AXBOROT XAVFSIZLIGI TUSHUNCHASINING NAZARIY TAHLILI VA HUQUQIY OMILLARI

Anvarova Muqaddas Xomidjon qizi

O‘zbekiston jurnalistika va ommaviy kommunikatsiyalar universiteti Xalqaro jurnalistika yo'nalishi 3- kurs talabasi

Annotatsiya: Axborot xavfsizligi - bu ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlash uchun xavfsizlik choralarini qo'llash jarayoni hisoblanadi. Tizim boshqaruvchisi axborot xavfsizligi uchun mas'ul shaxs sifatida ma’lum bir tashkilotning aktivlari, shu jumladan kompyuterlar, serverlar va tashkilot tarmog'ining barcha ishtirokchilari (foydalanuvchilari) mahalliy tarmog'i ma'lumotlarining himoya qilinishini ta'minlaydi. Bundan tashqari, tashkilotning binolari, inshootlari, infratuzilma ob'ektlari va eng muhimi, unda xodimlarning axborot xavfsizligi himoyaga olingan.

Kalit so’zlar: Axborot xavfsizligi, nazariy tahlil, huquqiy omillar, serverlar

Axborot makonida mavjud bo'lgan ma'lumotlarga ko'ra, axborot xavfsizligi - bu axborot xavfsizligi bo'limi bo'lib, uning doirasida ular kiberxavflar manbalarini aniqlash uchun kiberob'ektlarning shakllanishi, faoliyati va evolyutsiyasi jarayonlarini o'rganadilar. Bu holda ularning xususiyatlarini, shuningdek ularni tasniflashni va normativ hujjatlarni shakllantirishni aniqlash, ularning amalga oshirilishi kiberob'ektlarni barcha aniqlangan va o'rganilgan kiberxavf manbalaridan himoya qilishni kafolatlashi kerak.

Axborot xavfsizligi - bu ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlash uchun xavfsizlik choralarini qo'llash jarayoni hisoblanadi. Tizim boshqaruvchisi axborot xavfsizligi uchun mas'ul shaxs sifatida ma’lum bir tashkilotning aktivlari, shu jumladan kompyuterlar, serverlar va tashkilot tarmog'ining barcha ishtirokchilari (foydalanuvchilari) mahalliy tarmog'i ma'lumotlarining himoya

qilinishini ta'minlaydi. Bundan tashqari, tashkilotning binolari, inshootlari, infratuzilma ob'ektlari va eng muhimi, unda xodimlarning axborot xavfsizligi himoyaga olingan.

Axborot xavfsizligining maqsadi ma’lum bir tashkilotda aylanib yuradigan barcha ma'lumotlarni (uzatish yoki almashish jarayonida ham, saqlashda ham) himoya qilishdir. Hozirgi vaqtda axborot xavfsizligini ta'minlash uchun jiddiy choralar qo'llanilishi mumkin. Ushbu chora-tadbirlarning ba'zilariga kirishni nazorat qilish, xodimlarni o'qitish, axborot xavfsizligi bo'yicha audit va hisobot berish, xavflarni baholash, foydalanuvchi so'rovlari, mumkin bo'lgan hujumlar tahdidi kanallarini sinovdan o'tkazish va avtorizatsiyani (autentifikatsiyani) talab qilish kiradi (lekin barchasi faqat shular bilan cheklanmaydi). Axborot xavfsizligini ta'minlashning asosiy maqsadi ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini, dasturning maqsadga muvofiqligini hisobga olgan holda va tashkilot faoliyatiga hech qanday zarar etkazmasdan muvozanatli himoya qilishdir. Bunga, birinchi navbatda, asosiy vositalar va nomoddiy aktivlar, tahdid manbalari, zaifliklar, potentsial ta'sirlar va risklarni boshqarish imkoniyatlarini aniqlaydigan ko'p bosqichli risklarni boshqarish jarayoni orqali erishiladi. Ushbu jarayon risklarni boshqarish rejasining samaradorligini baholash bilan birga keladi. O'z navbatida, taniqli CISCO kompaniyasi nuqtai nazaridan axborot xavfsizligining uslubiy asoslariga ko'ra, ushbu tadqiqotning nazariy asosi sifatida axborot xavfsizligi tizimlar, tarmoqlar va dasturiy ta'minotni raqamli hujumlardan himoya qilish bo'yicha chora-tadbirlarni amalga oshirish tushuniladi. Bunday hujumlar odatda maxfiy ma'lumotlarga kirish, uni o'zgartirish va yo'q qilish, foydalanuvchilardan pul undirish yoki kompaniyalarning normal faoliyatini buzishga qaratilgan. CISCO ekspertlarining fikriga ko'ra, axborot xavfsizligi tamoyillari muvaffaqiyatli axborot xavfsizligi yondashuviga kiritilgan va himoya qilinishi kerak bo'lgan kompyuterlar, tarmoqlar, dasturlar yoki ma'lumotlarni qamrab oluvchi ko'p qatlamli himoya ko'rinishida ifodalangan[1]. Odamlar, ish oqimlari va texnologiyalar kiberhujumlardan

[1] The Home Computer Security Centre. (2009, july 10). Onttrek Oct. 29, 2015 uit http://www.lockdown.co.uk: http://www.lockdown.co.uk/?pg=password_guide available under a Creative Commons Attribution-ShareAlike 2.0 License.

samarali himoya qilish uchun tashkilotlarda bir-birini to'ldirishi kerak. Foydalanuvchilar kuchli parollarni tanlash, elektron pochta qo'shimchalaridan ehtiyot bo'lish va ma'lumotlarni zaxiralash kabi asosiy axborot xavfsizligi tamoyillarini tushunishlari va ularga rioya qilishlari kerak. Tashkilotdagi axborot xavfsizligi jarayonlari axborot va elektron muhitdan tashqaridagi xakerlarning muvaffaqiyatli hujumlariga qarshi kurashish uchun muvaffaqiyatli va samarali asosiy chora-tadbirlar majmuasi sifatida ishlab chiqilishi kerak. 1-jadvalda zamonaviy axborot xavfsizligi tahdidlarining turlari keltirilgan. Ushbu chora-tadbirlar to'plami hujumlarni qanday aniqlash, tizimlarni himoya qilish, tahdidlarni aniqlash, ularga qarshi kurashish va hujumlardan qanday qutulishni tushuntirishga yordam beradi. Axborot xavfsizligi texnologiyalari tashkilotlar va shaxslarni kiberhujumlardan himoya qilish uchun zarur vositalar bilan ta'minlaydigan muhim element hisoblanadi. Himoya qilinishi kerak bo'lgan asosiy komponentlar kompyuterlar, aqlli qurilmalar va routerlar kabi so'nggi, zamonaviy qurilmalardir: tarmoqlar va bulutli dasturlar kabilar. Ushbu komponentlarni himoya qilish uchun ishlatiladigan eng keng tarqalgan texnologiyalar qatoriga yangi avlod xavfsizlik dasturlari, DNS filtrlash, zararli dasturlarga qarshi dasturlar, antivirus dasturlari va elektron pochta xavfsizligi yechimlari kiradi.

Kiber tahdidlar	Tavsiflari
Ijtimoiy muhandislik yo'llari	Ijtimoiy tarmoqlardagi do'stlardan pochta jo'natmalari, kompyuterni viruslar uchun tekshirish yoki dasturlarni so'nggi versiyalarga yangilash taklifi bilan "onlayn tizim tekshiruvi yoki dasturiy ta'minotni yangilash" soxta sahifalari orqali amalga oshiriladi.
“Day Zero”	“Day Zero” dasturiy ta’minot ishlab chiquvchilari tomonidan aniqlangan vaqtga ishora qiladi. “Day Zero” - bu brauzer yoki dasturda foydalanish mumkin bo'lgan dasturdagi xavfsizlik xatosi orqali amalga oshiriladi.

Fishing (farming)	Internetdagi firibgarlikning bir turi, uning maqsadi foydalanuvchining maxfiy ma'lumotlarini olishdir. Bunga parollar, raqamlar va kredit kartalari ma'lumotlari, bank hisoblari va boshqa maxfiy ma'lumotlarni o'g'irlash kiradi. Fishing - bu banklar, provayderlar, to'lov tizimlari va boshqa kompaniyalardan pochta orqali yuboriladigan soxta bildirishnomalar yoki hisob-fakturalar bo'lib, ular qandaydir sabablarga ko'ra qabul qiluvchi zudlik bilan shaxsiy ma'lumotlarini uzatishi yoki yangilashi kerak.
Rivojlangan doimiy tahdidlar	Mavjud tahdidlarning doimiy rivojlanishi virus dasturida ma'lum bir kodni o'zgartirishning eng keng tarqalgan usullaridan biridir va shuning uchun uni antivirus tahdid sifatida aniqlamaydi. Zararli dastur ishlab chiquvchilari bunday tahdidlarni yangilash uchun kamroq kuch sarflashadi.
Mobil qurilmalar	Mobil qurilmalar va planshetlarda ko'proq xizmatlar va reklamalar joriy etilayotganligi sababli zararli reklamalarning paydo bo'lishi holatlari, ya'ni ularni qonuniy onlayn reklama tarmoqlariga yuklash amaliyoti sezilarli darajada ko'paymoqda.
Bulut texnologiyalar	Bulutli hisoblash, tizim resurslaridan ommaviy foydalanish tufayli, foydalanuvchi ma'lumotlarini bir-biridan ishonchli himoya qilishni talab qiladi. Xavfsiz bulutli hisoblash tizimida uzatiladigan va saqlanadigan ma'lumotlar bulutli hisoblash tizimining turli darajalarida yuzaga kelishi mumkin bo'lgan zaifliklardan foydalanish natijasida xavfsizlik qoidalari va jarayonlarini chetlab o'tish orqali buzilishi yoki soxtalashtirilishi mumkin.

1- jadval. Kiber tahdid turlari

Kibermakon - bu kiberob'ektlar ishlaydigan va o'zaro ta'sir qiladigan makon.

Ob'ektning kiberxavfsizligi - bu uning kibermakonga zarar yetkazmaslik qobiliyatini tavsiflovchi xususiyati.

Shu bilan birga, biz “kiber tahdid” yoki “axborot xavfsizligi” deganda, nima xavf ostida ekanligini hamma juda yaxshi tushunadi. Biroq, bu aniq ravishda qonun bilan belgilanmagan.

Mavjud "Axborot xavfsizligi" tushunchasi ma'lum printsiplar bilan himoyalanishi kerak bo'lgan ma'lumotlar to'plamidir: yaxlitlik, maxfiylik, mavjudlik. Masalan, ma'lumotlarning maxfiyligini buzmaydigan virus hujumi bo'lishi mumkin. Ammo troyan virusi bo'lishi mumkin - bu shunchaki korporativ dasturiy ta'minot va soatlarga kirib boradi. Va shu nuqtai nazardan, bu to'siqni anglatmaydi - chunki viruslar va xatcho'plar kabi boshqa tahdidlar maxsus belgilanishi kerak.

Kiberjinoyat, ta'rifiga ko'ra, kompyuter yoki tarmoq qurilmasi yordamida noqonuniy harakatni amalga oshiradi. Kiberjinoyatchilar axborot tizimlariga ruxsatsiz kirish uchun murakkab usullardan foydalanadilar[2].

Buzg'unchilar foydalanishi mumkin bo'lgan ijodiy usullardan ba'zilari bu orqa eshik dasturlari, fishing hujumlari va ijtimoiy muhandislikdir. An'anaviy xavfsizlik mexanizmlarini chetlab o'tib, kompyuter tizimlariga ulanish imkonini beruvchi marshrutni o'rnatish uchun ishlatilishi mumkin bo'lgan bir qator mashhur orqa eshik vositalari mavjud, masalan:

- Small, Netcat,
- Rolling,
- exe ishlab chiqaruvchisi,
- Pretator,
- Restorator va Tetris.

[2] Srinath, B. J. Cyber Security Awareness for Protection of National Information Infrastructure. Dept. of Information Technology. Ministry of Communication & Information Technology, Govt. if India. 2006. P.75.

Xakerlarning maqsadlari xodimlarning maxfiy ma'lumotlarini o'g'irlashdan tortib patentlar, intellektual mulk va xavfsizlik bilan bog'liq loyihalar (bu kredit kartalaridan ancha qimmatroq) orqali o'tishgacha.

Axborot tizimlarini himoya qilish doimiy iqtisodiy muammodir. Axborotni (ma'lumotlarni) himoya qilishni ta'minlash xarajatlari qimmat va jiddiydir. Kiberjinoyat hujumlari har yili 100 milliard dollar zarar keltiradi. Ko'p sonli kiberhujum urinishlari universitetlarni axborot tizimlarini mustahkamlashga majbur qilmoqda.

Tashkilotlar o'z aktivlarini, shu jumladan yaratilgan axborot ma'lumotlarini (shartli ma'lumotlar birliklari - ma'lumotlar bazalari), ish stollari, serverlar, binolar va eng muhimi, xodimlarni himoya qilishlari shart. Ma'lumotlar ma'lum bo'lishi kerak bo'lgan holatga ko'ra ajratilishi va tasniflanishi mumkin. Xodimlar va menejerlarning ma'lumotlari (shaxsiy) ommaviy ma'lumotlardan ajratilishi kerak.

Ma'lumotlar tasniflangandan so'ng, kirish nazoratini amalga oshirish uchun xavfsizlik ruxsatnomalari qo'llanilishi mumkin.

Davlatdagi mavjud infratuzilma tizimlarining ojiz nuqtalarining kiberxavfsizligini ta'minlash muammosini hal qilishning o'ziga xos xususiyatlari hozirgi kunda asosiy muammoga aylanib ulgurdi. Oxirgi nuqtalar ish stantsiyalari, serverlar, noutbuklar. Hatto tajovuzkorlar uchun korporativ mobil telefonlar ham aksariyat hollarda juda oddiy va ommabop kirish nuqtalari bo'lib, ularni axborot xavfsizligi xizmatlari tomonidan nazorat qilishning ahamiyatini oshiradi[3].

Muammoning keskinligini mutaxassislar uchun aniq bo'lgan haqiqat yanada kuchaytiradi, chunki murakkab maqsadli hujumlar uchinchi bobda batafsil ko'rib chiqilgan keng tarqalgan tahdidlar va “zero day” zaifliklar, noyob nostandart sxemalar – zararli dasturlardan umuman foydalanmasdan, turli xil "faylsiz" usullar va boshqalarsiz amalga oshirilmaydi. Bugungi kunda aksariyat tashkilotlarning infratuzilmalarida mavjud bo'lgan EPP (Endpoint Protection Peatform) so'nggi nuqtalarni himoya qilish

[3] Singh, G., Sharma, A., Rampal, K., Kular, R., Gupta, S., Sarita, R., et al.. India Risk Survey 2013. Pinkerton and Federation of Indian Chambers of Commerce and Industry (FICCI) 2013. P.124.

platformalari ommaviy, ilgari ma'lum bo'lgan tahdidlardan mukammal himoya qiladi, ammo ular, masalan, kiruvchi ogohlantirish yanada murakkab va xavfli hujumning tarkibiy qismlari bo'lishi mumkinligini aniqlay olmaydilar.tashkilotga katta zarar yetkazishi mumkin. Bu yerda misol sifatida ko'rib chiqilgan muqobil yechimlardan biri bu avvalgi Epp avlodi bilan avtomatik ravishda bog'lanishi kerak bo'lgan EDR (Endpoint Detection and Response) platformalaridir. Ushbu bobda aniq so'nggi nuqtalarga (shu jumladan faylsiz filless hujumlariga) qaratilgan kiber tahdidlarning rivojlanish tendentsiyalari, shuningdek Gamet, Forresher, Radicati Group kabi asosiy EDR yechim platformalarining texnik xususiyatlari va ishlash xususiyatlari batafsil ko'rib chiqiladi.

Faoliyatning turli sohalaridagi ko'plab tashkilotlar uchun tobora dolzarb muammo - bu keng tarqalgan tahdidlar, “zero day” zaifliklar, zararli dasturlardan foydalanmasdan noyob sxemalar, faylsiz usullar va boshqalar kombinatsiyasini tobora ko'proq qo'llaydigan maqsadli hujumlar bilan to'qnashuv ehtimoli. Profilaktik texnologiyalar asosida qurilgan standart echimlardan, shuningdek, faqat tarmoq trafigida murakkab zararli faoliyatni aniqlashga qaratilgan tizimlardan foydalanish korxonani murakkab maqsadli hujumlardan himoya qilish uchun etarli bo'lmasligi mumkin.

Ish stansiyalari, noutbuklar, serverlar va smartfonlarni o'z ichiga olgan so'nggi nuqtalar ham muhim nazorat ob'ektlari hisoblanadi, chunki ular ko'p hollarda tajovuzkorlar uchun juda oddiy va mashhur kirish nuqtalari bo'lib qoladi, bu esa ularni nazorat qilishning ahamiyatini oshiradi. Bugungi kunda aksariyat tashkilotlarning infratuzilmasida mavjud bo'lgan so'nggi nuqtalarni himoya qilish platformalari (Endpoint Protection Platform – EPP) ommaviy, taniqli va bir qator noma'lum tahdidlardan mukammal himoya qiladi, ammo aksariyat hollarda ilgari topilgan zararli dasturlar asosida qurilgan[4].

Vaqt o'tishi bilan kiberjinoyatchilarning hujum texnikasi sezilarli o'zgarishlarga duch keldi. Hujumchilar o'zlarining hujum yondashuvlarida ko'proq tajovuzkor bo'lib,

[4] Rusen, C. A. How to Start & Use The Windows Firewall with Advanced Security. Onttrek Oct. 29, 2015 uit http://www.digitalcitizen.life/gain-additional-control-using-windows-firewall-advancedsecurity available under Creative Commons Attribution-Noncommercial-Share Alike 4.0 International.

jarayonning barcha bosqichlarini tashkil qilishda yanada rivojlangan. Va shuning uchun ko'p sonli kompaniyalar, so'nggi nuqtalarni himoya qilish yechimlaridan (EPP) foydalanishlariga qaramay, hali ham murosaga kelisha olisholmayabdi. Bu shuni anglatadiki, bugungi kunda tashkilotlar ushbu turdagi tahdidlarga qarshi dastlab ishlab chiqilmagan an'anaviy himoya vositalari endi bardosh bera olmaydigan eng yangi, yanada murakkab tahdidlarni samarali aniqlashga yordam beradigan qo'shimcha vositalarga muhtoj. Ushbu himoya vositalari so'nggi nuqtalarda sodir bo'lgan hodisalarni aniqlasa-da, lekin odatda kiruvchi ogohlantirishlar tashkilot uchun muhim zararga olib kelishi mumkin bo'lgan yanada xavfli va murakkab sxemaning tarkibiy qismlari bo'lishi mumkinligini aniqlay olmaydi.

Zamonaviy so'nggi nuqtalarni himoya qilish murakkab tahdidlarning zamonaviy landshaftiga moslashishni talab qiladi va so'nggi nuqtalarga qaratilgan keng qamrovli hujumlarni aniqlash funksiyasini o'z ichiga olishi va topilgan ,,,,,hodisalarga tezkor javob bera olishi kerak. Murakkab tahdidlarga qarshi kurashish uchun EDR (Endpoint Detection and Response – EDR) yechimini joriy etishning kutilayotgan natijasi so'nggi qurilmalarning ilg'or himoyasini tashkil etish bo'ladi, bu esa kompleks maqsadli hujumlar yuzasining sezilarli darajada pasayishiga va shu bilan kiber tahdidlarning umumiy sonining kamayishiga olib keladi.

Sifatli sharhda EDR-ning asosiy texnologiyalari va ularning EPP sinf yechimlari bilan o'zaro ta'sirining xususiyatlari ko'rib chiqiladi. Shubhasiz, turli davlat va tijorat tashkilotlariga qaratilgan muvaffaqiyatli hujumlar haqida e'lon qilingan ma'lumotlar ularning haqiqiy sonining kichik bir qismidir. Ishonch bilan aytish mumkinki, kiberintsidentlar soni va ularning oqibatlari darajasi ommaviy axborot vositalarida bizga taqdim etilganidan ancha yuqori. Masalan, Kasperskiy Lab Global Corporate it Security Risks Survey biznes uchun axborot xavfsizligi xatarlari bo'yicha global tadqiqot davomida to'plangan raqamlar muvaffaqiyatli kiberhujumlar kompaniyalar uchun haqiqatan ham qimmatga tushishini tasdiqlaydi.

Foydalanilgan adabiyotlar:

1. Ahmad Javaid, Quamar Niyaz, Weiqing Sun, and Mansoor Alam. 2016. A deep learning approach for network intrusion detection system. In Proceedings of the 9th International Conference on Bio-inspired Information and Communications Technologies (BIONETICS).

2. Alhazmi, O., Malaiya, Y., Ray, I., 2005. Security Vulnerabilities in Software Systems: A Quantitative Perspective. In: Jajodia, S., Wijesekera, D. (Eds.), Proceedings of the 19th Annual IFIP 660 WG 11.3 Working Conference on Data and Applications Security. Vol. 3654 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, August 7-10, Storrs, Connecticut, USA, pp. 281–294.

3. Arora, A., Krishnan, R., Telang, R., Yang, Y., 2010. An Empirical Analysis of Software Vendors' 670 Patch Release Behavior: Impact of Vulnerability Disclosure. Information Systems Research 21 (1), 115–132.

4. Carayon, P., Duggan, R., & Krae mer, S. (2003). A model of red team performance. In K. J. Zink (Ed.), Seventh International Symposium on Human Factors in Organizational Design and Management. Aachen, Germany.