DIGITAL BUSINESS MANAGEMENT
TOPIC 8: IOT INTERNET OF THINGS OPERATING TECHNOLOGIES IN DIGITAL BUSINESS MANAGEMENT AND ITS APPLICATION IN DEVELOPED COUNTRIES

Мавзу бўйича режа саволлари

1. Buyumlar Interneti haqida ma`lumot
2. Buyumlar Internetida xavfsizlik
3. Buyumlar Interetida xavfsizlik va maxfiylik ta`minlash bo`yicha tavsiyalar

Buyumlar Interneti haqida ma`lumot

IoT sog‘liqni saqlash va transport tizimlarini takomillashtirishdan tortib, uylarimiz va ish joyimizni yanada samarali va xavfsiz qilishgacha bo‘lgan hayotimizning ko‘p jabhalarida inqilob qilish imkoniyatiga ega

IoT ilovalariga ba'zi misollar: - Aqlli uylar: termostatlar, yoritish tizimlari va xavfsizlik kameralari kabi IoT qurilmalari masofadan boshqarilishi mumkin va foydalanuvchilarning vazifalarni avtomatlashtirish uchun afzalliklarini o'rganishi mumkin. Narsalar Interneti (IoT) tushunchasi bir necha o'n yillar davomida mavjud bo'lib kelgan, ammo bu atamaning o'zi faqat 1999 yilda Britaniyalik texnologiya kashshofi Kevin Eshton tomonidan kiritilgan. IoT-ning g'oyasi - kundalik ob'ektlarni internetga ulash, ularning bir-biri bilan va odamlar bilan muloqot qilish imkonini beradi. IoT ning dastlabki kunlari mashinadan mashinaga (M2M) aloqaga qaratilgan edi, bu erda qurilmalar ma'lumotlarni taqdim etish va jarayonlarni avtomatlashtirish uchun bir-biri bilan va markaziy serverlar bilan bog'lanadi. Ushbu texnologiya asosan ishlab chiqarish jarayonlarini kuzatish va nazorat qilish uchun fabrikalar va omborlar kabi sanoat sharoitlarida ishlatilgan.

2000-yillarning oxirida smartfonlarning ko'tarilishi va simsiz tarmoqlarning ko'payishi iste'molchilarga mo'ljallangan IoT qurilmalarining rivojlanishiga olib keldi. IoT qurilmalarining birinchi to'lqini aqlli termostatlar, uy xavfsizlik tizimlari va taqiladigan fitnes-trekerlarni o'z ichiga oldi. Ushbu qurilmalar vazifalarni avtomatlashtirish va real vaqt rejimida ma'lumotlarni taqdim etish orqali iste'molchilar hayotini oson va qulayroq qilish uchun mo'ljallangan.

So'nggi yillarda IoT texnologiyasi rivojlanishda va yangi sohalarga kengayishda davom etdi. Bluetooth Low Energy (BLE) va Zigbee kabi kam quvvatli simsiz tarmoqlarning rivojlanishi kichik, arzon narxlardagi IoT qurilmalarini yaratish imkonini berdi, ular ko‘p sonlarda joylashtirilishi mumkin. Bu aqlli shaharlarning paydo bo'lishiga olib keldi, bu erda sensorlar va boshqa IoT qurilmalari transport, havo sifati va boshqa atrof-muhit omillarini kuzatish uchun ishlatiladi.

IoT texnologiyasi sog'liqni saqlash, qishloq xo'jaligi va boshqa sohalarda samaradorlik va mahsuldorlikni oshirish uchun ham qo'llanilmoqda. Misol uchun, IoT sensorlari qishloq xo'jaligida ekinlarning o'sishi va tuproq namligini kuzatish

yoki sog'liqni saqlash sohasida bemorlarning sog'lig'i haqidagi ma'lumotlarni kuzatish uchun ishlatilishi mumkin. Umuman olganda, IoT tarixi texnologiyaning barqaror evolyutsiyasi va kundalik ob'ektlarni internetga ulashning potentsial afzalliklari haqida xabardorlikning ortib borishi bilan tavsiflanadi. IoT o'sishda va etuklashda davom etar ekan, u kelgusi yillarda yashash va ishlash tarzimizni shakllantirishda tobora muhim rol o'ynashi mumkin. IoT Xavfsizligi - bu sizning biznesingiz uchun xavfsizlikka xavf tug'dirishi mumkin bo'lgan bir qator qurilmalarning zaifliklarini tuzatishga yordam berish bilan birga, xavflarni himoya qilish, aniqlash va monitoring qilish orqali Internet qurilmalari va ular bog'langan tarmoqlarni tahdidlar va buzilishlardan himoya qilish harakatidir.

Buyumlar Internetida xavfsizlik

Buyumlar Interneti (IoT) xavfsizligi tushunchasi IoT qurilmalari, tarmoqlari va ma’lumotlarini ruxsatsiz kirish, o‘zgartirish, oshkor qilish va yo‘q qilishdan himoya qilish bo‘yicha ko‘riladigan chora-tadbirlarni anglatadi.

Xavfsizlik IoTda juda muhim masala, chunki bu qurilmalar ko'pincha sog'liqni saqlash, sanoat nazorati tizimlari va muhim infratuzilma kabi nozik muhitlarda o'rnatiladi, bu erda xavfsizlik buzilishi jiddiy oqibatlarga olib kelishi mumkin. IoT xavfsizligini ta'minlashda bir qancha qiyinchiliklar mavjud. Asosiy muammolardan biri shundaki, IoT qurilmalari ko'pincha cheklangan ishlov berish quvvatiga va xotiraga ega bo'lib, murakkab xavfsizlik choralarini amalga oshirishni qiyinlashtiradi.

IoT xavfsizligi odatda apparat va dasturiy ta'minotga asoslangan chora-tadbirlarning kombinatsiyasini o'z ichiga oladi. IoT xavfsizligini tarmoqqa ulangan jismoniy IoT qurilmalariga qaratilgan kiberhujumlar ehtimolidan himoya qiluvchi kiberxavfsizlik strategiyasi va himoya mexanizmi sifatida tushunish mumkin. Kuchli xavfsizlik bo'lmasa, ulangan har qanday IoT qurilmasi oxir-oqibat infiltratsiya qilish, foydalanuvchi ma'lumotlarini o'g'irlash va tizimlarni buzish uchun yomon aktyor tomonidan buzish, murosaga kelish va nazorat qilish uchun zaifdir

IoT xavfsizligining asosiy muammosi shundaki, katta hajmdagi turli xil IoT qurilmalari tarmoqqa ulanishda davom etar ekan, parallel ravishda hujum yuzasi keskin kengaymoqda. Oxir-oqibat, butun tarmoq xavfsizligi holati eng kam xavfsiz qurilmaga taqdim etiladigan yaxlitlik va himoya darajasiga kamayadi. Inventarizatsiya - tarmoqdagi IoT qurilmalari va yangi qurilmalarni qanday xavfsiz boshqarish haqida aniq ko'rinish va kontekstga ega emas.

Tahdidlar - tuzatish qiyin yoki imkonsiz bo'lgan IoT qurilmalari operatsion tizimlarida yaxshi o'rnatilgan xavfsizlikning yo'qligi.

Ma'lumotlar hajmi - boshqariladigan va boshqarilmaydigan IoT qurilmalaridan yaratilgan katta hajmdagi ma'lumotlarni nazorat qilish.

Egalik - tashkilot ichidagi turli guruhlar tomonidan IoT qurilmalarini boshqarish bilan bog'liq yangi xavflar.

Xilma-xillik - cheksiz shakllari va funktsiyalari nuqtai nazaridan IoT qurilmalarining xilma-xilligi.

Operatsiyalar - birlashma inqirozi, bunda IoT qurilmalari asosiy operatsiyalar uchun juda muhim, ammo AT uchun asosiy xavfsizlik holatiga integratsiyalashuvi qiyin. IoT qurilmalariga tez-tez uchraydigan hujumlardan ba'zilari tarmoqni skanerlash, masofaviy kodni bajarish, buyruqlar kiritish va boshqalar kabi usullardan foydalangan holda amalga oshiriladigan ekspluatatsiyalardir. Hujumlarning 41 foizi qurilma zaifliklaridan foydalanadi, chunki IT orqali hujumlar ma’lum zaif tomonlardan foydalanish maqsadida tarmoqqa ulangan qurilmalar orqali skanerdan o‘tkazadi. Birinchi qurilmani buzgandan so'ng, boshqa zaif qurilmalarga kirish va ularni birma-bir buzish uchun lateral harakat ochiladi. Vaqti-vaqti bilan sinovdan o'tgan zamonaviy IT-ga asoslangan zararli dasturlarning oldini olish uchun eskirgan deb hisoblangan ushbu hujum taktikalaridan ba'zilarini qo'llashdan tashqari, tengdoshlar orasidagi buyruq va boshqaruv (C2) aloqasi va o'z-o'zidan tarqaladigan IoT zararli dasturlari qurtlari IoTda paydo bo'ladigan ikkita yangi hujum taktikasidir. xavfsizlik gorizonti. IoT qurtlari, aslida, IoT botnetlariga qaraganda keng tarqalgan. Ikkala taktika ham korxonadagi muhim biznes operatsiyalarini buzish uchun o'nlab yillar davomida saqlanib qolgan OT protokollariga qaratilgan. Buyumlar internetida maxfiylik (IoT) shaxsiy ma'lumotlarning himoyasi va bu ma'lumotlarning IoT qurilmalari va tizimlari kontekstida qanday to'planishi, ishlatilishi va almashishini nazorat qilish huquqini anglatadi.

IoT qurilmalari odatda atrof-muhit va ular bilan aloqada bo'lgan odamlar haqida ma'lumot to'playdigan sensorlar va boshqa texnologiyalar bilan jihozlangan. Bu ma’lumotlar biometrik ma’lumotlar, joylashuv ma’lumotlari va xatti-harakatlar namunalari kabi shaxsiy ma’lumotlarni o‘z ichiga olishi mumkin. Ushbu ma'lumotlarni to'plash va ulardan foydalanish, ayniqsa, agar u shaxsning bilimi yoki roziligisiz to'plangan bo'lsa yoki u shaxsning niyatidan boshqa maqsadlarda foydalanilsa, maxfiylik bilan bog'liq muammolarni keltirib chiqarishi mumkin.

Ushbu xavotirlarni bartaraf etish uchun IoT-da maxfiylikni himoya qilish uchun turli choralar ko'rish mumkin. Misol uchun, IoT qurilmalari o'z vazifasini bajarish uchun zarur bo'lgan minimal miqdordagi ma'lumotlarni to'plash uchun mo'ljallangan bo'lishi mumkin va ma'lumotlar ruxsatsiz kirishning oldini olish uchun anonimlashtirilishi yoki shifrlanishi mumkin. Shuningdek, foydalanuvchilarga o'z ma'lumotlari ustidan ko'proq nazorat berilishi mumkin, masalan, ma'lumotlar to'plashdan voz kechish yoki undan voz kechish, o'z ma'lumotlariga kirish va ularni o'chirish imkoniyati.

Umumiy ma'lumotlarni himoya qilish to'g'risidagi reglament (GDPR) va Kaliforniya iste'molchilarining maxfiyligi to'g'risidagi qonun (CCPA) kabi maxfiylik qoidalari, shuningdek, ma'lumotlarni to'plash, foydalanish va oshkor qilish standartlarini belgilash va shaxslarga huquqlar berish orqali IoTda maxfiylikni himoya qilishda muhim rol o'ynaydi. shaxsiy ma'lumotlariga kirish,

nazorat qilish va o'chirish. Buyumlar interneti (IoT) turli darajadagi xavfsizlik imkoniyatlariga ega ulangan qurilmalarning ko‘pligi tufayli yangi xavfsizlik muammolarini keltirib chiqardi. IoT uchun xavfsizlik tahdidlarining ba'zilari quyidagilarni o'z ichiga oladi:

1. Zaif parollar: Ko'pgina IoT qurilmalari taxmin qilish yoki buzish oson bo'lgan standart parollar bilan birga keladi, bu ularni shafqatsiz kuch hujumlariga qarshi himoyasiz qiladi.

2. Zararli dasturiy ta'minot va viruslar: IoT qurilmalari ularning xavfsizligini buzishi va tajovuzkorlarga maxfiy ma'lumotlarga kirishiga imkon beradigan zararli dasturlar yoki viruslar bilan zararlangan bo'lishi mumkin.

3. Xavfsiz aloqa: Ko'pgina IoT qurilmalari shifrlanmagan kanallar orqali muloqot qiladi, ular tajovuzkorlar tomonidan tutib olinishi va maxfiy ma'lumotlarni o'g'irlash uchun ishlatilishi mumkin. 4. Xizmatni rad etish hujumlari: tajovuzkorlar IoT qurilmalariga xizmat ko‘rsatishni rad etish hujumlarini amalga oshirishi mumkin, bu esa ularni trafik bilan to‘ldirishi va ularni yaroqsiz holga keltirishi mumkin.

5. Jismoniy hujumlar: IoT qurilmalariga jismoniy kirish va manipulyatsiya qilish mumkin, bu tajovuzkorlarga nozik ma'lumotlarni olish, qurilma sozlamalarini o'zgartirish yoki zararli dasturlarni o'rnatish imkonini beradi.

6. Xavfsizlik yangilanishlarining yo'qligi: Ko'pgina IoT qurilmalari xavfsizlik yangilanishlarini qabul qilish uchun mo'ljallanmagan, bu ularni vaqt o'tishi bilan paydo bo'ladigan yangi tahdidlarga qarshi himoyasiz qoldiradi. Ushbu tahdidlarni bartaraf etish uchun shifrlash, ko'p faktorli autentifikatsiya va muntazam xavfsizlik yangilanishlari kabi kuchli xavfsizlik choralarini qo'llash muhimdir. Har bir Iot qurilmasini sozlang

Ko'pgina yangi IoT qurilmalari har kuni bozorga chiqariladi. Masalan, aqlli soat yoki aqlli uy jihozlari. Siz ularni sotib olishingiz va ishlatishingiz mumkin.Odamlar orasida keng tarqalgan tendentsiya - bu ularni yaxshi sozlangan va qutidan chiqarishdan darhol foydalanish uchun xavfsiz deb o'ylash. Lekin ularni hech qanday xavf yoki xavfsizlik yoki maxfiylikni buzish xavfi yo'qligiga ishonch hosil qilish uchun sozlash muhimdir. IoT qurilmalari haqida bilib oling

Bozordan yangi "Internet of Things" qurilmasini sotib olganingizda, siz ulardan kundalik foydalanish uchun qanday foydalanishni o'rganasiz va bundan boshqa hech narsa bo'lmaydi. Bu ideal emas.Yangi qurilma va uning sozlamalari, konfiguratsiyasi, noyob xususiyatlari, qayta o'rnatish yoki qayta sozlash, ko'p qatlamli xavfsizlikni qo'shish imkoniyatlari va boshqalar haqida iloji boricha ko'proq ma'lumot olishga harakat qiling. Bunga qo'shimcha ravishda, tarmoqqa ulangan barcha qurilmalarni muntazam kuzatib boring. Qurilmalaringizni yangilab turing

Aksariyat IoT qurilmalari dasturiy ta'minot va proshivka yangilanishlarini o'z vaqtida oladi. Ushbu yangilanishlar xatolar yoki boshqa xavfsizlik bo'shliqlarini tuzatishni o'z ichiga oladi. Qurilma internetga ulanganda avtomatik

yangilanish xususiyatiga ega yoki yo'qligini ishlab chiqaruvchidan tekshiring.Agar bunday bo'lmasa, uni qo'lda yangilashingiz kerak bo'ladi. Agar qurilma standart parol bilan ta'minlansa, uni o'zingiz tanlagan yagona parolga o'zgartiring. IoT qurilmalarining standart parollari kiberjinoyatchilar uchun oson taxmindir. . Agar qurilmangiz bir nechta funksiyalarga ega bo‘lsa va sizga ularning barchasi kerak bo‘lmasa, faqat o‘zingiz foydalanadigan funksiyalarni yoqing va yo‘qlarini o‘chiring. Buning o'zi sizni xavfsizlik tahdidlarining yukidan qutqarishi mumkin.. O'zingizga tegishli IoT qurilmalari uchun hech qachon umumiy Wi-Fi tarmog'idan foydalanmang. Umumiy Wi-Fi-dan bir necha daqiqa yoki soat foydalangandan so'ng, siz xuddi shu qurilmalarni uy tarmog'ingizga ulaysiz. Bu vaziyat yomonlashganda.Qurilmalaringizga jamoat joylaridan kirgan troyanlar yoki zararli dasturlar osongina uy tarmog'ingizga o'tib, maxfiyligingizga jiddiy tahdid soladi. Umumiy Wi-Fi tarmog'idan foydalanish yaxshi fikr emasligining sababi shundaki, ularning yangilanishiga kafolat yo'q. Agar siz umuman umumiy tarmoqdan foydalanishingiz kerak bo'lsa, buni ishonchli VPN (Virtual Private Network) yordamida amalga oshirganingizga ishonch hosil qiling.

Адабиётлар ва интернет сайтлари:

Адабиётлар ва интернет сайтлари:

1. Радченко И., Николаев И., Технологии и инфраструктура Big data: Учебное пособие. – Санк-петербург: ИТМО, 2018.
2. Маркова В.Д.. Цифровая экономика. Учебник. :М.-“ИНФРА-М” 2019.- 186 стр..
3. Цифровая трансформация бизнеса: Изменение бизнес-модели для организации нового поколения / Питер Вайл, Стефани Ворнер ; Пер. с англ. — М. : Альпина Паблишер, 2019. — 257 с.
4. Интернет вещей. Новая технологическая революция / М. Кранц — «Эксмо», 2017. (Top Business Awards) ISBN 978-5-04-090627-7.
5. https://data-flair.training/blogs/hadoop-ecosystem-components/
6. Big Data от А до Я. Часть 1: Принципы работы с большими данными, парадигма MapReduce. https://habr.com/ru/post/267361/
7. Big Data от А до Я. Часть 2: Hadoop. https://habr.com/ru/company/dca/blog/268277
8. Akaev A.A., KenjabaevA.T., Ilxamova Yo.S., Jumaniyozova M.Yu. Iqtisodiyotda axborot komplekslari va texnologiyalari. Darslik.T.-“Fan va texnologiya”. 2019.- 510 bet.
9. Kenjabaev A.T., Ikramov M.M., Allanazarov A.A.. Axborot-kommunikatsiya texnologiyalari. O‘quv-qo‘llanma.T.-“O‘zbekitson faylasuflari milliy jamiyati nashriyoti”. 2017.- 408 bet.

10. Цифровая экономика: Учебник / Авторы-составители: Л. А. Каргина, С. Л. Лебедева [и др.]; под ред. Л. А. Каргиной. — М.: Прометей, 2020. — 222 с.
11. Lapidus L. sifrovaya ekonomika. Upravlenie elektronnыm biznesom i elektronnoy kommersiey. Uchebnik. M.: INFRA-M, 2019.- 348 str.
12. Технологии четвертой промышленной революции: [перевод с английского] / Клаус Шваб, Николас Девис. Москва: Эксмо,2022.-320с.