatilishi mumkin.
- **Sosyal muhandislik**: Foydalanuvchilarning psixologik zaifliklaridan foydalanish orqali ma’lumotlarni o‘g‘irlash. Masalan, xodimni telefon orqali aldash orqali tarmoqqa kirish mumkin.

Ushbu tahdidlarning xilma-xilligi tarmoq administratoridan keng qamrovli bilimlar, doimiy o‘qish va yangi texnologiyalarni o‘zlashtirishni talab qiladi. Administrator nafaqat mavjud tahdidlarga qarshi choralar ko‘rishi, balki kelajakda yuzaga kelishi mumkin bo‘lgan xavflarni bashorat qilishi va ularga tayyor bo‘lishi kerak. Masalan, sun’iy intellektga asoslangan hujumlar yoki kvant hisoblash texnologiyalari kelajakda kiberxavfsizlik landshaftini tubdan o‘zgartirishi mumkin.

Tarmoq administratorining asosiy vazifalari

Tarmoq infratuzilmasini boshqarish va himoya qilish

Tarmoq administratori tarmoq infratuzilmasining uzluksiz, xavfsiz va samarali ishlashini ta’minlaydi. Bu vazifa tarmoq uskunalarini (routerlar, kommutatorlar, serverlar, xavfsizlik devorlari) sozlash, ularga xizmat ko‘rsatish, yangilash va nosozliklarni bartaraf etishni o‘z ichiga oladi. Administrator tarmoqning ishlash ko‘rsatkichlarini real vaqtda monitoring qiladi, masalan, tarmoq tezligi, kechikishlar yoki ulanish muammolarini aniqlaydi va ularni tezkor hal qiladi.

Xavfsizlik nuqtai nazaridan, administrator tarmoqqa ruxsatsiz kirishni oldini olish uchun bir qator choralar ko‘radi. Masalan, u firewall (xavfsizlik devori) sozlamalarini optimallashtiradi, tarmoqqa faqat ruxsat berilgan qurilmalar ulanishini ta’minlaydi va VPN (virtual xususiy tarmoq) orqali xavfsiz aloqa kanallarini yaratadi.

Tarmoq segmentatsiyasi ham muhim strategiya hisoblanadi: tarmoq turli zonalarga bo‘linadi, har bir zona uchun alohida xavfsizlik qoidalari qo‘llaniladi. Bu yondashuv bir segmentda xavfsizlik buzilishi yuzaga kelsa, uning butun tarmoqqa tarqalishini oldini oladi. Misol tariqasida, bank tarmoqlarida mijozlar ma’lumotlari saqlanadigan serverlar alohida segmentda joylashadi va qat’iy nazorat qilinadi.

Administrator shuningdek, tarmoq uskunalarining dasturiy ta’minotini muntazam yangilaydi. Dasturiy ta’minotdagi zaifliklar xakerlar tomonidan foydalanilishi mumkin, shuning uchun yangilanishlar xavfsizlikni oshirishda muhim rol o‘ynaydi. Masalan, router dasturiy ta’minotidagi noma’lum zaiflik xakerlar tomonidan tarmoqqa kirish uchun ishlatilishi mumkin, ammo muntazam yangilanishlar bunday xavfni kamaytiradi.

Xavfsizlik siyosatini ishlab chiqish va amalga oshirish

Tarmoq administratori tashkilotning xavfsizlik siyosatini ishlab chiqishda va uni amalda joriy etishda muhim rol o‘ynaydi. Xavfsizlik siyosati tarmoqdan foydalanish qoidalarini, ma’lumotlarni himoya qilish choralarini, xodimlarning mas'uliyatini va xavfsizlik buzilishlariga javob berish tartibini belgilaydi. Administrator ushbu siyosatning tashkilotning ehtiyojlariga mos kelishini ta’minlaydi va uni barcha xodimlarga yetkazadi.

Masalan, administrator kuchli parollar qo‘yishni majburiy qiladi, masalan, kamida 12 belgidan iborat, katta-kichik harflar, raqamlar va maxsus belgilarni o‘z ichiga olgan parollar. Ikki faktorli autentifikatsiya (2FA) joriy etiladi, bu foydalanuvchi login va paroldan tashqari qo‘shimcha tasdiqlash (masalan, SMS-kod yoki autentifikator ilovasi) talab qiladi. Maxfiy ma’lumotlar shifrlanadi, bu ularni o‘g‘irlansa ham foydasiz qiladi. Administrator shuningdek, tarmoqdan foydalanishni cheklovchi qoidalar joriy etadi, masalan, shaxsiy qurilmalarni tarmoqqa ulashni ta’qiqlaydi yoki faqat ishonchli Wi-Fi tarmoqlaridan foydalanishni talab qiladi.

Xodimlarning kiberxavfsizlik bo‘yicha bilimlarini oshirish ham administratorning muhim vazifalaridan biridir. Ko‘pincha xavfsizlik buzilishlari inson omili tufayli yuzaga keladi, masalan, xodim fishing xatidagi havolani bosadi yoki maxfiy ma’lumotlarni ochiq joylashtiradi. Administrator xodimlar uchun

ISSN 3060-4567

muntazam treninglar tashkil qiladi, ularda fishing hujumlarini aniqlash, xavfsiz parollar yaratish va maxfiy ma’lumotlarni himoya qilish bo‘yicha ko‘nikmalar o‘rgatiladi. Bu tashkilotning umumiy xavfsizlik madaniyatini shakllantirishga yordam beradi.

Tizim monitoringi va tahdidlarni aniqlash

Tarmoq xavfsizligini ta’minlashda tizim monitoringi muhim ahamiyatga ega. Administrator tarmoq faoliyatini real vaqt rejimida kuzatib boradi va shubhali harakatlarni aniqlaydi. Buning uchun u Intrusion Detection Systems (IDS) va Intrusion Prevention Systems (IPS) kabi maxsus tizimlardan foydalanadi. IDS tarmoqda shubhali faoliyatni aniqlaydi va ogohlantirish yuboradi, IPS esa bunday harakatlarni avtomatik ravishda bloklaydi. Masalan, agar tarmoqda noodatiy trafik (masalan, bir IP manzildan ko‘p sonli so‘rovlar) aniqlansa, IPS uni bloklashi mumkin.

Administrator tarmoq jurnallarini (log files) muntazam tahlil qiladi. Jurnallar tarmoqda sodir bo‘lgan barcha voqealarni qayd etadi, masalan, foydalanuvchi ulanishlari, fayl o‘zgartirishlari yoki xavfsizlik hodisalari. Agar xavfsizlik buzilishi yuzaga kelsa, jurnallar muammoning manbasini aniqlashda muhim dalil bo‘ladi. Masalan, jurnalda tarmoqqa ruxsatsiz kirish urinishlari qayd etilgan bo‘lsa, administrator bu IP manzilni bloklashi va qo‘shimcha choralar ko‘rishi mumkin.

Monitoring jarayonida sun’iy intellekt va mashinaviy o‘qitish texnologiyalari tobora muhim ahamiyat kasb etmoqda. Bu tizimlar tarmoq trafifidagi anomaliyalarni aniqlash, odatdan tashqari xatti-harakatlar qoidalarini topish va potentsial tahdidlarni bashorat qilishda yordam beradi. Masalan, AI-ga asoslangan tizim foydalanuvchining odatiy faoliyatidan chetga chiqadigan harakatlarni (masalan, tungi vaqtda fayllarni ommaviy yuklab olish) aniqlashi va administratorni ogohlantirishi mumkin.

Xavfsizlik buzilishlariga javob berish va incident boshqaruvi

Xavfsizlik buzilishi yuzaga kelganda tarmoq administratori tezkor va samarali choralar ko‘rishga mas‘uldir. Bu jarayon incident boshqaruvi deb ataladi va quyidagi bosqichlarni o‘z ichiga oladi:

- **Aniqlash va baholash**: Xavfsizlik buzilishini aniqlash va uning ko‘lamini baholash. Masalan, zararli dastur tarmoqning qaysi qismiga tarqaldi yoki qanday ma’lumotlar o‘g‘irlandi?
- **Izolatsiya**: Buzilish tarqalishini oldini olish uchun zararlangan tizimni tarmoqdan ajratish. Masalan, zararlangan server tarmoqdan uziladi.
- **Bartaraf etish**: Muammoni hal qilish, masalan, zararli dasturni o‘chirish, zaifliklarni tuzatish yoki tarmoq sozlamalarini qayta ko‘rib chiqish.
- **Qayta tiklash**: Tizimning normal ishlashini tiklash va zaxira nusxalardan foydalanish. Masalan, fidya dasturi hujumida ma’lumotlar zaxira nusxalardan qayta tiklanadi.
- **Tahlil va oldini olish**: Buzilish sabablarini tahlil qilish va kelajakda bunday hodisalarni oldini olish uchun choralar ko‘rish. Masalan, zaiflik tuzatiladi yoki xodimlar uchun qo‘shimcha treninglar tashkil qilinadi.
- **Hujjatlashtirish**: Hodisani va ko‘rilgan choralarni qayd etish. Bu kelajakda o‘xshash muammolarni hal qilishda yordam beradi.

Administratorning tezkor harakatlari tashkilotning moliyaviy va obro‘ga oid yo‘qotishlarini kamaytiradi. Masalan, 2022 yilda yirik savdo kompaniyasi fidya dasturi hujumiga uchradi, ammo administratorning tezkor chorasi tufayli ma’lumotlar zaxira nusxalardan tiklandi va xizmatlar qisqa muddatda qayta ishga tushdi. Administrator shuningdek, xavfsizlik buzilishi haqida rahbariyatni xabardor qiladi va kerak bo‘lsa, huquq-tartib idoralariga murojaat qiladi.

Xodimlar bilan hamkorlik va xavfsizlik madaniyatini shakllantirish

Tarmoq xavfsizligi faqat texnik choralar bilan cheklanmaydi; inson omili ham muhim ahamiyatga ega. Administrator xodimlarning kiberxavfsizlik bo‘yicha bilimlarini oshirish uchun muntazam treninglar va seminarlar tashkil qiladi. Treninglarda quyidagi mavzular yoritiladi:

- Fishing hujumlarini aniqlash va ulardan himoyalanish.
- Xavfsiz parollar yaratish va ularni boshqarish.
- Maxfiy ma’lumotlarni himoya qilish qoidalari.
- Tashqi qurilmalarni (USB fleshkalar, tashqi disklarni) xavfsiz ishlatish.

Administrator shuningdek, tashkilot ichida xavfsizlik madaniyatini shakllantirishga harakat qiladi. Bu xodimlarni xavfsizlik qoidalariga rioya qilishga undash, shubhali harakatlar haqida xabar berishni rag‘batlantirish va mas'uliyatni oshirishni anglatadi. Masalan, xodim shubhali elektron pochta xabarini darhol administratorga xabar qilsa, bu potentsial fishing hujumining oldini olishga yordam beradi.

Administrator tomonidan qo‘llaniladigan texnologiyalar

Xavfsizlik devorlari va virtual xususiy tarmoqlar

Xavfsizlik devorlari (firewalls) tarmoq xavfsizligining asosiy vositalaridan biridir. Ular tarmoqqa kiruvchi va chiqadigan trafikni nazorat qiladi va ruxsatsiz kirishni bloklaydi. Administrator xavfsizlik devorini sozlash orqali faqat ruxsat berilgan IP manzillar, portlar yoki protokollar orqali ulanishga ruxsat beradi. Masalan, firewall ma’lum mamlakatlardan keladigan trafikni bloklashi yoki shubhali portlar orqali ulanishlarni cheklashi mumkin. Zamonaviy xavfsizlik devorlari (next-generation firewalls) nafaqat trafikni filtrlaydi, balki zararli dasturlarni aniqlash, tarmoq trafifini shifrlash va anomaliyalarni tahlil qilish imkonini ham beradi.

Virtual xususiy tarmoqlar (VPN) maxfiy ma’lumotlarni shifrlash va xavfsiz aloqa kanallarini ta’minlash uchun ishlatiladi. VPN tarmoqqa masofadan ulangan foydalanuvchilarning ma’lumotlarni xavfsiz uzatishini ta’minlaydi. Masalan, masofaviy ishlayotgan xodim kompaniya tarmog‘iga VPN orqali ulanadi, bu uning ma’lumotlari umumiy Wi-Fi tarmoqlarida o‘g‘irlanishining oldini oladi. Administrator VPN tizimini sozlaydi, foydalanuvchilar uchun kirish ruxsatlarini boshqaradi va shifrlash protokollarini yangilaydi.

Antiviral dasturlar va zararli dasturlarga qarshi himoya

Antivirus va antimalware dasturlari tarmoqqa zararli dasturlarni aniqlash va yo‘q qilish uchun muhim vositalardir. Administrator ushbu dasturlarni tarmoqqa o‘rnatadi va ularning doimiy yangilanishini ta’minlaydi. Zamonaviy antivirus dasturlari quyidagi funksiyalarni bajaradi:

- **Real vaqtda skanerlash**: Fayllar, elektron pochta va tarmoq trafiki real vaqtda tekshiriladi.
- **Avtomatik yangilanish**: Virus bazasi muntazam yangilanadi, bu yangi tahdidlarni aniqlash imkonini beradi.
- **Izolyatsiya va o‘chirish**: Zararli dastur aniqlansa, u izolyatsiya qilinadi yoki tizimdan o‘chiriladi.
- **Xatti-harakat tahlili**: Dasturlarning shubhali harakatlari (masalan, fayllarni shifrlash) aniqlanadi.

Administrator shuningdek, endpoint protection platformalaridan (EPP) foydalanadi. EPP tarmoqqa ulangan har bir qurilmani (kompyuterlar, smartfonlar, planshetlar) himoya qiladi va markazlashtirilgan boshqaruv imkonini beradi. Masalan, agar xodimning shaxsiy qurilmasi tarmoqqa ulansa va zararli dastur aniqlansa, EPP uni avtomatik bloklaydi.

Tarmoq monitoringi va tahlil vositalari

Tarmoq monitoringi va tahlil vositalari administratorga tarmoq faoliyatini real vaqtda kuzatish va potentsial tahdidlarni aniqlash imkonini beradi. Eng keng tarqalgan vositalar quyidagilar:

- **Wireshark**: Tarmoq trafifigini tahlil qilish uchun ishlatiladi. Administrator Wireshark yordamida tarmoq paketlarini ko‘rib chiqadi va shubhali faoliyatni aniqlaydi.
- **Nagios**: Tizim va tarmoqning ishlashini monitoring qiladi. Nagios tarmoq kechikishlari, server nosozliklari yoki resurslarning haddan tashqari yuklanishini aniqlaydi.
- **Splunk**: Jurnal ma’lumotlarini tahlil qilish va xavfsizlik hodisalarini aniqlash uchun ishlatiladi. Splunk sun’iy intellekt yordamida anomaliyalarni aniqlaydi va hodisalarni avtomatik tasniflaydi.
- **SolarWinds**: Tarmoq infratuzilmasini boshqarish va monitoring qilish uchun keng qamrovli yechim. Bu vosita tarmoqning ishlash ko‘rsatkichlarini vizualizatsiya qiladi va nosozliklarni aniqlaydi.

Ushbu vositalar administrator'ga tarmoqda yuzaga keladigan anomaliyalarni aniqlashda yordam beradi. Masalan, agar tarmoqda noodatiy trafik (masalan, bir IP manzildan ko'p sonli so'rovlar) aniqlansa, administrator bu DDoS hujumi yoki xakerlik urunishi ekanligini tahlil qiladi va tegishli choralar ko'radi.

Zaxira nusxalash va qayta tiklash tizimlari

Ma'lumotlarning yo'qolishi tashkilot uchun jiddiy oqibatlarga olib kelishi mumkin. Administrator muntazam zaxira nusxalar yaratadi va ma'lumotlarni qayta tiklash jarayonini rejalashtiradi. Zaxira nusxalar bulutli xizmatlarda (masalan, Amazon S3, Microsoft Azure) yoki alohida fizik serverlarda saqlanadi. Zaxira nusxalash jarayonida:

- **Muntazamlik**: Ma'lumotlar har kuni yoki haftada bir marta zaxiralanadi.
- **Shifrlash**: Zaxira nusxalar shifrlanadi, bu ularning o'g'irlanish xavfini kamaytiradi.
- **Sinaytish**: Zaxira nusxalar muntazam sinovdan o'tkaziladi, bu ularning ishlayotganligini tasdiqlaydi.

Masalan, fidya dasturi hujumi yuzaga kelsa, administrator zaxira nusxalar yordamida ma'lumotlarni qayta tiklaydi va tizimning normal ishlashini ta'minlaydi. Zaxira nusxalar tashkilotning faoliyatini uzluksiz davom ettirishda muhim ahamiyatga ega.

Sun'iy intellekt va mashinaviy o'qitish texnologiyalari

Sun'iy intellekt (AI) va mashinaviy o'qitish (ML) kiberxavfsizlikda tobora muhim rol o'ynamoqda. Administrator AI-ga asoslangan tizimlardan foydalanib, tarmoq trafifidagi anomaliyalarni aniqlaydi, potentsial tahdidlarni bashorat qiladi va xavfsizlik hodisalariga avtomatik javob beradi. Masalan:

- **Anomaliya aniqlash**: AI foydalanuvchilarning odatdan tashqari xatti-harakatlarini (masalan, tungi vaqtda fayllarni ommaviy yuklash) aniqlaydi.
- **Tahdid tahlili**: ML algoritmlari jurnal ma'lumotlarini tahlil qilib, xakerlik hujumlari qoidalarini aniqlaydi.

- **Avtomatlashtirilgan javob**: AI shubhali faoliyatni aniqlaganda avtomatik choralar ko‘radi, masalan, IP manzilni bloklaydi yoki foydalanuvchi sessiyasini to‘xtatadi.

Administrator AI tizimlarini sozlash va ularning natijalarini tahlil qilishda faol ishtirok etadi. Biroq, AI inson tajribasini to‘liq almashtira olmaydi, chunki murakkab hodisalarda administrator’ning qarori muhim ahamiyatga ega.

Xulosa

Kompyuter tarmoqlari xavfsizligini ta’minlashda tarmoq administratorining roli markaziy va ko‘p qirrali hisoblanadi. Administrator tarmoq infratuzilmasini boshqaradi, xavfsizlik siyosiyatini ishlab chiqadi va joriy etadi, tizim monitoringini amalga oshiradi, xavfsizlik buzilishlariga javob beradi va xodimlarning kiberxavfsizlik bilimlarini oshiradi. U xavfsizlik devorlari, VPN, antivirus dasturlari, monitoring vositalari, zaxira nusxalash tizimlari va sun’iy intellektga asoslangan texnologiyalardan foydalanadi. Zamonaviy kiberxavfsizlik tahdidlarining xilma-xilligi va murakkabligi administratorlardan keng qamrovli bilimlar, doimiy o‘qish va strategik yondashuvni talab qiladi.

Kelajakda tarmoq xavfsizligi sohasi yanada rivojlanadi. Sun’iy intellekt, mashinaviy o‘qitish, kvant hisoblash va IoT texnologiyalari kiberxavfsizlik landshaftini tubdan o‘zgartiradi. Biroq, administratorning tajribasi, tezkor qaror qabul qilish qobiliyati va tashkilot ichida xavfsizlik madaniyatini shakllantirishdagi roli muhim bo‘lib qoladi. Ushbu sohada olib boriladigan tadqiqotlar va innovatsiyalar tashkilotlarni kiberxavflardan himoya qilishda yangi imkoniyatlar yaratadi va xavfsiz raqamli muhitni shakllantirishga xiz. Tarmoq xavfsizligi nafaqat texnik masala, balki tashkilotning barqarorligi va ishonchliligini ta’minlashning asosiy omilidir.

FOYDALANILGAN ADABIYOTLAR

1. STALLINGS, W. (2021). *NETWORK SECURITY ESSENTIALS: APPLICATIONS AND STANDARDS*. BOSTON: PEARSON.

2. KIM, D., & SOLOMON, M. (2020). *FUNDAMENTALS OF INFORMATION SYSTEMS SECURITY*. SUDBURY: JONES & BARTLETT PUBLISHERS.

3. AXMEDOV, SH. (2019). *KIBERXAVFSIZLIK ASOSLARI*. TOSHKENT: FAN VA TEXNOLOGIYA.

4. ANDERSON, R. (2022). *SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE SYSTEMS*. CAMBRIDGE: WILEY.

5. XASANOV, B. (2021). *TARMOQ XAVFSIZLIGI VA MONITORING TIZIMLARI*. SAMARQAND: SAMDU NASHRIYOTI.

6. CISCO. (2023). *CYBERSECURITY OPERATIONS HANDBOOK*. SAN FRANCISCO: CISCO PRESS.

7. WHITMAN, M. E., & MATTORD, H. J. (2022). *PRINCIPLES OF INFORMATION SECURITY*. BOSTON: CENGAGE LEARNING.

8. QODIROV, A. (2020). *AXBOROT XAVFSIZLIGI VA TARMOQ TEXNOLOGIYALARI*. TOSHKENT: O‘ZBEKISTON MILLIY UNIVERSITETI NASHRIYOTI.