KIBERXAVFSIZLIK ASOSLARI.

Eshonqulov Samandar Qo‘chqorboy o‘g‘li
Hamdamov Lazizjon Ikromjon o‘g‘li
Jonibekov Ibrohim Erkin o‘g‘li
Bobolov Jahongir Qodir o‘g‘li
eshonqulov182@gmail.com
lazizjonhamdamov856@gmail.com
ibrohimjonibekov74@gmail.com
bobolovjahongir@gmail.com
Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universitetining Jizzax filiali axborot tizimlari va texnologiyalari yonalishi talabalari

Annotatsiya: Ushbu maqolamizda kiberxavfsizlik asoslari mavzusida bo‘lib, u quyidagilar haqida ma’lumotlar berib o‘tiladi. Kiberxavfsizlikning asosiy tushunchalari, kiberxavfsizlikning asosiy terminalogiyalari, kiberxujumlar, kiberxvsizlik bo‘yicha amaliyotlar, kibertahditlar tarixi, kiberxavfsizlik sertifikatlari va umumiy xulosa qismlaridan iborat.

Kalit so‘zlar: Kiberxavfsizlik, kibertahditlar, dasturiy taminot, maxfiylik, butunlik, mvjudlik, intrusionlar va hujumlar, protokol, internet protokoli, Virtual Private Network (VPN), Faervol, Domen nomlari serveri (DNS), shifrlash, deshifrlash, virus, autentifikatsiya, xaker.

Kiberxavfsizlikning to‘rtta asosiy qismi mavjud.

1. Qurilmani himoya qilish.

Kiber tahdidlarning kuchayishi bilan jismoniy shaxslar va kompaniyalar qurilmalarni himoya qilishga jiddiy ahamiyat berishlari kerak. Antivirus dasturlari yordamida internetga ulanadigan qurilmalarni himoya qilish, bloklash va o‘chirish

imkoniyatlarini yoqish, ikki faktorli autentifikatsiyani faollashtirish va tizim dasturiy ta'minotini muntazam ravishda avtomatik yangilashni amalga oshirish kerak. Ushbu qurilmalarda ya’ni noutbuklar, shaxsiy kompyuterlar, mobil telefonlar, sun'iy intellektga asoslangan qurilmalar (aqlli soatlar va boshqalar), iPad'lar, va internetga ulanadigan har qanday qurilmalarda yuqoridagilardan foydalanish kerak boladi. Qurilmani himoya qilish joylashuvidan qat'iy nazar, shaxslar va ularning qurilmalariga hujum qilish xavfini sezilarli darajada kamaytiradi.

2. Onlayn ulanishni ta'minlash.

Shaxsiy qurilma onlayn ulangandan so‘ng, internet orqali uzatiladigan ma'lumotlar ko‘proq himoya qilishni talab qiladi. Bundan tashqari, VPN-lardan foydalanish kerak. Virtual xususiy tarmoqlar ular internet-trafikni avtomatik ravishda shifrlaydi. VPN-dan foydalangan holda, barcha onlayn tranzaktsiyalar, jumladan, foydalanuvchi identifikatori, joylashuvi, brauzer ma'lumotlari va parollar va bank rekvizitlari kabi har qanday nozik ma'lumotlar himoyalangan bo‘ladi.

3. Elektron pochta aloqasini himoya qilish.

Kiberjinoyatchilar ko‘pincha jismoniy shaxslar yoki kompaniyalar haqida nozik ma'lumotlarni to‘plash uchun elektron pochtadan foydalanadilar. Maxfiy ma'lumotlarga mo‘ljallangan oluvchidan boshqa hech kim kirishiga yo‘l qo‘ymaslik uchun elektron pochta xabarlarini shifrlash tavsiya etiladi, chunki ular asl ma'lumotni yashiradi. Bundan tashqari, elektron pochtani shifrlash ko‘pincha bir martalik parolni autentifikatsiya qilishni o‘z ichiga oladi.

4. Fayllar va hujjatlarning zaxira nusxalarini o‘z vaqtida himoya qilish va amalga oshirish.

Zaxira nusxalari ikki toifaga bo‘linadi: masofaviy zaxiralash (oflayn) va bulutli saqlash (onlayn). Yechimlar o‘zlarining afzalliklari va kamchiliklari bilan farqlanadi. Masofaviy zaxiralash xizmatlari qulay va arzon, ammo unga istalgan joydan kirish oson emas. Shu bilan bir qatorda, bulutli echimlarga istalgan joydan kirish mumkin va ular turli joylardan ishlaydigan tashkilot uchun mos keladi. Biroq, muhim hujjatlar shifrlash

kodlari bilan o‘zlarining raqamli omboriga ega bo‘lishi kerak, chunki Internetga ulangan har qanday narsa kiber tahdid xavfiga ega. Biroq, kiber tahdidlar internetga ulangan har qanday narsaga ta'sir qilishi mumkin. Ma'lumotlar bazasi va infratuzilma xavfsizligini boshqarish tizimi bilan bulutli hisoblash yechimi kuchli tarmoq xavfsizligi, ilovalar xavfsizligi va bulut xavfsizligi bilan yuqori darajada xavfsizdir. Bundan tashqari, kuchli mobil xavfsizlik bulutli hisoblash xavfsizligini oshiradi. BCDR rejasini amalga oshirish orqali tashkilot tabiiy ofatlar, elektr ta'minotidagi uzilishlar, jamoa a'zolarining beparvoligi, apparatdagi nosozlik va kiberhujumlar kabi kutilmagan bulut xavfsizligi holatlaridan tezda tiklanishi mumkin, bu esa odatdagi operatsiyalarni qisqa vaqt ichida qayta tiklashga imkon beradi. Bundan tashqari, identifikatsiyani boshqarish tizimlari so‘nggi nuqta xavfsizligi va ma'lumotlar xavfsizligini eng yuqori darajada ta'minlaydi.

Kiberxavfsizlikning asosiy tushunchasi.

Kiberxavfsizlik texnologiyalar, jarayonlar va boshqaruv vositalaridan foydalangan holda tizimlar, tarmoqlar, dasturlar, qurilmalar va ma’lumotlarni kiberhujumlardan himoya qilishni nazarda tutadi. Kiberxavfsizlikning asosiy tushunchalari kiberhujum xavfini kamaytirish va tizimlar, tarmoqlar va texnologiyalarga ruxsatsiz kirishning oldini olishni o‘z ichiga oladi.

A. Kiberxavfsizlikning uchta tushunchasi

Kiberxavfsizlikning asoslari Markaziy razvedka boshqarmasi triadasida yotadi , ular:

- Maxfiylik
- Butunlik
- Mavjudligi

B. Kiberxavfsizlikning birlamchi asosiy tushunchalari

- Tahdidni aniqlash
- Axborotni xavfsiz saqlash
- Intrusionlar va hujumlarni aniqlash
- Bosqinlar va hujumlarga javob bering.

•Buzg'unchilikdan himoya qilishni qayta tiklang va ma'lumotlar bazasi xavfsizligini tiklang.

Kiberxavfsizlikning asosiy terminologiyalari

Yangi boshlanuvchilar uchun kiberxavfsizlik asoslari ushbu atamalarni o‘z ichiga olishi kerak. Kiberxavfsizlik asoslari terminologiyasini bilish yuqori texnologiyali dunyoni yaxshiroq tushunishga yordam beradi. Biroq, kiberxavfsizlikdagi texnologik yutuqlar yangi jargonlarning paydo bo‘lishi bilan birga keladi.

1. Internet protokoli (IP) manzili

Tarmoqdagi apparat qurilmalari IP-manzillar (Internet Protocol manzillari) orqali aniqlanadi. Mahalliy tarmoq yoki internet orqali ushbu qurilmalar bir-biri bilan aloqa o‘rnatishi va ma'lumotlarni uzatishi mumkin. Har bir manzilda raqamlar nuqtalar bilan ajratilgan. U 0 dan 255 gacha bo‘lgan to‘rtta raqamdan iborat. IP manzili quyidagicha ko‘rinishda bo‘lishi mumkin: 192.159.1.98 Internet-kompyuterlar, marshrutizatorlar va veb-saytlar identifikatsiya qilish uchun milliardlab noyob IP-manzillarga muhtoj, chunki ularni takrorlash mumkin emas. IPv6 yangi protokol bo‘lib, kelajakda tizimda noyob manzillar tugashi bilan kunlik ehtiyojlarni qondirish uchun mo‘ljallangan.

2. VPN - Virtual Private Network

Ommabop VPN nomi bilan tanilgan Virtual Private Network foydalanuvchilarga internetni kezish paytida o‘zlarining maxfiyligi va anonimligini saqlash imkonini beradi. VPN-lar Internet protokoli (IP) manzilini maskalash orqali onlayn faoliyatni deyarli kuzatib bo‘lmaydi. Xavfsiz Wi-Fi ulanish nuqtalariga qaraganda ko‘proq maxfiylikni ta'minlashdan tashqari, VPN xizmatlari xavfsiz va yuqori darajada shifrlangan ulanishlarni o‘rnatadi. VPN yordamida onlayn faoliyat kiberjinoyatchilar, korxonalar, hukumatlar va foydalanuvchilarni anonim havolalarni bosishga jalb qiladigan boshqa snooperlardan yashiringan.

3. Faervol

Xavfsizlik devori kompaniyaning xavfsizlik siyosatiga muvofiq tizimning kiruvchi va chiquvchi tarmoq trafigini kuzatib boradi va filtrlaydi. Faervollar xususiy ichki tarmoq

va uning asosiy darajasidagi Internet o‘rtasidagi to‘siqdir. Xavfsizlik devori halokatli ko‘rinadigan virtual trafikni bloklaydi va xavfsiz va xavfli bo‘lmagan trafikning uzluksiz oqishiga imkon beradi.

4. Domen nomlari serveri (DNS)

DNS - Domen nomi serveri internetning virtual telefon kitobi sifatida ishlaydi. Internetdagi har bir brauzer foydalanuvchilarga qurilmaning joylashuvini aniqlash imkonini beruvchi IP manzili bilan tanilganligi sababli, DNS domen nomini IP manziliga aylantiradi. Masalan, DNS www.mycompany123.com manzilini 204.0.6.42 raqamli IP manziliga o‘zgartiradi. Brauzerlar ma'lumotlarni DNS serverlari tomonidan topilgan IP-manzil yordamida kontentni yetkazib berish tarmog'idagi (CDN) kelib chiqish serverlariga yuboradilar.

5. Shifrlash va deshifrlash

Shifrlash - bu shifrlangan matn deb nomlanuvchi shifrlash algoritmi yordamida oddiy matnni (o‘qilishi mumkin bo‘lgan xabarni) kodlarga aylantirish jarayoni. Shu bilan birga, shifrni ochish shifrlangan matnni oddiy matnga aylantirish jarayonidir.

6. Shifrlash kaliti

Shifrlangan ma'lumotlar shifrlash kaliti yordamida shifrlangan va paroldan chiqariladi. Kalitlar noyob va takrorlash uchun murakkab, chunki ular maxsus shifrlash kodlari bilan bog'langan.

Kiberhujumlarning umumiy turlari

Bugun dunyo turli kiberhujumlar bilan qiynalmoqda. Biroq, agar biz kiberhujum turlarini bilsak, bizning tarmoqlarimiz va tizimlarimiz yaxshiroq himoyalangan. Kiberhujumlarning eng keng tarqalgan besh turi:

1. Zararli dastur hujumi

- **Virus**: Virus tarmoqdagi barcha fayllarni yuqtirishi mumkin bo‘lgan zararli dastur turi bo‘lib, uni yo‘q qilish eng qiyin turlaridan biri hisoblanadi. Kompyuter virusi o‘zining zararli kodini boshqa dasturlarga kiritish orqali o‘zini ko‘paytirishi mumkin.
- **Qurt**: butun tarmoqni tezda yuqtirish uchun kuchga ega bo‘ling va oxirgi

foydalanuvchining ishtirokini talab qilmaydi, chunki qurtlar o‘z-o‘zidan ko‘payishi mumkin.

•**Troyan**: aniqlash uchun eng qiyin zararli dasturlardan biri bu troyan zararli dasturidir, chunki u o‘zini qonuniy dastur sifatida yashiradi. Jabrlanuvchi zararli kod va ko‘rsatmalarni bajarishi bilanoq, zararli dastur mustaqil ravishda ishlashi mumkin. U ko‘pincha zararli dasturlarning boshqa shakllari uchun kirish nuqtasi sifatida ishlatiladi.

•**Reklama dasturi**: Yakuniy foydalanuvchilarga reklama dasturlari tomonidan keraksiz reklama (masalan, kontakt qalqib chiquvchi oynalar) taqdim etiladi.

•**Josuslarga qarshi dastur**: Ushbu turdagi zararli dastur oxirgi foydalanuvchidan shubhalanmasdan foydalanuvchi identifikatorlari va parollar kabi nozik ma'lumotlarni to‘playdi.

•**Ransomware**: Tizimga zarar etkazadigan, fayllarni shifrlaydigan va jabrlanuvchi to‘lovni to‘lamaguncha shifrlash kalitini ushlab turuvchi zararli dastur hujumining eng xavfli turlaridan biri sifatida tanilgan. To‘lov asosan P2P tarmog'iga ega kriptovalyuta shaklida bo‘ladi. Tashkilotlar borgan sari ko‘proq to‘lov dasturlari hujumiga uchramoqda, bu esa hayotiy muhim tizimlarni tiklash uchun millionlab pul sarflaydi, chunki ular tajovuzkorlarga ularni tiklash uchun pul to‘laydi. Bir nechta ransomware oilalari mavjud, ammo CryptoLocker, Petya va Locky eng mashhurlari.

2. Parol hujumi

Parol hujumlari ko‘pincha ma'lumotlarning buzilishiga olib keladi. Foydalanuvchi hisoblariga kirish uchun xaker autentifikatsiyani chetlab o‘tishga harakat qiladi.

3. Fishing hujumi

Xaker fishing hujumlari orqali foydalanuvchi ma'lumotlarini, jumladan, login ma'lumotlari, bank hisobi ma'lumotlari va kredit karta raqamlarini o‘g'irlashi mumkin. Hujumchilar ishonchli shaxslardan kelgan elektron pochta, tezkor xabarlar yoki matnli xabarlarni ochish uchun qurbonlarni aldash uchun niqoblardan foydalanadilar. Qabul qiluvchi zararli havolani bosgandan so‘ng, maxfiy ma'lumotlar ochiladi va zararli dastur o‘rnatiladi.

4. Clickjacking

Clickjackingda tajovuzkor odatda foydalanuvchini jalb qilish uchun onlayn reklamadan foydalanadi. Ular foydalanuvchini tizimga zararli dasturlarni o‘rnatuvchi boshqa sahifaga ochiladigan tugmalar yoki havolalarni bosish uchun aldamoqda. Adobe Flash plaginlari sozlamalari sahifasi klik qilishning eng shov-shuvli misollaridan biridir. Ushbu sahifa ko‘rinmas iframe-ga yuklanishi va tajovuzkorga Flash-dagi xavfsizlik sozlamalarini o‘zgartirishi mumkin, bu esa kompyuterning mikrofoni va kamerasidan Flash animatsiyalari tomonidan masofadan foydalanish imkonini beradi.

5. Kriptovalyutani o‘g'irlash

Kriptovalyutani o‘g'irlash yangi kiber-hujum bo‘lib, u kriptovalyuta keng joriy etilgandan so‘ng keskin o‘sdi. Hujumchilar boshqa birovning kompyuterida kriptovalyutani qazib olish uchun kriptojackingdan foydalanadilar. Hujum paytida tajovuzkor foydalanuvchining kompyuteriga uning tizimiga zarar etkazish yoki zararli havolalarni bosish uchun manipulyatsiya qilish orqali kirish huquqiga ega bo‘ladi. Ko‘pgina hollarda, foydalanuvchilar buni bilishmaydi, chunki Crypto Mining kodi fonda ishlaydi va nimadir noto‘g'ri ekanligini ko‘rsatadigan yagona ko‘rsatkich - bu ijro etilishdagi kechikish.

Kiberxavfsizlik bo‘yicha eng yaxshi amaliyotlar

Kiberhujumlar qiyin bo‘lishi mumkin va doimiy ravishda xavfsizlik xatarlarini fosh qilishning innovatsion usullarini izlayotgan kiberjinoyatchilarga ergashish juda qiyin. Biroq, ba'zi yo‘llar bilan kiberhujumlarning oldini olish mumkin:

1. Dasturiy ta'minotni muntazam ravishda yangilab turish

Oddiy dasturiy ta'minot yangilanishi yangilangan xususiyatlar, xatolarni tuzatish va xavfsizlik yangilanishlarini o‘z ichiga oladi. Xavfsizligingizni ta'minlash uchun dasturiy ta'minotni eng so‘nggi versiyasiga yangilash har doim yaxshi fikrdir.

2. Kompyuterning viruslar va zararli dasturlardan himoyalanganligiga ishonch hosil qilish

Internetga ulangan ekansiz, zararli dasturlardan butunlay himoyalana olmaysiz.

Agar siz virusga qarshi dastur va kamida bitta anti-malware dasturini o‘rnatsangiz, kompyuteringizning zaifligi sezilarli darajada kamayadi.

3. 2 faktorli autentifikatsiyani sozlang

Bundan tashqari, veb-xavfsizlik ikki faktorli autentifikatsiya orqali mustahkamlanadi, chunki u buzilgan parol xavfini darhol yo‘q qiladi. Hisoblaringizni xavfsiz saqlash uchun ikki faktorli autentifikatsiya endi bir nechta platformalarda mavjud.

4. VPN orqali ulanishlaringizni himoya qiling

Xavfsizroq veb uchun virtual xususiy tarmoqdan (VPN) foydalaning. Hatto internet provayderingiz ham sizning maxfiy ma'lumotlaringizni ko‘ra olmaydi, chunki VPN ulanishni shifrlaydi.

5. Havolalarni bosishda ehtiyot bo‘lish

Har safar tasodifiy giperhavola xabarlarini bosganingizda, ularning qonuniyligini ikki marta tekshirib ko‘ring, chunki havolalar ular bo‘lmagan narsa sifatida osongina maskalanishi mumkin.

6. Foydalanilmayotganda Bluetooth o‘chirilganligiga ishonch hosil qiling

Qurilmangiz yoqilgan bo‘lsa, xakerlar shaxsiy ma'lumotlaringizni Bluetooth orqali o‘g'irlashi mumkin. Agar siz Bluetooth-dan foydalanmasangiz, uni o‘chirib qo‘ying.

7. Kompyuteringizdagi reklama dasturlarini o‘chiring

Siz haqingizda ma'lumot to‘plagani uchun reklama dasturi orqali ko‘proq maqsadli reklamalarni olasiz. Maxfiyligingizni saqlab qolish uchun kompyuteringizni reklama dasturlarisiz saqlang va reklama blokerini o‘rnating.

8. Xavfsizlik tizimini yangilang

Yaxshi xavfsizlik tizimiga va ular mavjud bo‘lganda yangilanishlarga sarmoya kiritganingizga ishonch hosil qiling. Yuqori darajadagi xavfsizlikka sarmoya kiritish xavfsizlikni buzish uchun katta miqdorda to‘lashdan yaxshiroqdir.

9. Viruslarni skanerlash tashqi xotira qurilmalari

Ichki xotira qurilmalaridan tashqari, tashqi xotira qurilmalari ham zararli dasturlarga duch kelishi mumkin. Infektsiyalangan tashqi qurilmalar, agar siz ularni ulasangiz, zararli

dasturlarni kompyuteringizga tarqatishi mumkin. Shuning uchun, tashqi qurilmalarga kirishdan oldin, ular zararli dasturlardan xoli ekanligiga ishonch hosil qilish uchun qurilmani skanerlang.

10. Muhim ma'lumotlarning zaxiralanganligiga ishonch hosil qiling

Maxfiy ma'lumotlar xavfsizlik buzilishi natijasida yo‘qolishi mumkin. Yo‘qotilgan taqdirda ularni qayta tiklashga tayyor ekanligingizni ta'minlash uchun muhim ma'lumotlaringizni bulutga yoki mahalliy saqlash qurilmasiga tez-tez zaxiralab turish tavsiya etiladi. Bundan tashqari, maxfiy fayllarni parol bilan himoyalangan tizim bilan saqlashingizga ishonch hosil qiling.

Kibertahdidlar tarixi.

Kiber tahdidlarning notinch tarixi mavjud. Texnologiya cheklangan davrda kiberhujumni amalga oshirish juda qiyin edi. Faqat bir nechta odam tarmoqqa ulanmagan ulkan elektron mashinalarni qanday boshqarishni bilar edi, shuning uchun uni buzib bo‘lmaydi. Jon fon Neyman 1945 yilda dastur ko‘rsatmalarini ma'lumotlar bilan bir xil xotirada saqlashni taklif qildi. Saqlangan dasturlar kompyuterlarga qayta dasturlash va olish-dekodlash-bajarish siklini (FDE) bajarishni osonlashtirdi. Ushbu g'oya ko‘pincha "Von Neumann" arxitekturasi deb ataladi. 1950-yillarning oxirida telefon freaking - telefon protokollarini o‘g'irlash, buning natijasida "freaks" bepul qo‘ng'iroqlarni amalga oshirish va shaharlararo qo‘ng'iroqlar uchun pul to‘lamaslik uchun telekommunikatsiya muhandisligiga murojaat qilmasdan tarmoqda masofadan ishlashga imkon berdi. Afsuski, telefon kompaniyalari cheklangan manbalar tufayli freakslarni nazorat qila olmadilar va oxir-oqibat 1980-yillarda telefon freaklari yo‘qoldi. 1979 yilda Kevin Mitnik Ark kompyuteridan foydalangan holda Digital Equipment Corporation tomonidan ishlab chiqilgan operatsion tizimlarning nusxalarini yaratdi. Keyingi o‘n yilliklarda u hibsga olinishi va qamoqqa olinishiga sabab bo‘lgan bir nechta kiberhujumlarni amalga oshirdi. Hozirda u Mitnick Security Consulting kompaniyasining bosh direktori va asoschisi sifatida ishlaydi. Ushbu soha juda boy tarixga ega bo‘lgani uchun, odamlar so‘nggi o‘zgarishlardan xavotirda bo‘lishlari ajablanarli emas, chunki xakerlar tobora mustahkam

bo‘lgan xavfsizlik dasturlariga osongina kirib borishi mumkin.

Nima uchun kiberxavfsizlik juda muhim?

Kiberxavfsizlik shiddat bilan rivojlanayotgan soha bo‘lib, u doimiy ravishda kompaniyalar, davlat idoralari va jismoniy shaxslar uchun yangi muammolarni keltirib chiqaradi. Ba'zilar kiberxavfsizlik kompyuterlarni viruslarga qarshi dasturlar yoki boshqa xavfsizlik dasturlari yordamida viruslar va boshqa turdagi zararli dasturlardan himoya qilishni anglatadi, deb taxmin qilishlari mumkin, ammo bu mavzuning faqat bir tomoni.

Ma'lumotlar buzilishi va kiberhujumlar har qachongidan ham tez-tez uchraydi. Ular endi katta resurslarga va murakkab axborot xavfsizligi amaliyotiga ega yirik korporatsiyalar bilan cheklanib qolmaydi. Bugungi kunda kichik korxonalar va onlayn bozor saytlari yoki boshqa elektron tijorat xizmatlarini ishlatadiganlar ham xavf ostida.

Tashkilot tarmog'iga kirishi, maxfiy ma'lumotlarni o‘g'irlashi, zarar etkazishi va daromadning yo‘qolishiga olib kelishi va aktivlarini himoya qilmagani uchun jarimaga tortilishi uchun kompyuter yoki mobil qurilmaga kirish huquqiga ega bo‘lgan bir buzuq foydalanuvchi kerak bo‘ladi. Ular, shuningdek, kompaniyalarni javobgarlik xavfiga duchor qilishlari mumkin. Shunday qilib, har bir tashkilot axborot xavfsizligi asoslarini va nima uchun bu ularning biznesi uchun muhimligini tushunishi kerak. Bulutli hisoblashning ajoyib mavjudligi, shuningdek, uni ko‘plab kompaniyalar uchun mashhur tanlovga aylantiradi, ular istalgan joyda, istalgan vaqtda va istalgan joydan ma'lumotlarga kirishlari mumkin. Biroq, bulutli hisoblash bilan bog'liq ba'zi xavflar mavjud, masalan, jamoat mulki bo‘lgan bir nechta xizmatlar mavjud va uchinchi tomonlar ushbu xizmatlarga kirishlari mumkin. Shu sababli, xakerlar ushbu xizmatlarni osongina buzishi mumkin. Bundan tashqari, bulutli hisoblash ham hisobni o‘g'irlashning jiddiy xavfsizlik xavfini keltirib chiqaradi. Elektron pochta, bank, ijtimoiy media va boshqalar kabi bulutli hisoblardagi ma'lumotlar parol bilan himoyalanmagan bo‘lsa, u zaif bo‘lib qoladi va xakerlar ruxsatsiz harakatlarni amalga oshirish uchun ularga kirishlari mumkin.

Kiberxavfsizlik sertifikatlari

Kompyuter fanlari bo‘yicha bakalavr darajasiga ega bo‘lishdan tashqari,

kiberxavfsizlik bo‘yicha mutaxassislarning aksariyati o‘zlarining ilg'or tajribalar bo‘yicha bilimlarini tasdiqlovchi sertifikatlarga ega bo‘lishlari kerak. Kiberxavfsizlik bo‘yicha yuzlab sertifikatlar kirish darajasidan yuqori darajaga qadar mavjud. Shuning uchun, sizga pul va vaqt sarflashdan oldin sizga raqobatdosh ustunlik beradigan sertifikatni topish juda muhimdir.

Quyida sanoatdagi eng yaxshi amaliyotlarni taklif qiluvchi eng yaxshi uchta kiberxavfsizlik sertifikatlari keltirilgan:

1. Axborot tizimlari xavfsizligi bo‘yicha sertifikatlangan mutaxassis (CISSP)

Shubhasiz, CISSP sertifikati kiberxavfsizlik sohasidagi professional tashkilot (ISC)2 tomonidan berilgan kiberxavfsizlik sohasida eng ko‘p talab qilinadigan sertifikatlardan biridir. CISSP sertifikati sizning IT xavfsizligi haqida bilimdonligingizni va kiberxavfsizlik dasturlarini loyihalash, amalga oshirish, monitoring qilish va qo‘llab-quvvatlashga qodir ekanligingizni ko‘rsatadi.

2. ISACA CSX Kiberxavfsizlik asoslari sertifikati

ISACA kiberxavfsizlik asoslari sertifikati bilan shaxslar ilg'or texnologiyalarni o‘rganishlari va o‘zlarining eng yaxshi ko‘nikmalarini rivojlantirishlari mumkin. Bundan tashqari, kurs CSX ning ishlashga asoslangan sertifikatlash va sertifikat dasturlari orqali real hayotiy ko‘nikmalar va tajribalarni namoyish qilish imkonini beradi. CISM (Sertifikatlangan Axborot xavfsizligi menejeri) va CISA (Sertifikatlangan Axborot Tizimlari Auditori) ilg'or hisob ma'lumotlariga oraliq daraja beradi va xavfsizlik sohasida uzoq muddatli ISACA sertifikatlari qatoriga kiradi.

3. Sertifikatlangan axloqiy xaker (CEH)

Bu zararli o‘yinchilardan oldin zaifliklarni topish uchun tashkilotlarni qonuniy ravishda buzishni o‘z ichiga oladi, bu axloqiy xakerlik deb nomlanuvchi amaliyot, shuningdek oq qalpoqli xakerlik, penetratsiya testi yoki qizil jamoalar sifatida ham tanilgan. EC-Kengashi ushbu sertifikatni CEH dasturining bir qismi sifatida taklif qiladi. Eng yaxshi axloqiy xakerlik sertifikati kursini o‘rganing va siz kirish testini o‘tkazish, aniqlash, vektor qilish va hujumlarning oldini olish qobiliyatingizni namoyish eta olasiz.

Xulosa

Barcha o‘lchamdagi korxonalar tez rivojlanayotgan soha bo‘lgan kiberxavfsizlikdan tobora ko‘proq tashvishlanmoqda. Kiberhujumlar ilmiy-fantastik filmlardek tuyulishi mumkin bo‘lsa-da, haqiqat shundaki, ular odatiy holga aylanib bormoqda. Bundan tashqari, keyingi bir necha yil ichida kiber jinoyatlar ko‘payadi. Kiberxavfsizlikning buzilishi har qanday joyda sodir bo‘lishi mumkin. Kiberxavfsizlik zamonaviy dunyoning ajralmas qismiga aylandi. Shaxsiy, moliyaviy va korporativ ma’lumotlarning xavfsizligi bizning kelajagimiz uchun muhim ahamiyatga ega. Shu sababli har bir foydalanuvchi va tashkilot o‘z ma’lumotlarini himoya qilish uchun kiberxavfsizlik qoidalariga rioya qilishi kerak. Internetni xavfsiz va ishonchli foydalanish orqali biz zamonaviy texnologiyalarning foydali tomonlaridan unumli foydalanamiz va kiberjinoyatchilikka qarshi barqaror tizimlarni yaratamiz.

Foydalanilgan adabiyotlar.

1. "Cybersecurity and Cyberwar: What Everyone Needs to Know" - P.W. Singer va Allan Friedman
2. "Cybersecurity Essentials" - Charles J. Brooks, Christopher Grow, Philip Craig.
3. "The Importance of Cybersecurity in the Modern Age" - Journal of Cybersecurity (odamlar uchun ommaviy jurnal)
4. "Understanding Cyber Threats: An Overview" - IEEE Xplore Digital Library.
5. National Institute of Standards and Technology (NIST) - nvlpubs.nist.gov (kiberxavfsizlikka oid me'yorlar)
6. Cybersecurity & Infrastructure Security Agency (CISA) - cisa.gov (kiber tahdidlar va xavfsizlik strategiyalari haqida ma'lumot).
7. IBM Cyber Security Intelligence Index - ibm.com (kiber xavfsizlik statistikasi).