KIBERXAVFSIZLIK: TAHDIDLAR VA YECHIMLAR

Komilov Mehriddin Malikovich
Buxoro pedagogika instituti 1-kurs talabasi,
Harbiy tayyorgarlik fakulteti

Annotatsiya: *Jamiyatda kiberxavfsizlik haqidagi bilimlarni berish usullari va vositalaridan foydalanish asoslarini ishlab chiqish. Jamiyat taraqqiyotining asosi sifatida kiberxavfsizlik haqida bilim berish.*

Kalit so'zlar: *kiberxavfsizlik, xulq-atvor, bilim, ko'nikma, xabardorlik, ijtimoiy mobilizatsiya, tarmoq, axborotni himoya qilish, tahdidlar, kiberhujumlar, jamiyat.*

Tadqiqotning maqsadi: *bu muammo zamonaviy dunyoda dolzarb muammoga aylandi, bu erda kibermakonda axborotni himoya qilish juda keskin.*

Аннотация: *Разработка основ использования методов и средств передачи знаний о кибербезопасности в обществе. Предоставление знаний о кибербезопасности как основе развития общества.*

Ключевые слова: *кибербезопастность, поведение, знания, навыки, осведомленность, социальная мобилизация, сеть, защита информации, угрозы, кибер-атаки, общество.*

Целью исследования: *данная проблема стала актуальностью вопроса в современном мире, где защита информации в кибер-пространстве стоит крайне остро.*

Annotation: *Development of the basics of using methods and means of transferring knowledge about cybersecurity in society. Providing knowledge about cybersecurity as the basis for the development of society.*

Key words: *cybersecurity, behavior, knowledge, skills, awareness, social mobilization, network, information protection, threats, cyber attacks, society.*

The purpose of the study: *this problem has become an urgent issue in the modern world, where the protection of information in the cyber space is extremely acute.*

Kirish

Prezidentimiz rahnamoligida mamlakatimizda barcha sohalarni qamrab olgan keng ko‘lamli islohotlar amalga oshirildi va bu ishlar bugungi kunda yangi bosqichda va yanada keng ko‘lamda davom ettirilmoqda. Bu davlat boshqaruvi tuzilmasi bo‘ladimi, xavfsizlik tarmog‘ini boshqarish, sog‘liqni saqlash, sport, ta’lim sohalari bo‘ladimi, barcha sohalarda ijobiy natijalar beradi. Yosh avlodni kiberxavfsizlik ruhida tarbiyalash dolzarb vazifadir. Bu oila va ta’lim muassasalarida ta’lim va tarbiyaga e’tiborni kuchaytirishni taqozo etadi.

Ma’lumotlar uzatish tarmoqlari, kompyuter tizimlari va mobil qurilmalarning ishonchli va xavfsiz ishlashi davlat faoliyati va jamiyatning iqtisodiy barqarorligini saqlashning hayotiy shartidir. Asosiy ommaviy axborot tizimlarining xavfsizligiga ko'plab omillar ta'sir qiladi: kiberhujumlar, jismoniy ta'sir natijasida yuzaga kelgan buzilishlar, dasturiy ta'minot va apparatdagi nosozliklar, inson xatosi. Sanab o'tilgan hodisalar zamonaviy jamiyatning axborot tizimlarining barqarorligiga qanchalik bog'liqligini aniq ko'rsatib turibdi.

Muhokama va natijalar

Kiberxavfsizlik davlatning strategik muammosi sifatida tobora ko'proq ko'rib chiqilmoqda, bu mamlakat iqtisodiyotiga har tomonlama ta'sir ko'rsatadi, shu jumladan dasturiy ta'minot va boshqaruv tizimlarini milliy ishlab chiqaruvchilar, AKT infratuzilmasini ta'minlash uchun asbob-uskunalar va butlovchi qismlarni ishlab chiqaruvchilarning o'zaro hamkorligi, bozor raqobatbardoshligi pastligi xorijiy ishlab chiqaruvchilarning echimlaridan foydalanish zaruriyatini keltirib chiqaradi. Amalda bu hodisa infratuzilmaning barcha segmentlarida ham maxsus davlat organlari, ham fuqarolik sektori uchun “yopiq” dasturiy va texnik vositalardan majburiy foydalanish hisobiga xorijiy ishlab chiqaruvchilarga qaramlikning tez ortishiga va axborot xavfsizligi darajasining pasayishiga olib keladi.

Yaqin kelajakda xorijiy uskunalar ishlab chiqaruvchilari va dasturiy ta'minot ishlab chiqaruvchilariga qaramlik juda muhim darajaga yetishi mumkin. Masalan, yaratilgan virtual “temir parda”ga qaramay, Xitoy rasmiylari mobil qurilmalar uchun Android dasturiy platformasidan keng foydalanish (2012-yilda Xitoy bozoridagi platformaning ulushi 86,4 foizni tashkil etgan) tufayli “ochiq” kodga asoslangan, ammo AQSh razvedkasi tomonidan nazorat qilinganligi sababli o‘zlarining to‘liq qaramligi va zaifligini tan oldi. Iqtisodiy nuqtai nazardan, bu hodisa mobil qurilmalar ishlab chiqarish uchun "ochiq" dasturiy ta'minotdan foydalangan holda elektronika sanoati va real sektorning rivojlanishiga ijobiy ta'sir ko'rsatadi, biroq ayni paytda milliy xavfsizlikka haqiqiy tahdid tug'diradi, uni xorijiy razvedka xizmatlari nazorati ostiga o'tkazadi. Milliy kiberxavfsizlik yetakchi iqtisodiy kuchlar darajasiga mos kelishi uchun, jumladan, davlat tomonidan AKT sohasi ishtirokchilari o‘rtasidagi o‘zaro hamkorlik tizimini rivojlantirish va samaradorligini oshirishga qaratilgan izchil chora-tadbirlarni amalga oshirish zarur. O'z navbatida, korxona ishlab chiquvchilari va ishlab chiqaruvchilari taklif etilayotgan yechimlarning ishonchliligi va xavfsizligiga yuqori talablarni qo'yib, o'zlari ishlab chiqaradigan/ishlab chiqarayotgan mahsulotlarning axborot xavfsizligi masalalariga alohida e'tibor qaratishlari va faqat o'ta og'ir holatlarda va alohida mahsulotlarning bozorga yo'naltirilganligini oshirish zarur bo'lganda, ular xorijiy ishlab chiqaruvchilar va dasturiy ta'minot ishlab chiqaruvchilarining yechimlaridan foydalanishlari kerak. Kiberxavfsizlik zamonaviy dunyodagi eng muhim mavzulardan biridir, chunki texnologiyalar hayotning barcha sohalariga kirib boradi va bizni o'rab oladi.

Kiberxavfsizlik nima?

Kiberxavfsizlik - bu ma'lum bir ish sharoitida va ma'lum vaqt oralig'ida kompyuterga zarar etkazishning mumkin bo'lmagan miqdoridan oshib ketadigan, aniqlangan va o'rganilgan manbalardan ko'ra ko'proq zarar etkazishning mumkin emasligini tavsiflovchi axborot xavfsizligi (ingliz tilidan "Axborot xavfsizligi" - axborot xavfsizligi) bo'limi , kiberob'ektlarning ishlashi va evolyutsiyasi, kiberxavfsizlik manbalarini aniqlash, shuningdek ularning xususiyatlarini aniqlash va aniqlash, shuningdek ularni tasniflash va me'yoriy hujjatlarni shakllantirish (normativ hujjat, har xil faoliyat turlariga yoki ularning natijalariga taalluqli qoidalar, umumiy tamoyillar yoki xususiyatlarni belgilovchi hujjat), ularning amalga oshirilishi barcha aniqlangan kiberobyekt manbalarini ishonchli himoya qilishni kafolatlashi kerak.

Kiberhujum nima?

Axborot tizimiga hujum. Axborot tizimi (AT) - axborotni saqlash, qidirish va qayta ishlash uchun mo'ljallangan tizim va axborotni taqdim etuvchi va tarqatuvchi tegishli tashkiliy resurslar (inson, texnik, moliyaviy va boshqalar).

Axborot tizimiga hujum - bu tajovuzkorning uchta xususiyatdan birini buzishga qaratilgan qasddan harakatlari majmui:

1. Axborotning mavjudligi – axborot (avtomatlashtirilgan axborot tizimining resurslari) holati bo‘lib, undan foydalanish huquqiga ega bo‘lgan sub’ektlar ulardan to‘siqlarsiz foydalanishi mumkin.

Kirish huquqlariga quyidagilar kiradi: axborotni o'qish, o'zgartirish, saqlash, nusxalash va yo'q qilish huquqi, shuningdek resurslarni o'zgartirish, foydalanish va yo'q qilish.

2. Axborotning maxfiyligi - umumiy foydalanish uchun mo'ljallanmagan hamda egasi uchun intellektual yoki iqtisodiy ahamiyatga ega bo'lgan axborotning butunligini saqlash va sizib chiqishidan himoya qilishdir. Maxfiylikni saqlash va axborotni himoya qilish uchun tashkiliy, huquqiy va texnik choralar qo'llaniladi.

3. Axborotning yaxlitligi - axborotning unga hech qanday o'zgarish bo'lmagan holati yoki o'zgartirish faqat unga huquqqa ega bo'lgan sub'ektlar tomonidan ataylab amalga oshiriladi.

Hujumni amalga oshirishning uch bosqichi mavjud:

1. Ular hujum qilmoqchi bo'lgan ob'ekt haqida ma'lumotni tayyorlash va yig'ish bosqichi.

Bu bosqich ham bir necha bo'limlarga bo'lingan.

Ma'lumotlar to'plami

Ma'lumot to'plash hujumni amalga oshirishning asosiy bosqichidir. Birinchidan, hujum nishoni tanlanadi va u haqida ma'lumot yig'iladi (operatsion tizimning turi va versiyasi, ochiq portlar va ishlaydigan tarmoq xizmatlari, o'rnatilgan tizim va amaliy dasturlar va uning konfiguratsiyasi va boshqalar). Keyin hujum qilingan tizimning eng zaif joylari aniqlanadi, ularning ta'siri tajovuzkor xohlagan natijaga olib keladi. Buzg'unchi hujum nishoni va boshqa tugunlar o'rtasidagi o'zaro ta'sirning barcha kanallarini aniqlashga harakat qiladi. Bu sizga nafaqat amalga oshirilayotgan hujum turini, balki uni amalga oshirish manbasini ham tanlash imkonini beradi. Misol uchun, hujumga uchragan tugun Unix va Windows NT bilan ishlaydigan ikkita server bilan o'zaro ta'sir qiladi. Hujum qilingan tugun bir server bilan ishonchli aloqaga ega, lekin boshqasi bilan emas. Qo'llaniladigan hujum turi, tanlangan amalga oshirish vositalari va boshqalar tajovuzkor hujumni amalga oshirish uchun qaysi serverdan foydalanishiga bog'liq. Keyin olingan ma'lumotlarga va kerakli natijaga qarab, eng katta ta'sir ko'rsatadigan hujum tanlanadi. Bu harakatlar turli usullar yordamida amalga oshiriladi.

Atrof-muhitni o'rganish

Ushbu bosqichda tajovuzkor mo'ljallangan hujum nishoni atrofidagi tarmoq muhitini o'rganadi. Bunday hududlarga, masalan, "jabrlanuvchi" Internet-provayderining tugunlari yoki hujum qilingan kompaniyaning uzoqdagi ofisining tugunlari kiradi. Ushbu bosqichda tajovuzkor "ishonchli" tizimlar (masalan, sheriklar tarmog'i) va hujum nishoniga to'g'ridan-to'g'ri bog'langan tugunlar (masalan, ISP router) va boshqalar manzillarini aniqlashga harakat qilishi mumkin. Bunday harakatlarni aniqlash juda qiyin, chunki ular uzoq vaqt davomida va

xavfsizlik vositalari (xavfsizlik devorlari, hujumlarni aniqlash tizimlari va boshqalar) tomonidan boshqariladigan hududdan tashqarida amalga oshiriladi.

Tarmoq topologiyasini identifikatsiya qilish

Tarmoq topologiyasini aniqlash uchun tajovuzkorlar tomonidan ikkita asosiy usul qo'llaniladi:

1.TTLni o'zgartirish (TTL modulyatsiyasi),

2.yozuv marshruti.

Birinchi usul Unix uchun traceroute va Windows uchun tracert dasturlari tomonidan qo'llaniladi. Ular IP-paket sarlavhasida tarmoq paketi bosib o'tgan marshrutizatorlar soniga qarab o'zgaruvchan Live to Live maydonidan foydalanadilar. Ping yordam dasturi ICMP paketining marshrutini yozib olish uchun ishlatilishi mumkin. Ko'pincha tarmoq topologiyasi xavfsizligi noto'g'ri sozlangan ko'plab tarmoq qurilmalarida o'rnatilgan SNMP protokoli yordamida aniqlanishi mumkin. RIP protokolidan foydalanib, siz tarmoqdagi marshrutlash jadvali va boshqalar haqida ma'lumot olishga harakat qilishingiz mumkin. Va 2-usulga kelsak, aytishimiz mumkinki, bu usul to'g'ridan-to'g'ri marshrutlash Sessiyani boshlash protokolini (SIP) qanday amalga oshirishini tavsiflaydi. Seans chegarasi tekshiruvi (SBC) va SIP proksi-server o'rtasida trafikni yo'naltirish uchun ba'zi SIP parametrlari o'ziga xos qiymatlarga ega bo'lishi kerak. Ushbu maqola mahalliy SBC va SIP proksi xizmati o'rtasidagi ulanishni sozlash uchun mas'ul bo'lgan ovozli ma'murlar uchun mo'ljallangan. SIP, ingliz Sessiyani boshlash protokoli, sessiyani boshlash protokoli - bu foydalanuvchi bilan aloqa seansini o'rnatish va tugatish usulini tavsiflovchi ma'lumotlar uzatish protokoli, shu jumladan multimedia kontentini almashish (IP telefoniya, video va audio konferentsiyalar, tezkor xabarlar, onlayn o'yinlar Session chegara nazoratchisi - VoIP xavfsizligini ta'minlaydigan tarmoq qurilmasi, shuningdek, mos kelmaydigan signallarni uzatish moslamalari). SBC qurilmalari korporativ tarmoqlarda va xizmat ko'rsatuvchi provayder tarmoqlarida qo'llaniladi va odatda tarmoq chetida (provayderning korporativ sxemaga kirish nuqtasi) joylashtiriladi.

2. Hujumni amalga oshirish bosqichi

Hujumni amalga oshirish bosqichi - bu tarmoq paketlarining muayyan ketma-ketligini muayyan tarmoq xizmatlariga yuborish, tugunni ishlamay qolishiga olib keladi yoki uzoq tugunning tarmoq xizmatlariga ba'zi so'rovlarni yuborish, bu esa himoyalangan ma'lumotlarga kirishga olib keladi.

3. Bosqinchi haqidagi izlar va ma'lumotlarni yo'q qilish bosqichi.

Hujum izlarini yo'q qilish uchun tajovuzkorlar DNS serverlarini yo'q qiladilar (DNS server - bu saytlarning IP manzillarini saqlaydigan yoki keshlaydigan va ularni so'rov bo'yicha brauzerga beradigan maxsus kompyuter. Ya'ni, DNS server hosts.txt faylini faqat katta hajmda almashtirgan kontaktlar kitobidir. Endi brauzerda domenga kirganingizda, DNS serverlari avtomatik ravishda domen va IP nomini o'rnatib, qurilma o'rtasida bog'lanishni o'rnatasiz).

APT (Advanced Persistent Threats) kabi murakkab hujumlar ko'pincha katta jurnal fayllarida aniqlanmaydi. Ularni tanib olish imkonini beruvchi nafaqat texnik infratuzilma, balki tahdid mavjudligidan darak beruvchi asosiy voqealar haqidagi bilimdir. Ushbu maqolada biz murakkab hujumlarni qanday aniqlash, noto'g'ri pozitivlar sonini kamaytirish va muhim voqeani o'tkazib yuborish xavfini minimallashtirish uchun jurnal tahlilini o'rnatishni tushuntiramiz.

Nima uchun murakkab hujumlarni o'z vaqtida aniqlash muhim ahamiyatga ega.

APT kabi murakkab hujumlar kompaniyalar uchun eng xavfli tahdidlardan biridir. Ular ma'lumotlarni to'plash, tizimlarni buzish yoki ularning ishlashini buzish uchun infratuzilmada uzoq muddatli mavjudligini saqlab qolish maqsadida yashirin tarzda ishlaydi. Bunday hujumlarni erta aniqlash nafaqat yo'qotishlarning oldini olish, balki kompaniyalar barqarorligini ta'minlashning asosiy omilidir.

2024 yilning yanvaridan oktyabrigacha murakkab hujum hodisalari soni 2023 yilning shu davriga nisbatan 45 foizga oshdi. Hujumga uchragan tashkilotlar faoliyat ko'rsatayotgan iqtisodiyot tarmoqlari soni 4 tadan 16 taga ko'paydi. Ko'pincha davlat idoralari, sanoat kompaniyalari va aloqa operatorlari xavf ostida. Ushbu turdagi APT tahdidlarining xavfli tomoni shundaki, ular ko'pincha o'zlarini qonuniy trafik sifatida yashiradilar, lekin o'zlarini noodatiy harakatlar kombinatsiyasi orqali namoyon qiladilar. Bularga faolligi past bo‘lgan uzoq davom etadigan seanslar, ruxsati bo‘lmasligi kerak bo‘lgan imtiyozli hisoblarga kirishga urinishlar, noodatiy DNS va HTTP so‘rovlari, ish vaqtidan tashqari harakatlar, tunnel o‘tkazish va chalkashliklardan foydalanish hamda xavfsizlik sozlamalaridagi o‘zgarishlar kiradi. APT hujumlarini samarali aniqlash uchun ushbu hodisalarning korrelyatsiyasini tahlil qilish va anomaliyalar va shubhali xatti-harakatlar modellarini aniqlash uchun maxsus vositalardan foydalanish muhimdir.

Xavfsizlik jurnallari APTlarga qarshi turishda muhim rol o'ynaydi. Ushbu ma'lumotlar tizimlar va tarmoqdagi faollikni qayd etib, foydalanuvchi va tizim xatti-harakatlaridagi og'ishlarni aniqlashga yordam beradigan raqamli tarixni yaratadi. Jurnal tahlili zararli faoliyatni ko'rsatadigan anomaliyalarni aniqlash imkonini beradi: shubhali so'rovlar, imtiyozlarga ega bo'lgan atipik harakatlar yoki zaifliklardan foydalanishga urinishlar. To'g'ri jurnal boshqaruvisiz kompaniyalar o'z obro'sini yo'qotishi va katta yo'qotishlarga olib kelishi mumkin bo'lgan hujumlarga qarshi himoyasiz qoladi.

Murakkab hujumlarni ko'rsatadigan jurnallardagi asosiy voqealar

APT va boshqa ilg'or tahdidlarni aniqlash uchun jurnallardagi asosiy voqealarni diqqat bilan tahlil qilish muhimdir. Ushbu signallar infratuzilmani buzish, yashirish yoki hujumga tayyorlashga urinishlarni ko'rsatishi mumkin (Advenced Persistent Threats) ko'pincha ko'p bosqichli hujum jarayoni va korporativ infratuzilmada uzoq muddatli mavjudligi bilan tavsiflanadi. Murakkab, maqsadli hujumlarni amalga oshirishni bilvosita yoki to'g'ridan-to'g'ri ko'rsatadigan asosiy hodisalarni ko'rib chiqish mumkin: Tarmoqning g'ayritabiiy faoliyati. Masalan, tashkilot infratuzilmasini tashqi va ichki razvedka qilishda; noma'lum domenlar va IP manzillar bilan o'zaro aloqa.

Xavfsizlik jurnallarida shubhali avtorizatsiya yozuvlari. Misol uchun, bir nechta muvaffaqiyatsiz urinishlardan so'ng muvaffaqiyatli kirish muvaffaqiyatli qo'pol kuch hujumini ko'rsatishi mumkin. Tashlab ketilgan akkauntlardan kutilmagan harakatlar yoki kompaniyaning markaziy ofisi, sho‘ba korxonalari yoki xodimlarning o‘zlari joylashgan joy bilan bog‘liq bo‘lmagan IP manzillardan ruxsat olish ham shubha uyg‘otadi.

Xodim qurilmalarida shubhali harakat. Noqonuniy faoliyat qurilmada yangi jarayonlarni ishga tushirish, tizim konfiguratsiyasini o'zgartirish, xavfsizlik tizimlarini o'chirishga urinishlarni o'z ichiga olishi mumkin.

Ekspluatatsiyadan keyingi bosqichni amalga oshirishni ko'rsatadigan faoliyat. Masalan, yangi imtiyozli hisoblarni yaratish, hisoblar o'rtasida o'tish, katta hajmdagi korporativ ma'lumotlarni olishga harakat qilish yoki muvaffaqiyatli olish.

Imtiyozlar va xavfsizlik siyosatidagi o'zgarishlar ham axborot xavfsizligi xodimlarining e'tiborini jalb qilishi kerak. Foydalanuvchi huquqlarini asossiz ravishda oshirish, yuqori imtiyozlarga ega yangi hisoblarni qo'shish yoki xavfsizlik siyosatini o'zgartirish tajovuzkor mavjudligini aniqlash yoki kirishni kengaytirishga tayyorlanayotganligini ko'rsatishi mumkin. Bu hodisalarni avvalo yozib olish va tahlil qilish kerak.

Jurnallardagi xavotirli hodisalarning yana bir varianti - atipik maqsadlarda qonuniy vositalardan foydalanish. Jurnallar odatda ishlatilmaydigan tizimlarda ishlatiladigan PowerShell, WMI yoki boshqa ma'muriy vositalar orqali bajariladigan buyruqlarni ko'rsatishi mumkin. Bu tajovuzkorlar o'z harakatlarini xodimlarning faoliyati sifatida yashirish usullaridan biridir. Jurnallarning qismlarini o'chirish, ularning mazmunini o'zgartirish yoki muayyan jarayonlar uchun jurnalni o'chirish kabi izlarni yashirishga urinishlar ham murakkab hujumning aniq belgilaridir.

Muayyan voqea umuman e'tiborni jalb qilmasligi mumkin, shuning uchun nima sodir bo'layotganini kengroq ko'rib chiqishga arziydi. Har bir murakkab hujum ketma-ket va o'zaro bog'liq harakatlar zanjiridan iborat bo'lib, ular birgalikda hujum vektorini tashkil qiladi. Hujumning barcha bosqichlarida tajovuzkorlarning harakatlariga xos bo'lgan umumiy belgilarni aniqlash mumkin:

Xiralashish. Kod va trafikni aniqlashni qiyinlashtirish uchun xiralashtirish usullaridan foydalanish.

Qonuniy hisoblardan foydalanish. Buzg'unchilar ko'pincha tizimga kirish uchun o'g'irlangan yoki buzilgan hisoblardan foydalanadilar.

Uzoq muddatli faoliyat. APT hujumlari tarmoqdagi uzoq muddatli yashirin faoliyat bilan tavsiflanadi.

Turli monitoring vositalari bunday faoliyatni aniqlashga yordam beradi. Hamma uchun tushunarli bo'lgan SIEM-dan tashqari, tarmoq trafigini tahlil qilish vositalari muhim ahamiyatga ega. Bundan tashqari, EDR/XDR yechimlari, UEBA foydalanuvchi xatti-harakatlarini tahlil qilish tizimlari va sinov muhiti zararli dasturlarini tahlil qilish tizimlaridan foydalanish ham muhimdir. Biz inson omili haqida unutmasligimiz kerak - tajribali xavfsizlik tahlilchilari o'zlarining bilimlari va sezgilaridan foydalanadilar.

Murakkab APT hujumlarining xarakteristikasi jurnallarni tahlil qilish orqali aniqlanishi mumkin bo'lgan xususiyatlarni o'z ichiga oladi. Masalan, tajovuzkorlar tarmoq resurslarini uzoq va past intensivlikdagi skanerdan o'tkazishi mumkin, bu esa aniqlanmaslik uchun to'satdan anomaliyalarga yo'l qo'ymaydi. Bir xil IP-manzillarga, lekin turli tarmoq segmentlariga ulanish uchun takroriy urinishlar ko'pincha kuzatiladi, bu yashirin aloqa kanalini o'rnatishga urinishlarni ko'rsatishi mumkin. Shuningdek, noma'lum jarayonlar yoki ilovalarning paydo bo'lishiga alohida e'tibor berilishi kerak, ayniqsa ular tashqi serverlar bilan o'zaro aloqada bo'lsa yoki nostandart operatsiyalarni bajarsa.

Alohida, bog'liq bo'lmagan hodisalar kamdan-kam hollarda murakkab hujumlarni ko'rsatadi. Agar hujumning o'zi haqida gapiradigan bo'lsak, uni "murakkab" qiladigan narsa o'ldirish zanjiri. Agar tahlil doirasida biz yagona metodologiya (masalan, Cyber Kill Chain yoki

Unified Kill Chain) doirasidagi voqealarning yagona zanjiriga "chiziqlangan" voqealarni aniqlay olsak, unda "etuk" hujumchi belgilari mavjudligi haqida gapirishimiz mumkin.

Hodisalarni keyingi o'rganish ochiq manbalarga asoslangan ma'lum guruhlar yoki APTlarga mos kelishi mumkin bo'lgan ko'rsatkichlarni aniqlaydi. Bunday faoliyatning ko'plab misollari bo'lishi mumkin va ularni aniqlash ham infratuzilmani qayd etish sozlamalariga, ham tadqiqotni olib borayotgan tahlilchining tajribasiga bog'liq.

Misol: Muvaffaqiyatsiz kirish hodisalari

Qarama-qarshi misol ham mavjud: IP-manzilga chiquvchi ulanish perimetrda qayd etilgan, bu regulyatorning xavfsizlik byulletenlariga ko'ra, zararli bo'lishi mumkin. Hodisalarning batafsil tahlili xostga ulanish uchun bir nechta urinishlarni ko'rsatadi (RDP, SMB), lekin muvaffaqiyatli kirish yo'q. Chiquvchi ulanish tarixini tekshirish foydalanuvchi brauzeri orqali noqonuniy domen bilan bir xil manzilda joylashgan qonuniy domenga ulanishlarni ko'rsatadi. Voqealarning yagona zanjiri yo'q edi, shuning uchun APT yoki murakkab hujum haqida gapirish mumkin emas. Albatta, voqeani APT bilan bog'liq deb tasniflash faqat bitta hodisaga asoslangan holda amalga oshirilishi mumkin - avval atributlangan IP manzil yoki domenga masofaviy ulanish. Biroq, bunday ko'rsatkichlarning dolzarbligini ko'rib chiqishga arziydi, chunki vaqt o'tishi bilan domenlar bo'linishi va IP manzillari boshqa shaxslarga foydalanish uchun o'tkazilishi mumkin.

Ushbu hodisalar va ularning o'zaro munosabatlari xavfsizlik mutaxassislariga, hatto hujumchilar o'z harakatlarini yashirishga harakat qilganda ham murakkab tahdidlarni aniqlashga yordam beradi.

Kiberhujum bo'lganini qanday tushunish mumkin?

Aniqki: antiviruslar va xavfsizlik devorlarining xavfsizlik hodisalarini kuzatib boring. Bundan tashqari, ushbu fikrlarga e'tibor berishga arziydi.

1. Foydalanuvchilar tomonidan o'rnatilishi yoki ishga tushirilishi ruxsat etilmagan dasturiy ta'minotni ishga tushirish. Misol: Powershell.exe\cmd.exe faylida buxgalter hisobi nomidan seans ochilganini ko'rsangiz, bu tashvishga sabab bo'ladi.

2. Noma'lum tarmoq trafigi. Misol: mavjud bo'lmagan DNS serverlariga kiruvchi tugunlar.

3. Ish vaqtidan tashqari foydalanuvchilarning faol faoliyati.

4. Shubhali tizim yuki. Misol: protsessorning anormal yuklanishi.

5. Ro'yxatga olish kitobidagi shubhali o'zgarishlar. Misol: ishga tushirish uchun dasturlarni qo'shish.

6. Kritik tizim xato xabarlari va tizimni qayta ishga tushirish. Bu kompaniyaning axborot tizimiga hujum qilishga urinishdan dalolat berishi mumkin.

7. Fayllar va dasturlar bilan g'ayritabiiy ishlash. Misol: shifrlangan fayllarning paydo bo'lishi yoki uchinchi tomon dasturlarini o'rnatish, fayllarni tashqi muhitga nusxalash.

8. Operatsion tizim, antivirus va amaliy dasturlar sozlamalaridagi shubhali o'zgarishlar. Misol: ish joyida antivirus dasturini o'chirib qo'yish.

9. Noma'lum elektron pochta faoliyati. Misol: bu erda hamma narsa oddiy - spam.

10. Avtorizatsiya jurnallaridagi anomaliyalar. Misol: noto'g'ri parollarni kiritish uchun bir necha marta urinish.

Agar kiberhujum aniqlansa nima qilish kerak?

Birinchidan, ustuvorliklarni belgilaylik. Buning uchun buzilgan axborot resurslari va texnik vositalarning tanqidiylik darajasini baholash kerak: kritik, yuqori, o'rta yoki past. Zarar darajasi tekshirish uchun qancha vaqt ketishini va qarorlar qanchalik tez qabul qilinishini aniqlaydi.

MUHIM! Agar siz kiberhujumni aniqlagan bo'lsangiz, hech qanday holatda uskunani elektr ta'minotidan uzib qo'ymang, bu tergov uchun zarur bo'lgan qimmatli ko'rsatkichlarning yo'qolishiga va ishga tushirilganda tizimning ishlamay qolishiga olib kelishi mumkin.

O'zingizni kiberhujumlardan qanday himoya qilish kerak?

O'zingizni kiberhujumlardan himoya qilish uchun keng qamrovli yondashuv va bir nechta asosiy qadamlar talab etiladi. Mana bir nechta asosiy choralar:

1. Antivirus dasturlari va xavfsizlik devorlaridan foydalaning: Tahdidlarni aniqlash va bloklashda yordam berish uchun antivirus dasturini o'rnating va kiruvchi va chiquvchi trafikni boshqarish uchun xavfsizlik devoridan foydalaning.

2. Dasturiy ta'minotni yangilang: Operatsion tizimlaringizni va dasturiy ta'minotingizni muntazam yangilab turing, chunki yangilanishlar ko'pincha kiberjinoyatchilar tomonidan ishlatilishi mumkin bo'lgan zaifliklarni tuzatadi.

3. Murakkab parollar va ikki faktorli autentifikatsiya (2FA): uzun, murakkab parollardan foydalaning va hisoblaringiz xavfsizligini yaxshilash uchun ikki faktorli autentifikatsiyani yoqing.

4. Ma'lumotlarni shifrlash: qurilmalarda va tarmoq bo'ylab harakatlanayotganda nozik ma'lumotlarni shifrlash. Bu ma'lumot noto'g'ri qo'llarga tushib qolsa ham himoya qilishga yordam beradi.

5. Elektron pochta va havolalar bilan ehtiyot bo'ling: Elektron pochta xabarlaridagi qo'shimchalar va havolalar bilan ehtiyot bo'ling, ayniqsa ular noma'lum jo'natuvchilardan kelgan bo'lsa. Bu fishing urinishi bo'lishi mumkin.

6. Ma’lumotlaringizning zaxira nusxasini yarating: to‘lov dasturi kabi hujum sodir bo‘lgan taqdirda ularni qayta tiklash uchun muhim ma’lumotlaringizning muntazam zaxira nusxalarini yarating.

7. Kirishni cheklash: Muhim tizimlar va ma'lumotlarga faqat o'z vazifalarini bajarish uchun haqiqatan ham muhtoj bo'lgan xodimlarga kirishni minimallashtiring.

8. Xodimlarni o'qitish: xodimlarni kiberxavfsizlik asoslariga o'rgatish muhim, chunki inson omili ko'pincha zaiflikka aylanadi.

9. Tarmoq va tizim monitoringi: Shubhali faoliyatni o'z vaqtida aniqlash va chora ko'rish uchun tarmoq faoliyatini doimiy ravishda kuzatib boring.

10. Xavfsizlik siyosatini amalga oshirish: Ichki xavfsizlik siyosatini, shu jumladan qurilmalar va tarmoq resurslaridan foydalanish qoidalarini ishlab chiqish va amalga oshirish.

Ushbu tavsiyalarga amal qilish orqali siz kiberhujumlar xavfini sezilarli darajada kamaytirishingiz va raqamli infratuzilmangizning xavfsizlik darajasini oshirishingiz mumkin.

Xulosa

Xulosa qilib aytganda, bir qator tadqiqotlar shuni ko'rsatdiki, samarali monitoring oddiy xatti-harakatlarning asosiy ko'rsatkichlarini aniqlashdan boshlanadi. Asosiy tizim profilini o'rnatish tahdid signallari bo'lishi mumkin bo'lgan og'ishlarni ajratib ko'rsatish imkonini beradi. Noto'g'ri signallarni oldini olish uchun kompaniya ishining o'ziga xos

xususiyatlarini hisobga olish muhimdir. Qoidalarni muntazam ko'rib chiqish va yangi operatsion stsenariylarga avtomatlashtirilgan moslashish tizimni yangilab turishga yordam beradi. Xavfsizlik ma'lumotlari va hodisalarni boshqarish (SIEM) tizimlaridan foydalanish katta hajmdagi jurnallarni qayta ishlashni ancha osonlashtiradi. SIEM turli manbalardan olingan ma'lumotlarni birlashtiradi va potentsial xavfli hodisalarni ta'kidlash uchun korrelyatsiya qoidalaridan foydalanadi. Samaradorlikni oshirish uchun qoidalarni muntazam yangilab turish va tahlil qilish uchun yangi shablonlarni joriy etish tavsiya etiladi. Jurnalni tahlil qilishda maksimal samaradorlikka erishish uchun texnologik echimlarni mutaxassislarning tajribasi bilan birlashtirish kerak. Monitoringni optimallashtirish, SIEMni joriy qilish va jarayonlarni muntazam takomillashtirish xavfsizlikni sezilarli darajada yaxshilashga yordam beradi va kiber tahdidlarga tezda javob beradi.

Menejerlar ko'pincha serverlar va ma'lumotlar xavfsizligini ta'minlash uchun mas'uliyatli odamlarni yollashlari kerak, deb hisoblashadi, oddiy xodimlar esa ko'plab tushunarsiz shartlar bilan ko'p sahifali yo'riqnomani o'qib chiqishlari va jurnalga imzo qo'yishlari kerak. Qoidaga ko'ra, eng yaxshi holatda bu jurnal diagonal ravishda o'qiladi va ko'pincha u ko'r-ko'rona imzolanadi.

Kompaniya o'zini kiber tahdidlardan himoya qilish uchun qanday choralar ko'rishi kerak?

1-qadam: Mas'uliyatni taqsimlash

Kompaniyada ma'lumotlar xavfsizligi ikki darajada nazorat qilinishi kerak - boshqaruv va o'rta boshqaruv kompaniyaning egasi axborot va serverlarning umumiy himoyasi uchun javobgardir. Biznes asoschisi har bir xodim amal qilishi kerak bo'lgan qoidalar yoki qoidalar to'plamini yozadi. Ijtimoiy media akkauntlaringizdan chiqish kabi oddiy ko'rsatmalar bo'lishi mumkin yoki xavfsizlik qonunlariga rioya qilish kabi murakkabroq ko'rsatmalar xodimlarni xabardor qilish uchun javobgardir. Ular xodimlarga qoidalar haqida ma'lumot berishlari, treninglar o'tkazishlari va qoidalarga rioya etilishini nazorat qilishlari kerak. O'rtacha bu har chorakda bitta mashg'ulot. Har kuni xavfsizlik qoidalariga rioya qilishni ta'minlash hatto kichik kompaniyalar uchun ham juda qiyin. Shu sababli, siz axborot xavfsizligi qoidalariga berilib ketmasligingiz kerak, siz treninglar, o'quv mahorat darslari va Internet xavfsizligi bo'yicha qiziqarli viktorinalar yordamida umuman axborot muhitida iste'mol qilish madaniyatiga ta'sir qilishingiz kerak;

2-qadam. Qoidalarni yarating

Agar xodimlar asosiy xavfsizlik standartlariga rioya qilsalar, buzilishlar minimallashtirilishi mumkin.

Axborot xavfsizligi qoidalari quyidagicha ko'rinishi mumkin:

1) Hisoblaringiz uchun murakkab parollardan foydalaning va ularni har 2-3 oyda o'zgartiring. Qwerty123, itning ismi, ismi va tug'ilgan sanasi kabi juda oddiy parollardan saqlaning.

2) Ishni tugatgandan so'ng masofaviy ish stoli (RDP) seanslarini yoping. 3) Antivirus holatini doimo yoqilgan holda saqlang.

4) Shaxsiy kompyuteringizda saqlangan barcha muhim ma'lumotlarni muntazam ravishda zaxiralang.

5) Ulanishlar xavfsizligini tekshiring. HTTPS bilan boshlangan veb-sayt manzili xavfsizdir. Agar manzil HTTP bilan boshlansa, bu ulanish xavfsiz emasligini bildiradi.

6) Shaxsiy va ish elektron pochta xabarlarini ajrating. Ish elektron pochtasidan shaxsiy maqsadlarda foydalanmang va aksincha.

7) Noma'lum yoki shubhali manzildan yuborilgan xatlarni ochmang.

3-qadam. Tekshirish ro'yxatlarini amalga oshirish

Ko'rsatmalar oddiy inson tilida yozilishi kerak. Bu shunchaki matnli hujjat emas, balki nazorat ro'yxati - axborot xavfsizligi bo'yicha fikrlar ro'yxati bo'lsa yaxshi bo'lardi. Uni ofisning ko'zga ko'ringan joyiga qo'yish mumkin va xodimlardan narsalarni to'ldirgandan keyin tekshirishni so'rash mumkin. Nazorat varaqlarining mazmuni ko'p jihatdan kompaniyada qanday dasturiy ta'minot qo'llanilishiga, xodimlarning Internetda qancha ishlashiga va hokazolarga bog'liq. Barcha tashkilotlar uchun bir qator universal qoidalar mavjud:

Parolni har oy o'zgartiring;

RDP masofaviy ish stolini o'chirish;

Antivirus dasturlarini o'rnatish;

Murakkab login va parollardan foydalanish;

Veb-saytlarning manzillar panelidagi ulanishlar xavfsizligini tekshirish.

4-qadam: Muhimligini etkazing

Xodimlaringizga kiberxavfsizlik nima uchun muhimligini tushuntiring. Misol uchun, siz ularga shaxsan nima xavf ostida ekanligini aytishingiz mumkin. Ularning ma'lumotlari noto'g'ri qo'llarga tushishi mumkin. Firibgar sizdan ma'lumotlarni to'lashni talab qilishi mumkin, u bilan sizni shantaj qilishi mumkin, aks holda u Internetda tarqatadi.

Haqiqiy tahdid eng yaxshi motivatordir. Agar kompaniyaga kiber tahdid allaqachon ro'y bergan bo'lsa, bu haqda jasorat bilan gapirishingiz kerak. Shunday qilib, xodimlar bu ular ham duch kelishi mumkin bo'lgan va shunga mos ravishda azob chekishi mumkin bo'lgan haqiqiy vaziyat ekanligini tushunishadi.

Rossiyadagi eng yirik energetika kompaniyalaridan birida xodim o'z menejeri bilan shaxsiy elektron pochta orqali yozishmalarini yuborgani uchun ishdan bo'shatildi, unda pudratchilar bilan tuzilgan shartnomalar shartlari, qarz miqdori va shartnoma chegaralari mavjud. Gmail elektron pochta xizmati uchun foydalanuvchi shartnomasi (shaxsiy elektron pochta ro'yxatdan o'tgan joyda) Google elektron pochta xabarlari tarkibiga kirish huquqiga ega deb hisoblaydi va sud bunday ma'lumotlar uchinchi shaxsga ma'lum bo'lgan deb hisoblaydi. Xuddi shunday taqdir qarz agentliklaridan birining xodimi bilan ham sodir bo'ldi, u maxfiy ma'lumotlarni go'yoki uyda ishlash uchun flesh-diskga ko'chirgan, ammo ishdan bo'shatilgan.

Xodimlaringizga aytib beradigan uchta hikoya

2020-yil sentabr oyida Germaniyadagi shifoxonalardan biri bemorga tibbiy yordam ko‘rsata olmadi, chunki muassasa kompyuterlari virus bilan zararlangan. Ayol boshqa shahardagi shifoxonaga olib ketilayotganda vafot etgan. Bir kun avval klinikaga xakerlik hujumi uyushtirildi - 30 ta serverga kirish shifrlangan. Tibbiyot muassasasi ishi deyarli ikki hafta davomida falaj bo'lib qoldi. Buyuk Britaniyada 58 yoshli ayol ilgari direktor bo‘lib ishlagan bosmaxonadan o‘ch olishga qaror qildi. Ayol kompaniyaning Dropbox akkauntiga kirib, korporativ ma’lumotlarni o‘z ichiga olgan 5000 ga yaqin faylni butunlay o‘chirib tashladi.

Nashriyot yo‘qolgan ma’lumotlarni tiklay olmadi, 100 000 funt sterling miqdorida zarar ko‘rdi va yopilishga majbur bo‘ldi.

O'tgan yilning may oyida AQShning mustamlaka quvurlari tizimi falaj bo'lgan ransomware virusi hujumiga uchradi. Quvur besh kun davomida ishlamay qolgan, bu esa AQShda benzin yetkazib berishda uzilishlarga sabab bo‘lgan. Ishga qaytish uchun kompaniya xakerlarga 4,4 million dollar to‘lashi kerak edi.

5-qadam: O'rgatish va jazolash

Parollar qanchalik muhimligini tushuntirish, ularni yaratish va saqlash uchun ishonchli dasturlar haqida gapirish kerak, qoida tariqasida, kichik kompaniyalar menejerning vakolati va tajribasi yordamida xodimlarni mustaqil ravishda Internetda axborot gigienasi bo'yicha o'qitadilar yoki xodimlar bilan muloqotda raqamli xavfsizlikning muhimligini tushuntirib beradigan tashqi mutaxassisni - murabbiyni taklif qilishadi. Shuningdek, u xodimlarning ko'rsatmalariga rioya qilishiga to'sqinlik qiladigan qo'rquv va to'siqlarga qarshi kurashadi. Masalan, eng ko'p uchraydigan e'tirozlardan biri - qoidalarga rioya qilish uchun vaqt yo'qligi va ularning noaniq afzalliklari xodimlarni kiberxavfsizlik asoslariga o'rgatuvchi va olingan bilimlarni sinab ko'radigan alohida kompaniyalar ham mavjud. Ular fishing hujumlarini aniqlash ko'nikmalarini rivojlantiradilar va xodimlarning xabardorligini kerakli darajada ushlab turadilar. Taniqli kompaniyalar tajribasiga murojaat qilish arziydi. Misol uchun, bir oy davomida bir yilda bir marta Facebook o'z xodimlarini fishing hujumlari, ommaviy spam jo'natmalari va boshqa kiber tahdidlarni simulyatsiya qilish orqali sinovdan o'tkazadi. Hujumlarni muvaffaqiyatli qaytarganlar esdalik sovg'alari va boshqa sovg'alar bilan taqdirlanadilar.

Bu nafaqat jazolarga, balki xodimlarni rag'batlantirishning ijobiy dasturlariga ham e'tibor qaratish lozim. Merilend universitetining kiberxavfsizlik laboratoriyasi tadqiqotchilari tomonidan 2014-yilda o‘tkazilgan tadqiqot shuni ko‘rsatdiki, kollej o‘quvchilari “Security Empire” kompyuter o‘yinini o‘ynab kriptografik xavfsizlik, autentifikatsiya usullari va dasturiy ta’minotini yangilashni oson o‘rgangan. Ushbu o'yindagi o'yinchilar kiberxavfsizlikda xatolarga yo'l qo'yganlarida moliyaviy muammolar va ishlab chiqarishdagi muvaffaqiyatsizliklarga duchor bo'lgan kompaniyalarning egalariga aylanishadi. Ushbu o'yinda talabalar eng muvaffaqiyatli kompaniyani yaratish uchun raqobatlashadilar. Nega kompaniya xodimlari uchun ham shunday qilmaslik kerak?

6-qadam. Mutaxassislikka ega bo'ling

Kompaniyada axborot xavfsizligi bo'yicha alohida mutaxassisni yollashdan foyda yo'q. Vaqt va moliyaviy xarajatlar nuqtai nazaridan, xizmatga ulanish yoki bir martalik maslahatlarni sotib olish yanada oqilona bo'ladi. Alohida xodimni uyda saqlashdan ko'ra, mutaxassisni autsorsing qilish foydaliroq.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. Davlat organlarining taqsimlangan multiservis tarmoqlarida axborot xavfsizligi tahdidlarini aniqlash algoritmi / A. Yu., A. M. Sokolov, S. S. Shirokov, N. N. Prokimnov // Amaliy informatika. - 2023. - T.

2. Barinova A. Qanday qilib HR axborot xavfsizligi bo'yicha treningni mustaqil ravishda o'tkazishi mumkin: asosiy tahdidlar bo'yicha tayyor ma'ruza xulosasi / A. Barinova // HR direktori. - 2022. - 5-son.

3. Belov A. S. Axborot xavfsizligi tizimini modernizatsiya qilish: chastotani aniqlashga yondashuv: chastotani aniqlashga yondashuv / A. S. Belov, M. M. Dobryshin, D. E. Shugurov // Axborot xavfsizligi. Insayder. - 2022 yil.

4. Vasilev V. I. Transformator texnologiyasidan foydalangan holda axborot xavfsizligiga joriy tahdidlarni baholash / V. I. Vasilev, A. M. Vulfin, N. V. Kuchkarova // Kiberxavfsizlik masalalari. - 2022. - 2-son.

5. Gladkix A. V. Intellektual tarmoqlarda DDoS hujumlaridan himoya qilish usullari / A. V. Gladkix // Jamiyatning raqamli transformatsiyasi va axborot xavfsizligi: Butunrossiya materiallari. ilmiy va amaliy konf. (Ekaterinburg, 2022 yil 18 may) - Ekaterinburg, 2022 yil.

6. Gladkov A. N. Axborot xavfsizligi sohasidagi vakolatlarni shakllantirish jihati sifatida kiber tahdidlarning vizualizatsiyasi / A. N. Gladkov, S. N. Goryachev, N. S. Kobyakov // Axborot xavfsizligi. Insayder. - 2023 yil - 1-son.

7. Golubev G. D. Kam quvvatli global tarmoqlarning xavfsizligini ko'rib chiqish: tahdidlar, muammolar va potentsial echimlar / G. D. Golubev // Jamiyatning raqamli transformatsiyasi va axborot xavfsizligi: Butunrossiya materiallari. ilmiy va amaliy konf. (Ekaterinburg, 2022 yil 18 may) - Ekaterinburg, 2022 yil.

8. Vinokurov A.Yu. An'anaviy kriptografik algoritmlar. [Elektron resurs] // Kirish rejimi: ww.enlight.ru/crypto/algorithms/algs. (kirish sanasi: 20.05.2021).

9. Yosh olim No33 (480) 2023 yil avgust - Abdullaev E. A.Kiberxavfsizlik: Raqamli asrdagi muammolar va mudofaa strategiyalari

10. Yosh olim No7 (349) 2021 yil fevral - Malik T.N.Kiberxavfsizlik: muammolar va istiqbollar

11. Yosh olim No 23 (418) 2022 yil iyun - Pavlov A. A.Smart City tizimini joriy etish jarayonida davlat va kommunal xizmatlar tizimida axborot xavfsizligi

12. Yosh olim No5 (452) 2023 yil fevral - Strunin D. A.Kiberhujumlar va ularning raqamli iqtisodiyotga ta'siri

13. Yosh olim No 51 (446) 2022 yil - Boldirixin N.V., Karpenko M.V., Kornilova A.V. Tarmoq hujumlarining analitik sharhi

14. Yosh olim No 17 (412) 2022 yil aprel - Ijuninov M.A., Strunin D.A., Antipko A.V. Kiberhujumlarning raqamli iqtisodiyotga ta'siri

15. Yosh olim No22 (364) 2021 yil may - Avxadeeva G.I. Internet xavfsizligi

16. "Ko'rinmas bo'lish san'ati. Katta ma'lumotlar asrida maxfiylikni qanday saqlash kerak, Kevin Mitnik. 2021 yil

17. Jeymi Bartlettning "Yer osti interneti". 2017 yil

18. "Tarmoqdagi sharpa", Kevin Mitnik, 2012 yil

19. “Hacking. Ekspluatatsiya san'ati, Jon Erikson 2021