“KIBERXAVFSIZLIKNING ZAMONAVIY TAHDIDLARI”

Surxondaryo Viloyati Termish shahar Termiz

Iqtisodiyot va Servis unverseteti Axborot tizimlari va texnologiyalari

(tarmoqlar va sohalar bo'yicha) 2-bosqich talabasi

Sa'dullayeva Sevinch Sa'dullo qizi

Annotatsiya: *Ushbu maqolada kiberxavfsizlik sohasidagi zamonaviy muammolar, kiberjinoyat turlari va axborot xavfsizligini ta'minlash usullari muhokama qilinadi.*

Kalit so‘zlar: *kiberxavfsizlik, kiberjinoyat, kiberetika , bulutli hisoblash, axborot xavfsizligi.*

Tadqiqotlar shuni ko'rsatadiki, o'rtacha tashkilotda 800 dan ortiq bulut ilovalari mavjud bo'lib, ularning aksariyati biznesga tayyor emas. Oxirgi ikki yil ichida bu o‘rtacha ko‘rsatkich o‘sishda davom etmoqda. Aksariyat tashkilotlar bu faktni 80–90 foiz deb baholamoqda. Mavjud muhit haqida aniqroq tasavvurga ega bo'lish uchun ko'pchilik tashkilotlarning birinchi qadami Shadow IT havfini baholashdan iborat. Tashkilotda aniqlangan eng xavfli ilovalarga kirish orqali IT ma'murlari kompaniya uchun umumiy xavfni kamaytirishi mumkin. Bu aniqlash uchun qo'shimcha foydalanish tahlilini talab qiladi.

Ushbu qo'shimcha tushuncha qatlami bilan IT tashkilotlari xavfni kamaytirish strategiyalarini ishlab chiqishi mumkin, masalan, alohida foydalanuvchilar yoki bo'limlarga muqobil ilovalarni topishga o'rgatish yoki eng xavfli ilovalarga kirishni cheklash siyosatini qo'llash lozim. Topilgan ilovalarning biznesga tayyorligini aniqlash uchun tashkilotlar ushbu ilovalar kompaniyaning xavfsizlik siyosati, muvofiqlik siyosati yoki boshqa korporativ talablarni hisobga

olgan holda foydalanishga mos kelishini bilishi kerak. Ushbu tushunchalar yordamida tashkilotlar qaysi ilovalarni sanktsiyalash, qaysilariga ruxsat berish va nazorat qilish va qaysi birini butunlay blokirovka qilish haqida ongli qarorlar qabul qilishlari mumkin.

Korxonalar raqamli transformatsiya (RT) tashabbuslarini tezlashtirar ekan, operatsiyalarni shiddat bilan qayta loyihalashtirar ekan va bulutli xizmatlardan foydalangan holda butun biznes modellarini qayta tasavvur qilar ekan, bunday keng miqyosda qabul qilish kiber jinoyatchilar uchun kiberfiribgarlik qilish uchun yangi imkoniyatlar yaratmoqda. Ushbu tashkilotlar o'z operatsiyalarini juda tez raqamli o'zgartirishga o'tayotgani sababli, xavfsizlikni samarali boshqarish haqida o'ylash uchun ko'pincha vaqt kam bo'ladi. Korxonalar ko'pincha tasdiqlangan eng yaxshi amaliyotlarni qo'llamaslikni tanlaydilar, bu esa xavflarni to'g'ri baholash va boshqarishni qiyinlashtiradi (agar imkonsiz bo'lsa). Korxonalar doimiy o‘zgarishlarga moslashgani va bulutga faol o‘tayotgani sababli, turli xil qarashlar va kun tartibini yaxlit strategiyaga birlashtirish zarurati tug‘iladi. Bulutga o'tishni birinchi navbatda xavfsizlik strategiyasini faol rivojlantirish imkoniyati sifatida qaraydigan tashkilotlar nozik tranzaksiyalar va ma'lumotlarni himoya qilish bilan birga bulut xizmatlaridan foydalanishni ta'minlashni muvozanatlashi kerak.

Kiberjinoyat - bu kompyuterni sodir etish yoki o'g'irlik qilishning asosiy vositasi sifatida ishlatadigan har qanday noqonuniy faoliyatni nazarda tutuvchi atama. AQSh Adliya departamenti kiberjinoyat tushunchasini kompyuter yordamida dalillarni saqlash uchun ishlatadigan har qanday noqonuniy faoliyatni o'z ichiga olgan holda kengaytirmoqda. O'sib borayotgan kiberjinoyatlar ro'yxatiga kompyuterlar tomonidan sodir etilgan jinoyatlar, jumladan, tarmoqqa kirish va kompyuter viruslarining tarqalishi, shuningdek, shaxsiy ma'lumotlarni o'g'irlash, ta'qib qilish, qo'rqitish va terrorizm kabi mavjud jinoyatlarning kompyuter variantlari mavjud bo'lib, ular uchun jiddiy muammoga aylangan. odamlar va xalqlar. Umuman olganda, oddiy inson tili bilan aytganda, kiberjinoyat deganda kompyuter va Internetdan foydalanib, shaxsning shaxsini

o‘g‘irlash, kontrabandani sotish yoki qurbonlarni bezovta qilish yoki zararli dasturlar orqali operatsiyalarni to‘xtatish maqsadida sodir etilgan jinoyat sifatida ta’riflash mumkin.

Ma'lumotlarning maxfiyligi va xavfsizligi har doim har qanday tashkilot e'tibor beradigan eng yuqori xavfsizlik choralari bo'lib qoladi. Biz hozirda barcha ma'lumotlar raqamli yoki kiber shaklda saqlanadigan dunyoda yashayapmiz. Ijtimoiy tarmoq saytlari foydalanuvchilar o'zlarini do'stlari va oila a'zolari bilan xavfsiz muloqot qilish uchun joy beradi. Uy foydalanuvchilari uchun kiberjinoyatchilar shaxsiy ma'lumotlarni o'g'irlash uchun ijtimoiy tarmoq saytlarini nishonga olishni davom ettiradilar. Nafaqat ijtimoiy tarmoqlarda, balki bank operatsiyalari paytida ham inson barcha zarur xavfsizlik choralarini ko'rishi kerak.

Veb-serverlar. Ma'lumot olish yoki zararli kodni tarqatish uchun veb-ilovalarga hujumlar tahdidi saqlanib qolmoqda. Kiberjinoyatchilar o'zlarining zararli kodlarini buzilgan veb-serverlar orqali tarqatadilar. Ammo ko'pchiligi ommaviy axborot vositalarining e'tiborini tortadigan ma'lumotlarni o'g'irlash hujumlari ham katta xavf tug'diradi. Endi biz veb-serverlar va veb-ilovalarni himoya qilishga ko'proq e'tibor qaratishimiz kerak. Veb-serverlar, ayniqsa, ma'lumotlarni o'g'irlash uchun kiber jinoyatchilar uchun eng yaxshi platformadir. Shu sababli, ushbu jinoyatlar qurboni bo'lmaslik uchun har doim xavfsizroq brauzerdan foydalanish kerak, ayniqsa muhim tranzaktsiyalar paytida.

Zararli dasturiy ta'minot skanerlari odatda tizimda mavjud bo'lgan barcha fayl va hujjatlarni zararli kod yoki zararli viruslar uchun skanerlaydigan dasturdir. Viruslar, qurtlar va troyan otlari ko'pincha birgalikda guruhlangan va zararli dastur deb ataladigan zararli dasturlarga misoldir.

Xavfsizlik devori - bu Internet orqali kompyuteringizga kirishga urinayotgan xakerlar, viruslar va qurtlarni filtrlashga yordam beradigan dasturiy ta'minot yoki apparat qismidir. Internetga kiradigan yoki undan chiqadigan barcha xabarlar mavjud xavfsizlik devori orqali o'tadi, u har bir xabarni tekshiradi va belgilangan

xavfsizlik mezonlariga javob bermaydiganlarni bloklaydi. Shuning uchun xavfsizlik devorlari zararli dasturlarni aniqlashda muhim rol o'ynaydi.

Antivirus dasturlari - viruslar va qurtlar kabi zararli dasturlarni aniqlaydigan, oldini oladigan va zararsizlantirish yoki o'chirish uchun choralar ko'radigan kompyuter dasturi. Aksariyat antivirus dasturlari avtomatik yangilash xususiyatini o'z ichiga oladi, bu dasturga yangi virus profillarini yuklab olish imkonini beradi, shunda ular yangi viruslar aniqlangandan so'ng darhol tekshiriladi. Antivirus dasturi har bir tizim uchun zarur va asosiy zaruratdir.

Xulosa qilib aytadigan bo’lsak kompyuter xavfsizligi keng ko'lamli mavzu bo'lib, dunyo tobora o'zaro bog'lanib borayotgani va muhim tranzaktsiyalarni amalga oshirish uchun tarmoqlardan foydalanilgani sababli tobora muhim ahamiyat kasb etmoqda. Axborot xavfsizligi kabi kiberjinoyatlar ham yil sayin turli yo'llarni bosib o'tishda davom etmoqda. Rivojlanayotgan va buzg'unchi texnologiyalar, shuningdek, har kuni kashf etilayotgan yangi kiber vositalar va tahdidlar tashkilotlarni nafaqat o'z infratuzilmasini himoya qilishda, balki buning uchun yangi platformalar va razvedka talab qilishda ham qiyinchilik tug'dirmoqda. Kiberjinoyat uchun mukammal yechim yo'q, lekin biz kibermakonda xavfsiz va xavfsiz kelajakka ega bo'lish uchun uni minimallashtirishga harakat qilishimiz kerak.

Foydalanilgan adabiyotlar:

1. Cybercrime [Electronic resource] // https://en.wikipedia.org/wiki/Cybercrime.

2. VV Byts', RM Zulunov. Specification of matrix algebra problems by reduction. Journal of Mathematical Sciences. T. 71, 2719–2726 (1994).

3. Web Server and its Types of Attacks [Electronic resource] // URL: https://www.greycampus.com/opencampus/ethicalhacking/web-server-and-its-types-of-attacks.

4. The NIST Definition of Cloud Computing [Electronic resource] // URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecia

5. Advanced persistent threat [Electronic resource] // URL: https://en.wikipedia.org/wiki/Advanced_persistent_thr eat.

6. Stallings W. Cryptography and Network Security: Principles and Practice, 7th Edition / W. Stallings. - London: Pearson plc, Cop. 2017. - 766 p

Ilm fan taraqqiyotida raqamli iqtisodiyot va zamonaviy ta'limning o'rni hamda rivojlanish omillari