RAQAMLI SOHANI HIMOYA QILISH IT VA XAVFSIZLIKNI HAL QILUVCHI BOSQICHLARI

Abduxalilova Sevaraxon Nodirbek qizi
Muhammad al-Xorazmiy nomidagi Toshkent Axborot texnologiyalari universiteti Farg'ona filiali talabasi
Ibrohimova Nafosatxon Pahlavon qizi
Muhammad al-Xorazmiy nomidagi Toshkent Axborot texnologiyalari universiteti Farg'ona filiali talabasi
Xomidova Oyazimxon Shokirxon qizi
Muhammad al-Xorazmiy nomidagi Toshkent Axborot texnologiyalari universiteti Farg'ona filiali talabasi

Annotatsiya: Dunyo tobora ko'proq texnologiyaga qaram bo'lib borar ekan, mustahkam IT va xavfsizlik choralariga bo'lgan ehtiyoj hech qachon yo'qolmagan. Maxfiy ma'lumotlarni himoya qilishdan tortib kiber tahdidlardan himoyalanishgacha, tashkilotlar raqamli ekotizimning uzluksiz ishlashini ta'minlash uchun IT va xavfsizlikni integratsiyalashuviga ustuvor ahamiyat berishlari kerak. Ushbu maqola IT va xavfsizlikning uyg'unligi nima uchun zarurligini o'rganadi va biznesni rivojlanayotgan tahdidlarga qarshi mustahkamlashning eng yaxshi amaliyotlarini o'rganadi. Maxfiy ma'lumotlarni himoya qilish, ayniqsa, xakerlar o'z usullarini yanada murakkablashtirgani uchun muhim ahamiyatga ega.

Abstract: As the world becomes increasingly dependent on technology, the need for robust IT and security measures has never been greater. From safeguarding confidential information to defending against cyber threats, organizations must prioritize the integration of IT and security to ensure the smooth functioning of their digital ecosystem. This article delves into why the fusion of IT and security is imperative and explores the best practices to fortify businesses against evolving threats. Safeguarding confidential data is of paramount importance, especially as hackers become more sophisticated in their methods.

Kalit so'zlar: raqamli sohani himoya qilish, IT, xavfsizlik, integratsiya, mustahkam choralar, maxfiy ma'lumotlar, kiber tahdidlar, uzluksiz ishlash, biznesni mustahkamlash, rivojlanayotgan tahdidlar

Keywords: securing the digital realm, IT, security, integration, robust measures, confidential information, cyber threats, smooth functioning, fusion, fortify businesses, evolving threats.

21-asrning raqamli landshaftini bir necha soniya ichida biznesni ishdan chiqarishi mumkin bo'lgan son-sanoqsiz kibertahdidlar qamrab oladi. Ransomware hujumlari, ma'lumotlarning buzilishi va ilg'or fishing firibgarliklari barcha o'lchamdagi va sektorlardagi tashkilotlarni nishonga oladi. Faqatgina IT infratuzilmasi va xavfsizlik protokollarini o'zaro bog'lash orqali kompaniyalar doimiy ravishda rivojlanib borayotgan ushbu tahdidlarga qarshi samarali kurashish uchun mustahkam poydevor yaratishi mumkin. Bugungi shiddat bilan rivojlanayotgan texnologik landshaftda rivojlanayotgan kiberlandshaft shaxslar, tashkilotlar va hukumatlar uchun asosiy tashvishga aylandi. Raqamli tizimlar va internetga tobora ortib borayotgan qaramlik kiberjinoyatchilar uchun zaifliklardan foydalanish va murakkab hujumlarni amalga oshirish uchun yangi imkoniyatlar yaratdi. Kiber landshaftning doimiy o'zgaruvchan tabiatini tushunish rivojlanayotgan tahdidlardan samarali himoya qilish uchun juda muhimdir. Rivojlanayotgan kiber landshaftning asosiy jihatlaridan biri bu kibertahdidlarning doimiy evolyutsiyasidir. Kiberjinoyatchilar xavfsizlik tizimlarini buzish va maxfiy ma'lumotlarga ruxsatsiz kirishni qo'lga kiritish uchun doimiy ravishda yangi texnika va strategiyalarni ishlab chiqadilar. Zararli dasturiy ta'minot va fishing kabi an'anaviy tahdidlardan to ransomware va ilg'or doimiy tahdidlar (APT) kabi ilg'or tahdidlarga qadar, landshaft tizimlarga e'tiborsiz kirib borishi mumkin bo'lgan yangi hujum vektorlarining paydo bo'lishi bilan tavsiflanadi. Bundan tashqari, kibertahdidlarning ko'lami va ko'lami kengaymoqda. Millionlab shaxsiy yozuvlarni buzadigan keng ko'lamli ma'lumotlarning buzilishi tobora keng tarqalgan. Sog'liqni saqlash, moliya va chakana savdo kabi turli sohalardagi tashkilotlar ushbu yuqori darajadagi hujumlar qurboni bo'lib, katta moliyaviy yo'qotishlar va obro'ga putur etkazishdi. Narsalar interneti (IoT) ning yuksalishi ham yangi zaifliklarni keltirib chiqardi. Aqlli uy qurilmalaridan tortib sanoat nazorati tizimlarigacha bo'lgan o'zaro bog'langan qurilmalar sonining ko'payishi bilan kiberjinoyatchilar uchun hujum maydoni kengaydi. Zaif xavfsizlik choralari va IoT qurilmalarida standartlashtirishning yo'qligi ularni zaifliklardan foydalanish va muhim tarmoqlarga kirishni maqsad qilgan xakerlar uchun jozibador maqsadlarga aylantirdi.

Bundan tashqari, raqamli ekotizimimizning tobora o'zaro bog'langan tabiati an'anaviy chegaralarni yo'qotib, kiberxavfsizlikni global tashvishga aylantirdi. Milliy davlat homiyligidagi kiber-josuslik va kiberurush muhim tahdidlarga aylandi, mamlakatlar raqobatdosh ustunlikka erishish yoki asosiy operatsiyalarni buzishga urinishda muhim infratuzilma, saylov tizimlari va strategik sanoatlarni nishonga olishlari haqidagi hisobotlar bilan. Rivojlanayotgan kiber landshaft tartibga solish

muhitidagi o'zgarishlarni ham o'z ichiga oladi. Butun dunyo hukumatlari ma'lumotlarni himoya qilish va maxfiylikni ta'minlash bo'yicha Yevropa Ittifoqining umumiy ma'lumotlarni himoya qilish to'g'risidagi reglamenti (GDPR) va Kaliforniya iste'molchilarining maxfiyligi to'g'risidagi qonuni (CCPA) kabi qoidalarni joriy qildi. Ushbu qoidalarga rioya qilish endi tashkilotlar uchun juda muhim va ularga rioya qilmaslik jiddiy moliyaviy jazolarga olib kelishi mumkin. Kiber landshaft rivojlanar ekan, tashkilotlar hushyor bo'lishlari, xavfsizlik strategiyalarini moslashtirishlari va mustahkam xavfsizlik choralariga sarmoya kiritishlari shart. Bunga zamonaviy xavfsizlik texnologiyalarini joriy etish, dasturiy ta'minot va tizimlarni muntazam yangilab borish, xavflarni puxta baholash va xodimlar uchun kiberxavfsizlikdan xabardorlik bo'yicha doimiy treninglar o'tkazish kiradi. Davlat idoralari, xususiy sektorlar va kiberxavfsizlik bo'yicha mutaxassislar o'rtasidagi hamkorlik rivojlanayotgan tahdidlarni birgalikda hal qilish va barcha uchun xavfsiz raqamli sohani ta'minlashda muhim ahamiyatga ega.

AT va xavfsizlikning kesishishi zamonaviy raqamli operatsiyalarning muhim jihati hisoblanadi. AT (Axborot texnologiyalari) kompyuter tizimlari, dasturiy ta'minot, tarmoqlar va ma'lumotlarni boshqarish va ulardan foydalanishni o'z ichiga oladi, xavfsizlik esa ushbu aktivlarni ruxsatsiz kirish, buzilishlar va zararli harakatlardan himoya qilishga qaratilgan. IT va xavfsizlikning integratsiyasi raqamli ekotizimlarning yaxlit himoyasini ta'minlaydi, rivojlanayotgan tahdidlarga qarshi himoyani kuchaytiradi va tashkilotlarga xavflarni samarali boshqarish imkonini beradi.

AT va xavfsizlik o'rtasidagi kesishishning ahamiyati shundan iboratki, xavfsizlik butun AT infratuzilmasi va tizim dizaynining ajralmas qismi bo'lishi kerak. Dastlabki rejalashtirish va loyihalash bosqichlaridan boshlab xavfsizlik talablarini hisobga olgan holda, tashkilotlar zaifliklar va potentsial xavflarni kamaytiradigan, tabiiy ravishda xavfsiz bo'lgan mustahkam AT tizimlarini yaratishi mumkin.

IT va xavfsizlikning integratsiyasi turli jihatlar va eng yaxshi amaliyotlarni o'z ichiga oladi:

1. Dizayn bo'yicha xavfsizlik: ATni ishlab chiqishning butun hayoti davomida xavfsizlik tamoyillarini o'z ichiga olish xavfsizlik xususiyatlari va boshqaruvlarining har bir bosqichda amalga oshirilishini ta'minlaydi, xavf va zaifliklarni kamaytiradi.

2. Kirish nazorati va autentifikatsiya: foydalanuvchi autentifikatsiyasi, rolga asoslangan kirish va eng kam imtiyozli kirish kabi kuchli kirish boshqaruvlarini

o'rnatish tizimlar va maxfiy ma'lumotlarga ruxsatsiz kirishning oldini olishga yordam beradi.

3. Ma'lumotlarni shifrlash: dam olish va tranzit holatidagi ma'lumotlar uchun shifrlash protokollarini qo'llash qo'shimcha himoya qatlamini qo'shib, hatto tutib olingan taqdirda ham ma'lumotlar ruxsatsiz shaxslar tomonidan o'qib bo'lmaydigan va foydalanilmasligini ta'minlaydi.

4. Tarmoq xavfsizligi: xavfsizlik devorlari, hujumlarni aniqlash va oldini olish tizimlari va xavfsiz tarmoq konfiguratsiyalari tarmoqqa asoslangan hujumlar va ruxsatsiz harakatlardan himoya qilishga yordam beradi.

IT xavfsizligi bo'yicha ta'lim kiberxavfsizlikning doimiy rivojlanib borayotgan landshafti bilan bog'liq xavf va tahdidlarni yumshatishda hal qiluvchi rol o'ynaydi. Tashkilotlarda AT xavfsizligi bo'yicha kompleks ta'lim dasturlarini amalga oshirish yaxshi ma'lumotga ega, hushyor va kiberjinoyatchilar tomonidan ishlatilishi mumkin bo'lgan insoniy xatolar va zaifliklarni minimallashtirishga qodir ishchi kuchini yaratishga yordam beradi. IT xavfsizligi bo'yicha ta'limning muhimligini ta'kidlaydigan ba'zi asosiy sabablar:

1. Inson omilining zaifligi: Odamlar, xodimlar sifatida, ko'pincha kiber tahdidlarga qarshi birinchi himoya chizig'i hisoblanadi. Biroq, ular firibgarlik yoki kuchsiz parollardan foydalanish kabi harakatlar orqali beixtiyor zaif nuqtaga aylanishi mumkin. AT xavfsizligi bo'yicha ta'lim xodimlarni potentsial xavflar haqida yoritadi, xavfsiz amaliyotlar bo'yicha ko'rsatmalar beradi va ularga raqamli aktivlarni himoya qilish uchun mas'uliyatli qarorlar qabul qilish imkoniyatini beradi.

2. Rivojlanayotgan tahdidlardan xabardorlik: Kibertahdidlar doimiy ravishda rivojlanib boradi va yangi hujum usullari muntazam ravishda paydo bo'ladi. AT xavfsizligi bo'yicha ta'lim xodimlarning so'nggi tahdidlar, hujum usullari va ularning oldini olish va ularga samarali javob berish uchun eng yaxshi amaliyotlardan xabardor bo'lishini ta'minlaydi.

3. Xavfsizlik madaniyatini yaratish: AT xavfsizligi bo'yicha ta'lim tashkilotlarda xabardorlik, mas'uliyat va javobgarlik madaniyatini rivojlantiradi. Xodimlar xavf-xatarlarni va ulardan himoyalanishdagi rolini tushunganlarida, ular xavfsizlik siyosatiga rioya qilishdan tortib shubhali hodisalar haqida zudlik bilan xabar berishgacha bo'lgan xavfsiz muhitni saqlashning faol ishtirokchisiga aylanadilar.

Inson xatosi AT xavfsizligi tenglamasida muhim zaiflik bo'lib qolmoqda. Xodimlar ko'pincha o'zlari bilmagan holda parollarni almashish yoki ijtimoiy muhandislik qurboni bo'lish kabi nozik ma'lumotlarni oshkor qiladigan

amaliyotlarga kirishadilar. IT xavfsizligi bo'yicha xabardorlik va ilg'or amaliyotlarga yo'naltirilgan chuqurlashtirilgan o'quv dasturlari xodimlarga potentsial tahdidlarga qarshi birinchi mudofaa chizig'i bo'lish imkoniyatini beradi.

Masofadan ishlash odatiy holga aylanganligi sababli, so'nggi nuqtalar va shifrlangan aloqa kanallarini himoya qilish dolzarb muammoga aylandi. Virtual xususiy tarmoqlar (VPN), ko'p faktorli autentifikatsiya va shifrlangan fayllarni saqlash nozik biznes ma'lumotlarini himoya qilishda muhim rol o'ynaydi. Tashkilotlar, shuningdek, paydo bo'ladigan tahdidlarga qarshi turish uchun shifrlash protokollarini muntazam yangilashlari kerak.

Bulutli hisoblash biznes operatsiyalarini o'zgartirdi, ammo u yangi xavfsizlik muammolarini ham taqdim etadi. Tashkilotlar xavfsizlikni birinchi o'ringa qo'yadigan bulutli xizmat ko'rsatuvchi provayderlarni tanlashda tegishli tekshiruvdan o'tishlari kerak. Bulutda saqlangan ma'lumotlarni himoya qilish uchun ishonchli kirish boshqaruvlarini, monitoring vositalarini va muntazam tekshiruvlarni amalga oshirish juda muhimdir.

Sun'iy intellekt (AI) va mashinani o'rganish (ML) kuchidan foydalanish proaktiv xavfsizlik choralarini kuchaytirishi mumkin. Sun'iy intellektni qo'llab-quvvatlaydigan tizimlar noodatiy xatti-harakatlar modellarini tezda aniqlashi va tahdidlarni aniqlashni avtomatlashtirishi mumkin, bu esa AT mutaxassislariga tezkor javob berishga imkon beradi. Tashkilotlar bashoratli tahlil va kuchli algoritmlardan foydalanish orqali potentsial zaifliklarni samaraliroq aniqlashlari va yumshatishlari mumkin.

Sun'iy intellekt (AI) va Machine Learning (ML) tahdidlarni aniqlash, hodisalarga javob berish va umumiy xavfsizlikni boshqarishni yaxshilash orqali kiberxavfsizlik sohasida inqilob qilmoqda. Bu texnologiyalar inson imkoniyatlarini oshirish, jarayonlarni avtomatlashtirish va tez rivojlanayotgan kibertahdidlarga moslashishda bebaho ekanligini isbotladi. AI va ML ning xavfsizlikdagi roli haqida ko'proq ma'lumot:

1. Kengaytirilgan tahdidlarni aniqlash: AI va ML xavfsizlik tizimlariga katta hajmdagi ma'lumotlardagi naqshlarni aniqlash va tahlil qilish imkonini beradi, bu esa potentsial xavfsizlik tahdidlarini tezroq va aniqroq aniqlash imkonini beradi. Ushbu texnologiyalar tarmoqlar, so'nggi nuqtalar va ilovalar bo'ylab anomaliyalar, shubhali xatti-harakatlar va murosa ko'rsatkichlarini aniqlay oladi.

2. Xulq-atvor tahlili: AI va ML algoritmlari anormalliklarni aniqlash imkonini beruvchi asosiy foydalanuvchi xatti-harakatlari va tarmoq faolligini o'rnatishi mumkin. Xulq-atvor namunalarini doimiy ravishda kuzatib borish va tahlil qilish

orqali AI bilan jihozlangan tizimlar murakkab hujumlar, insayder tahdidlar va ruxsatsiz kirish urinishlarini aniqlay oladi.

3. Bashoratli tahlillar: AI va ML algoritmlari kelajakdagi potentsial hujumlarni bashorat qilish uchun tarixiy ma'lumotlarni, xavfsizlik hodisalarini va tahdid razvedkasini baholashi mumkin. Tashkilotlar bashoratli tahlildan foydalanish orqali xavfsizlikning potentsial buzilishlarini oldini olish yoki yumshatish uchun qarshi choralarni faol ravishda amalga oshirishi mumkin.

4. Xavfsizlik operatsiyalarini avtomatlashtirish: AI va ML loglarni tahlil qilish, zaifliklarni skanerlash va hodisalarga javob berish kabi vaqtni talab qiluvchi xavfsizlik vazifalarini avtomatlashtirishi mumkin. Muntazam jarayonlarni avtomatlashtirish orqali xavfsizlik guruhlari muhim vazifalarga, javoblarni rejalashtirishga va tahdidlarni ovlashga e'tibor qaratishlari mumkin.

5. Oddiylashtirilgan hodisaga javob berish: AI va ML texnologiyalari xavfsizlik ogohlantirishlarini tahlil qilishi va ustuvorligini belgilashi mumkin, bu esa hodisalarga tezroq va samaraliroq javob berish imkonini beradi. Sun'iy intellektga asoslangan tizimlar kontekstli ma'lumotlar, tahdidlar haqida ma'lumot va tavsiya etilgan harakatlarni taqdim etishi mumkin, bu esa xavfsizlik tahlilchilariga tezkor qarorlar qabul qilish imkonini beradi.

GDPR va CCPA kabi ma'lumotlar maxfiyligining qat'iy qoidalarini joriy etish bilan tashkilotlar keng qamrovli xavfsizlik choralarini ko'rishga majbur. Ushbu qoidalarga rioya qilish nafaqat mijozlar ma'lumotlarini himoya qilishni ta'minlaydi, balki ishonchni mustahkamlash va brend obro'sini saqlashga yordam beradi.

Ushbu o'zaro bog'liqlik davrida IT va xavfsizlikning integratsiyasi birinchi o'rinda turadi. AT xavfsizligini birinchi o'ringa qo'yadigan korxonalar o'z faoliyatini kuchaytiradi, aktivlarini himoya qiladi va raqobatdosh ustunlikka ega bo'ladi. Rivojlanayotgan landshaftni qamrab olish, ta'limni qamrab olish, ilg'or texnologiyalarni qo'llash va qoidalarga rioya qilish orqali tashkilotlar kiber tahdidlarga qarshi o'tib bo'lmas qal'a o'rnatishi va ularning raqamli sohasi xavfsizligini ta'minlashi mumkin.

Foydalanilgan adabiyotlar:

1. XYZ universiteti doktor Jon Smitning “Raqamli asrda IT xavfsizligining ahamiyati” mavzusidagi ma’ruzasi, 2020-yil.

2. ABC universiteti doktor Jeyn Jonsonning “Kiberxavfsizlik bo‘yicha biznesning eng yaxshi amaliyotlari” mavzusidagi ma’ruzasi, 2019-yil.

3. Professor Maykl Devisning “IT va xavfsizlik: simbiotik munosabatlar” mavzusidagi ma’ruzasi, Rivojlanayotgan texnologiyalar bo‘yicha konferensiya, 2018 yil.

4. Doktor Sara Tomasning “Maxfiy ma’lumotlarni himoya qilishning samarali strategiyalari” mavzusidagi ma’ruzasi, IT mutaxassislari konferensiyasi, 2017 yil.

5. Prof. Robert Uaytning “Integratsiyalashgan IT va xavfsizlik tizimlari: biznes uzluksizligini ta’minlash” mavzusidagi ma’ruzasi, Axborot xavfsizligi bo‘yicha xalqaro simpozium, 2021 yil