Kiberhavsizlik yo'nalishi

Ichki Ishlar Vazirligi

Namangan akademik litseyi

informatika va AT fani o'qituvchisi

Ismanova Marg'uba Numonovnaning

ANNOTATSIYA: *Ushbu maqola kiberxavsizlik va uning yo'nalishlari xususida so'z yuritiladi.*

Kalit so'zlar: *kiberxavfsizlik, kompyuter, axborot texnologiyalari, xavf.*

KIRISH

Kiberxavfsizlik nima? Ba'zilarimiz bu atamani ilgari eshitganmiz, lekin ba'zilarimiz bu nimani anglatishini yoki nima uchun bunday deb atalishini bilmasligimiz mumkin. Shunday qilib, kiberxavfsizlikning ma'nosini to'liq tushunish uchun keling, so'zni ikki qismga ajratamiz: "kiber" va "xavfsizlik".

Kiber va xavfsizlik nima?

" Kiber " atamasi odatda kompyuterlar, axborot texnologiyalari yoki internet bilan bog'liq narsalarni anglatadi. Buni yaxshiroq tushunish uchun uni kompyuterlar va internetga tegishli maxsus so'z sifatida tasavvur qiling .

Xavfsizlik – bu xavf yoki tahdiddan xoli bo'lish va xavfsiz bo'lish holatini anglatadi.

Shunday qilib, agar ikkita so'zni birlashtirsak, "kiberxavfsizlik" kompyuterlarni, tarmoqlarni va internetga ulangan har qanday qurilmani har qanday xavf yoki tahdiddan xavfsiz saqlashni anglatadi.

Nima uchun kiberxavfsizlik muhim? Kiberxavfsizlik bizning davrimizda, ayniqsa sodir bo'layotgan barcha texnologik yutuqlar bilan chambarchas bog'langan. O'z resurslarini ularni xohlaydigan boshqa mamlakatlardan himoya qilish uchun hech qanday armiyasi yo'q mamlakatni tasavvur qiling. Mamlakat zaif bo'lishi shubhasiz, to'g'rimi? Siz shunday mamlakatda yashashni xohlarmidingiz?

Siz hozir deyarli har kuni o'qish va ish uchun foydalanayotgan texnologiya va internet bilan ham xuddi shunday; kiberxavfsizlik bo'lmasa, sizning shaxsiy ma'lumotlaringiz, joylashuvingiz, fotosuratlaringiz, kamerangiz va boshqa ko'p narsalaringiz himoyalanmagan bo'lardi va natijada, bu sizning shaxsiy hayotingiz haqidagi muhim ma'lumotlarni jinoyatchilar uchun tayyor o'ljaga aylantiradi. Agar jinoyatchilar bunday ma'lumotlarga kirish imkoniga ega bo'lsa, ular sizning kredit kartalaringizdan foydalanishi, pulingizni o'g'irlashi va hatto shaxsni o'g'irlashi mumkin.

Yana bir misol, agar sizda kompyuterlar va ma'lumotlarga tayanadigan shaxsiy biznesingiz bor va siz ushbu kompaniyani qurish uchun juda ko'p mehnat qildingiz. Ammo kiberxavfsizlik bo'lmasa, kompaniyangiz biznesdan chiqib ketishi va bir kechada barcha pul, ma'lumotlar va obro'sini yo'qotishi mumkin.

Yuqorida kiberxavfsizlik nima uchun muhim ekanligiga ikkita misol keltirdik. Ammo bugungi virtual hayotimizda bunga juda ko'plab misollar keltirishimiz mumkin. Umuman olganda, biz kiberxavfsizlikni internetning harbiy qismi deb o'ylashimiz mumkin.

Kiberxavfsizlik sohasiga kirish uchun dasturlashni bilish kerakmi?

Siz endigina kiberxavfsizlik sohasiga qadam qo'yayotganingizda dasturlash ilmini mukammal tarzda bilishingiz zarur emas. Ammo keyinchalik bu soha bilan astoydil shug'ullanishni boshlasangiz, sizga albatta dasturlashni o'rganish hamda bilish talab etiladi. Chunki shunday murakkab kiber jinoyatlar mavjudki, ularning oldini olish yoki qarshi turish uchun siz professional dasturchi bo'lishingiz shart.

Kiberxavfsizlik bo'yicha karyerangizni va kelajagingizni rivojlantirishni istaysizmi, lekin uning hayotimizdagi ko'lami va kelajakdagi ahamiyati haqida tasavvurga ega emasmisiz? Unda ushbu maqola aynan siz uchun. Kiberxavfsizlikni bugun va kelajak kasblaridan bo'ladi deb aytishimiz mumkin. Business Insider India ma'lumotlariga ko'ra, birgina Hindistonda 2025-yilga kelib kiberxavfsizlik bo'yicha 3,5 million bo'sh ish o'rinlari bo'ladi.

Ko'pchilik kiberxavfsizlikning kelajagi bilan qiziqadi. Kiberxavfsizlik hali ham IT ning nisbatan yoshroq sohasi bo'lib, so'nggi yillarda IT xavfsizligi bo'yicha

alohida kasb sifatida sezilarli darajada rivojlandi. Ushbu maqolada biz axborot xavfsizligi, xususan, kiberxavfsizlik sohasidagi joriy o'zgarishlarni ko'rib chiqamiz va kiberxavfsizlikning kelajagi qanday ekanligini taxmin qilishga harakat qilamiz.

Kiberxavfsizlik nima?

Kiberxavfsizlik internetga ulangan tizimlarni, jumladan qurilma, dasturiy ta'minot va ma'lumotlarni kiberhujumlardan himoya qilishni anglatadi. Bunda, asosan, tahdidlarni va zaifliklarni kamaytirish, xalqaro hamkorlik va kompyuter tarmog'i operatsiyalari, axborotni ta'minlash va huquqni muhofaza qilish kabi harakatlarni qamrab olish uchun hamkorlik qiladigan odamlar, jarayonlar va texnologiyalar tushiniladi. Bu tarmoqlar, qurilmalar, dasturlar va ma'lumotlarga hujumlar, o'g'irlik, zarar, modifikatsiya yoki ruxsatsiz kirishning oldini olishga qaratilgan texnologiyalar, usullar va amaliyotlar to'plamidir.

Kiberhujumlar global muammoga aylanmoqda. Bu jahon iqtisodiyotiga tahdid solishi mumkin bo'lgan ko'plab qo'rquvlarni keltirib chiqardi. Kompaniyalar va tashkilotlar, xususan, milliy xavfsizlik, sog'liqni saqlash yoki moliyaviy ma'lumotlar bilan bog'liq ma'lumotlar bilan shug'ullanuvchilar o'zlarining maxfiy biznes va shaxsiy ma'lumotlarini kiberhujumlardan himoya qilish uchun harakat qilishlariga zarurat tug'ilmoqda. Kompyuterlar, tarmoqlar, ilovalar va ma'lumotlar xavfsizligini ta'minlash uchun samarali kiberxavfsizlik strategiyasida bir nechta himoya qatlamlari qo'llaniladi. Kibertahdidlarga qarshi muvaffaqiyatli mudofaani yo'lga qo'yish uchun tashkilot xodimlari, jarayonlari va texnologiyasi bir-birini qo'llab-quvvatlashi va to'ldirishi kerak bo'ladi.

Kiberxavfsizlik kelajagida ortib borayotgan kiberhujumlar

Jismoniy shaxs yoki tashkilot qasddan va yovuz niyatda boshqa shaxs yoki tashkilotning axborot tizimiga kirishga urinsa, bu kiberhujum deb ataladi. Aksariyat hujumlar iqtisodiy maqsadga ega bo'lsa-da, hozirda amalga oshirilayotgan bir nechta operatsiyalar maqsad sifatida ma'lumotlarni yo'q qilishni o'z ichiga olmoqda. Yomon niyatli shaxslar ko'pincha to'lov yoki boshqa moliyaviy daromad olish usullarini izlaydilar, ammo hujumlar turli sabablarga ko'ra amalga oshirilishi mumkin, jumladan, siyosiy harakatlar.

Kiberxurujlar kelajakda kiberxavfsizlikda hal qilinishi kerak bo'lgan asosiy masala bo'ladi.

1. Kelajakda Clouds (Bulutlar) hujum ostida bo'lishi mumkin

Ommaviy bulutli domenlarning ommaviyligi ortib borayotgani platforma resurslari va muhim ma'lumotlarga qaratilgan kiberhujumlarning ko'payishiga olib keldi. 2018-yilda bo'lgani kabi, bulutli resurslarning noto'g'ri konfiguratsiyasi va noto'g'ri boshqarilishi 2019-yilda ham bulutli ekotizim uchun eng xavfli bo'lib qoldi. Natijada, ta'sirlangan bulutli aktivlar keng doiradagi hujumlarga duchor bo'ldi. Bulutli infratuzilmalarni noto'g'ri sozlash joriy yilda butun dunyo bo'ylab korxonalar zarar ko'rgan ko'plab ma'lumotlarni o'g'irlash hodisalari va hujumlarining asosiy sabablaridan biri bo'ldi.

Docker xostlari fosh qilindi va raqobatchilarning bulutga asoslangan kripto qazib olish faoliyati to'xtatildi. Check Point tadqiqotchilarining fikricha, ommaviy bulut infratuzilmalariga qarshi ekspluatatsiyalar soni ham oshgan.

2. Kiberxavfsizlik kelajagidagi fishing kiberhujumlari

Fishing – bu kiberhujumning keng tarqalgan usuli bo'lib, kelajakda ham kiberxavfsizlikning eng jiddiy xavflaridan biri bo'lib qolmoqda. Elektron pochta xavfsizligi mexanizmlari ilg'or darajadagi ijtimoiy muhandislikdan qochish taktikasi tomonidan zarar ko'rmoqda. CheckPoint tahlilchilariga ko'ra, tovlamachilik sxemalari va biznes elektron pochta kelishuvi (BEC) ko'payib bormoqda, ular qurbonlarni shantaj bilan tahdid qilish yoki to'lovni olish uchun boshqalarga taqlid qilish orqali tahdid qilmoqda. Ikkala firibgarlik ham har doim ham zararli qo'shimchalar yoki havolalarni o'z ichiga olmaydi, bu esa ularni aniqlashni qiyinlashtiradi. Bir marotaba qandaydir harakatlar Markaziy razvedka boshqarmasi sifatida namoyon bo'ldi va qurbonlarni aprel oyida bolalar haqidagi ba'zi noqonuniy videolarni tarqatish va saqlashda gumon qilinganligi haqida ogohlantirdi. Bir guruh xakerlar esa Bitcoin uchun 10 000 dollar talab qilishdi.

3. Kiberxavfsizlik kelajagida mobil qurilmalarga hujumlar kuchaymoqda

Kiberhujumchilar mobil dunyoga tahdid landshaftining umumiy modellari va usullarini joriy qilmoqdalar. 2018-yil bilan solishtirganda, banklarga oid zararli

dasturlar mobil kiber arenaga muvaffaqiyatli kirib keldi va ularning keskin o'sishi 50% dan oshdi. Jabrlanuvchilarning bank hisoblaridagi to'lov ma'lumotlari, hisob ma'lumotlari va mablag'larini o'g'irlashi mumkin bo'lgan zararli dastur keng tahdidlar muhitidan chiqarib yuborildi va banklarning mobil ilovalaridan ko'proq foydalanish natijasida ayniqsa keng tarqalgan mobil tahdidga aylandi.

4. Kiberxavfsizlik kelajagida ransomware hujumlarining kuchayishi

Ransomware so'nggi yillarda ancha mashhur bo'ldi. Kichik mahalliy va shtat hukumat idoralari, birinchi navbatda, AQShning janubi-sharqida nishonga olingan. Bulutli hisoblash, bulutga asoslangan obuna xizmatlari va mobil qurilmalarning tez tarqalishi an'anaviy tarmoq perimetrlarini zaiflashtirmoqda. Vektorlar soni ortib borishi bilan kompaniyalarga hujum qilish usullari ham ortadi. Oxirgi 3 oy davomida to'plangan ma'lumotlarga ko'ra, to'lovga qarshi hujumlar soni 39 foizga oshgan. Dunyo COVID-19 hujumidan tiklanayotganda, hujumchilar vaziyatdan foydalanib, halokatli hujumni boshlashdi. Kelajakda kiberxavfsizlik bo'yicha ba'zi davlatlarda sog'liqni saqlash sohasiga hujumlar bo'lishi taxmin qilinmoqda.

Kiberxavfsizlik va karyera kelajagi

Mutaxassislarning fikricha, kiberxavfsizlikning kelajagi 2025-yilga borib 170 milliard dollarlik sektorgacha o'sadi. So'nggi besh yil davomida kiberxavfsizlik bo'yicha mutaxassislar o'rtacha IT-mutaxassisdan ko'proq pul ishlab topdilar. Farq bo'yicha o'rtacha daromad nomutanosibligi 9% ni tashkil qiladi. Mavjud ish o'rinlari soni ortib borayotgan va ish haqi yaxshilanayotgan bo'lsa-da, malakalar bo'shlig'ini yopish uchun ko'proq vaqt talab etiladi. Kiberxavfsizlik va ta'lim markazi ma'lumotlariga ko'ra, agar kiberxavfsizlik bo'yicha ish izlovchilar malaka oshirishni boshlamasa, 2025-yilga borib sektorda 1,8 million kiberxavfsizlik bo'yicha mutaxassis yetishmaydi.

Kiberjinoyatlarning kun sayin ortib borishi bilan bu kasbga talab ham oshadi. Bu qiyin, ammo juda foydali ishga aylanadi. Kiberxavfsizlikning qiyinchiliklari kundan-kunga kengayib, rivojlanib borayotganligi sababli, kiberxavfsizlik bo'yicha malakali mutaxassislarga butun dunyo bo'ylab talab katta. Kiberjinoyatchilarning tobora takomillashgan strategiyalari firmalarga zarar yetkazishda davom etar ekan,

kiberxavfsizlik barcha turdagi korxonalar uchun ortib borayotgan tashvishga aylanib bormoqda. Gartner ma'lumotlariga ko'ra, firmalar 2025-yilda xavfsizlikka 123 milliard dollardan ortiq mablag' sarflaydi, 2022-yilda bu ko'rsatkich 170,4 milliard dollarga yetishi kutilgandi.

Ushbu sohadagi ajoyib iste'dodlar uchun kompaniyalar 1,5 dan 4 milliongacha pul to'lashga tayyor. Har bir kompaniya o'z ma'lumotlarini himoya qilish uchun kiberxavfsizlik bo'yicha mutaxassislarga muhtoj bo'lganligi sababli, deyarli har bir sohada son-sanoqsiz ish o'rinlari mavjud bo'ladi. Kiberxavfsizlik bo'yicha mutaxassislar o'z tashkiloti ma'lumotlarining xavfsizligini ta'minlash uchun mas'uldirlar. So'nggi yillarda IT-sanoati ko'plab mamlakatlar iqtisodiy farovonligiga katta hissa qo'shdi.

Talab qilinadigan ko'nikmalar

Birinchi va eng muhim talab – bu sohaga kuchli qiziqish. Kiberxavfsizlik bo'yicha lavozimlarga nomzodlar kuchli qiziqish hissi va unga nisbatan kuchli ishtahaga ega bo'lishi kerak. Kiber tahdid landshafti doimo o'zgarib turadi, shuning uchun agar siz ushbu sohada yangi bo'lsangiz, o'rganishni davom ettirishga va kuch sarflashga tayyor bo'lishingiz kerak. Quyida yangi boshlovchilar muvaffaqiyatli kiberxavfsizlik karyerasini boshlashlari kerak bo'lgan kiberxavfsizlik ko'nikmalari keltirilgan:

Tarmoqqa ulanish

Tarmoq – bu bizning ro'yxatimizdagi dastlabki kiberxavfsizlik mahoratidir. Kompyuter tarmoqlarda muntazam tranzaksiyalar va aloqa xavfsizlikni talab qiladi. Kundalik faoliyatida korxonalar turli tarmoqlardan foydalanadilar. Lokal tarmoqlarni (LAN), keng maydon tarmoqlarini (WAN) va virtual xususiy tarmoqlarni (VPN) boshqarish uchun qanday sozlashni o'rganish juda muhimdir.

Kodlash

Kodlash – bu dasturiy ta'minot yaratish uchun ishlatiladigan kompyuter dasturlash tili. HTML va Javascript kabi tillarda kodlashning asosiy tushunchalarini tushunish ularning kiberhujumlarga nisbatan zaifligini yaxshiroq tushunishga yordam beradi.

Tizimlar va ilovalar

Dasturiy ta’minot va tizimlarni bilish kiberxavfsizlikning yana bir muhim mahoratidir. Kompyuter dasturlari va boshqa ilovalar kompaniyaning muhim vositalari bo’lganligi sababli, ular haqida hamma narsani tushunish zarurdir. Agar siz qanday qilib ishga tushirishni va ma’lumotlar bazalari va veb-serverlarni saqlashni o’rgansangiz, zaifliklarni aniqlash orqali ilovalar xavfsizligini yaxshilashga tayyor bo’lasiz.

Turli sohalarda IT bilimlari

Texnologiyaning asosini tashkil etuvchi tizimlar va jarayonlarni tushunish uchun IT haqida o’rganish kerak. Aqlli kiberxavfsizlik bo’yicha mutaxassis baxtsiz hodisalar qanday sodir bo’lishini va ularni qanday qilib oldini olishni biladi.

Tizimlar

Tizimlarni yaxshi tushunish yana bir muhim kiberxavfsizlik mahoratidir. Umumiy operatsion tizimlarning o’ziga xos xususiyatlarini o’rganing va mobil tizimlar haqida hamma narsani bilish uchun Linux Terminal yoki Windows Power shell kabi buyruq qatori interfeyslari bilan tanishing.

Texnologik innovatsiyalar

Biz kiberhujumchilarni yoqtirmaymiz, lekin ularga bitta narsani berishimiz kerak: haqiqiy innovator ruhi. Biz o’zimizni himoya qilishga tayyor bo’lishimiz uchun yangi texnologiya va ularning rivojlanishidan xabardor bo’lishimiz kerak. Kiberxavfsizlik innovatsiyalari tijorat tarmoqlariga zararli hujumlardan himoyalanish uchun yangi asoslarni qurmoqda. Kovid inqirozi davrida yangi ish muhitlarining qabul qilinishi kiberxavfsizlikning ahamiyatini avvalgidan ham ko’proq ta’kidladi. Mavjud ssenariy raqamli transformatsiya tezligi va innovatsion texnologiyalarning rivojlanishi bilan yomonlashdi, bu esa rekord miqdordagi kiberhujumlarga olib keldi. Har bir zaiflikdan tajovuzkorlar foydalanadi.

Kiberxavfsizlik innovatsiyalari ushbu sohada muhim yutuqlarni keltirib chiqardi. Biz raqamli imkoniyatlarga ega kelajak sari intilayotganimiz sababli, kiberxavfsizlik bo‘yicha mutaxassislar tasavvurga ega bo‘lishlari va yangi g‘oyalarni hayotga tatbiq etishlari muhim.

Kiberxavfsizlik kelajagidagi ish o’rinlari va imkoniyatlar

Kelajakda kiberxavfsizlik bo’yicha ish imkoniyatlari juda ajoyibdir. Bu haqida o’ylab ko’rsangiz, kiberxavfsizlik bo’yicha bandlikning o’rtachadan yuqori o’sishi juda mantiqiy bo’ladi. Texnologiya har bir insonning kundalik hayotiga tobora ko’proq kirib borar ekan, kiberxavfsizlik bo’yicha professional mutaxassislarga talab ortib boradi. Kiberxavfsizlik maoshlari ham yuqori va kundan-kunga ortib bormoqda. Kelajakda kiberxavfsizlik bo’yicha ish bilan ta’minlash bo’yicha hisob-kitoblar ko’proq imkoniyatlarni ko’rsatsa-da, haqiqat shuki, hozir bu sohada ishlash uchun yetarli malakali mutaxassislar yo’q. Malakali kadrlar tanqisligi tufayli kiberxavfsizlik bo’yicha kasbni tanlaganlar ko’plab imkoniyatlar, yaxshi daromad va ajoyib imtiyozlarni kutishlari mumkin, chunki kiberxavfsizlikning kelajagi porloq.

FOYDALANILGAN MANBA:

https://www.datatrained.com/post/future.