KIBERXAVFSIZLIK MAQSADLARI

Radjabova Madina Shavkatovna, Mirzanazarov M. Sh
Yusupova S.M, AmonovA.H.
Abdullayev I.K, Bekbayev J.R
Hafizov Sh.F
Toshkent axborot texnologiyalari unversiteti
abdujabbor.madina.1989@gmail.com

Anatatsiya: *Kiberxavfsizlik texnologiyasining murakkab tabiati va kiberxavfsizlik tahdidlari tobora kuchayib borayotganini hisobga olsak, siyosatchilar doimiy ravishda so'nggi tahdidga qanday munosabatda bo'lish bo'yicha qarorlar bilan to'qnash kelishlarini kutish mumkin.*

Kalit so'zlar: *kiberxavfsizlik, tahdid, zaiflik, kiberxavfsizlik sistemagrammasi, xavfsizlik, autentifikatsiya, veb ilovalar.*

Kiberxavfsizlik choralariga oid qarorlar ko'pincha texnologlarga topshirilganligi sababli, siyosatchi bu qarorlar qabul qilinayotganini ko'rmasligi va shu sababli turli xil muqobil yondashuvlarning tashkiliy ta'sirini o'lchash imkoniga ega bo'lmasligi mumkin.

Aslida, kiberxavfsizlik qurollari poygasi ko'pincha juda kam muqobil variantlarni taklif qiladi. Kiberxavfsizlik texnologiyasi joriy etilgandan so'ng deyarli darhol uning qo'llanilishi ba'zi bir tartibga soluvchi organ tomonidan sanoat standarti deb e'lon qilinadi va bu tashkilotlarni aniqlangan qarshi choralar yondashuviga to'sqinlik qiladi. Masalan, agar tartibga solinadigan tashkilot xavfsizlik devorlaridan foydalanmagan kiberxavfsizlik yondashuvidan foydalanishga qaror qilsa, ular tartibga soluvchi auditorlar tomonidan batafsil tekshiruvga duch kelishadi. Kiberxavfsizlik mutaxassislariga tashkiliy yondashuvni qayta ko'rib chiqishdan ko'ra, eng yangi xavfsizlik vositalari va texnologiyalaridan xabardor bo'lishni davom ettirish osonroq ko'rinadi.

E'tibor bering, bu kiberxavfsizlik siyosati maqsadlari o'sha paytda kiberxavfsizlik bo'yicha tashkiliy maqsadlarga mos kelmagan va hozir ham mos kelmasligi kerak. Shunga qaramay, ushbu bobda biz kiberxavfsizlik siyosati maqsadlariga erishilganligini aniqlash uchun foydalanilgan usullarni ham ko'rib chiqamiz. Xavfsizlik maqsadlarini qo'yganlar ko'pincha xavfsizlik maqsadlariga erishish uchun xato qilishlarini kuzatamiz. Biz hozirgi kiberxavfsizlik ko'rsatkichlari xavfsizlikni umuman o'lchamaydi degan xulosaga keldik. Bob kiberxavfsizlik maqsadlari qanday belgilanishi va

kiberxavfsizlik maqsadlariga erishish qanday o‘lchanishi mumkinligini ko‘rsatadigan uchta amaliy tadqiqotlar bilan yakunlanadi.

Kiberxavfsizlik ko‘rsatkichlari

O‘lchov - bu empirik dunyodan rasmiy munosabatlar dunyosiga xaritalash jarayoni hisoblanib, natijalari ko‘rib chiqilayotgan ob’ektning atributini tavsiflaydi.

Tutib bo‘lmaydigan atributga mos keladigan o‘lchovlar kombinatsiyasi olingan o‘lchovlar hisoblanadi va o‘lchanadigan narsaning mavhum modeli konteksida talqin qilinishi kerak (ISO/IEC 2007). Ko‘rsatkichlar umumiy atama bo‘lib, ma’lum bir sohani tavsiflovchi o‘lchovlar to‘plamini anglatadi . Kiberxavfsizlik to‘g‘ridan-to‘g‘ri o‘lchov ob’ekti emas yoki olingan o‘lchovlar yoki ko‘rsatkichlarni osongina aniqlash uchun tizimning yetarlicha tushunilgan atributi.

Shunday qilib, kiberxavfsizlik ko‘rsatkichlari bilan shug‘ullanuvchilar boshqa narsalarni o‘lchaydilar va ulardan xavfsizlik maqsadlariga erishish haqida xulosa chiqaradilar. Ushbu muammo xavfsizlik ko‘rsatkichlari deb nomlangan tadqiqot sohasini yaratdi (Jaquith and Geer 2005). Jismoniy xavfsizlik ko‘rsatkichlari an’anaviy ravishda tizimning dizayn tahdidiga (DBT) qarshi turish maqsadiga erishish qobiliyatiga qaratilgan (Garsia 2008). DBT eng kuchli va innovatsion raqibning xususiyatlarini tavsiflaydi, undan himoya qilishni kutish mumkin.

Nyu-York shahrida bu murakkab aloqa vositalari va portlovchi qurilmalar bilan jihozlangan terrorchi shaxs bo‘lishi mumkin. Aydaxoda bu mototsikllarda avtomatik hujum qurollarini olib yurgan 20 kishilik bezorilar bo‘lishi mumkin. Xavfsizlikka DBT yondashuvini qabul qilish tizim tomonidan talab qilinadigan xavfsizlikni himoya qilishning kuchini uning qanday hujumga uchrashi mumkinligining texnik tavsifiga qarab hisoblash kerakligini anglatadi. Jismoniy xavfsizlikda bu jarayon oddiy. Agar DBT ma’lum turdagi portlovchi moddalarga ega bo‘lgan 20 kishidan iborat bo‘lsa, unda ruxsatsiz kirish uchun jismoniy to‘siqlarning kuchi ushbu 20 kishi qo‘llashi mumkin bo‘lgan tonna kuchga bardosh berishi kerak .

Kiberxavfsizlik sistemagrammalarini tushunish

To‘siqni himoya qilish materiallari ko‘rsatilgan, tahdidni kechiktirish va javob berish tizimlari ishlab chiqilgan va shunga muvofiq tekshirish sinovlari o‘tkaziladi. Kiberxavfsizlikda quyidagi atamalari mavjud:

- Jinoyatchi;
- Tahdid;
- Ekspluatatsiya;
- Zaiflik .

Bu atamalari savdo shartlari bo‘lib, ularning ma’nosi alohida va o‘zaro bir biriga bog‘liqdir. 1- rasmdagi sistemagrammada ko‘rsatilganidek, jinoyatchi jismoniy yoki yuridik shaxsdir.

Tahdid - bu jinoyatchi tomonidan sodir etilishi mumkin bo‘lgan yoki amalga oshirilmasligi mumkin bo‘lgan potentsial harakat. Ekspluatatsiya hujumni o‘z ichiga olgan texnik tafsilotlarga ishora qiladi.

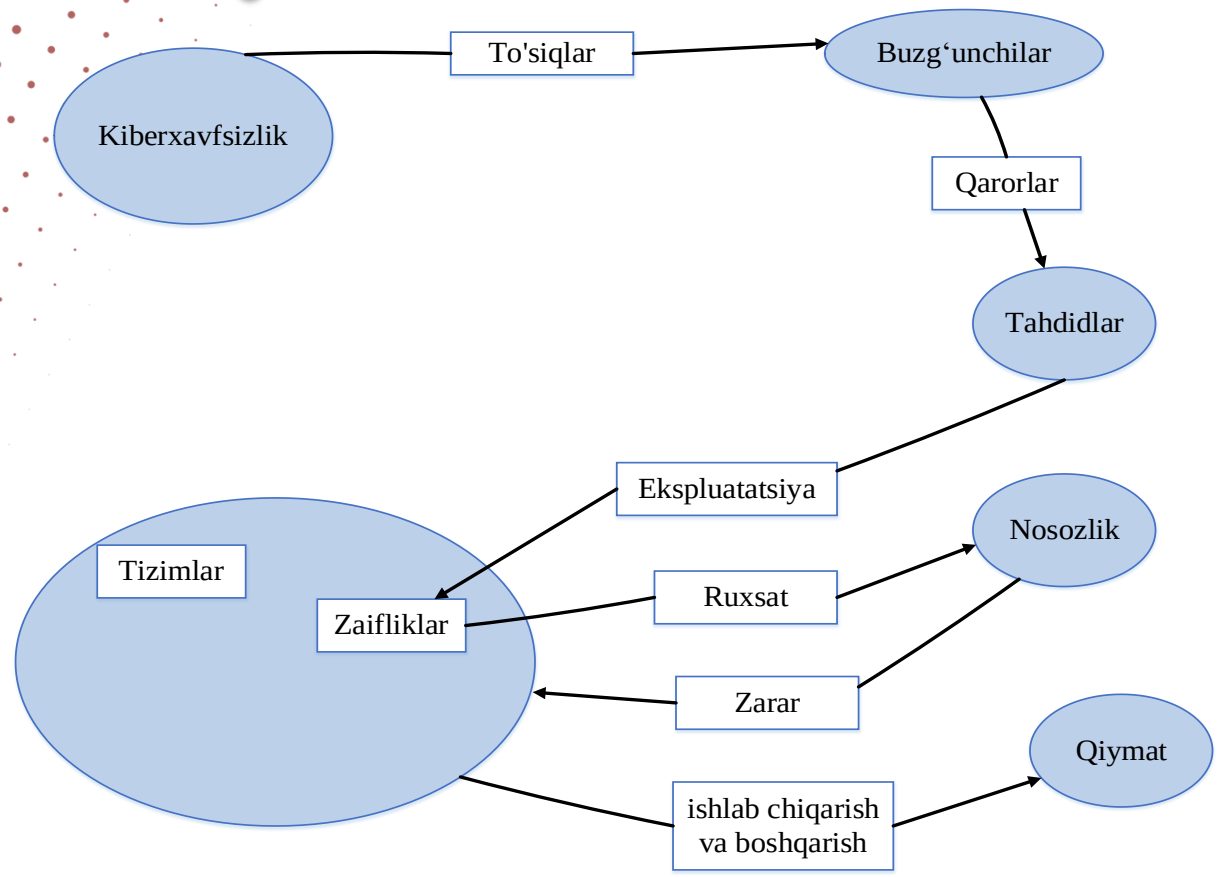
Zaiflik - bu ekspluatatsiyaning muvaffaqiyatli bo‘lishiga imkon beruvchi tizim xarakteristikasi.

Shunday qilib, 1-rasmdagi sistemagrammaning asosiy tayanchi shunday o‘qiladi: “Xavfsizlik tizim zaifliklaridan foydalanib, qiymatga salbiy ta’sir ko‘rsatadigan zararni keltirib chiqaradigan tahdidlarni amalga oshiradigan jinoyatchilarni to‘xtatadi” (Bayuk , Barnabe et al. 2010).

Kompyuter tizimlari paydo bo‘lganidan beri, kompyuter xavfsizligi uchun DBTlar potentsial jinoyatchilarni, masalan, joyriderlar, kiber yo‘q qilishning zararli agentlari va josuslik agentlari ko‘rinishidagi xakerlarni ko‘rib chiqdilar.

Biroq, DBTning jismoniy xavfsizligini tahlil qilishdan farqli o‘laroq, tahdidga javoban ishlab chiqilgan qarshi choralar tahdid ishtirokchilarining o‘ziga va ularning eng so‘nggi taktikalari qanday bo‘lishi mumkinligiga emas, balki eng so‘nggi tahdidni amalga oshirish uchun foydalanilgan texnologiya zaifliklariga e’tibor qaratdi.

Tizim zaifligining har bir turi xavfsizlik bo‘yicha hamjamiyat xabardor bo‘lish bosqichiga yetganligi sababli, bozorga xavfsizlikka qarshi choralar ko‘rish bo‘yicha tegishli texnologiyalar to‘plami paydo bo‘ldi va tobora ortib borayotgan eng yaxshi amaliyot tavsiyalarining bir qismiga aylandi.

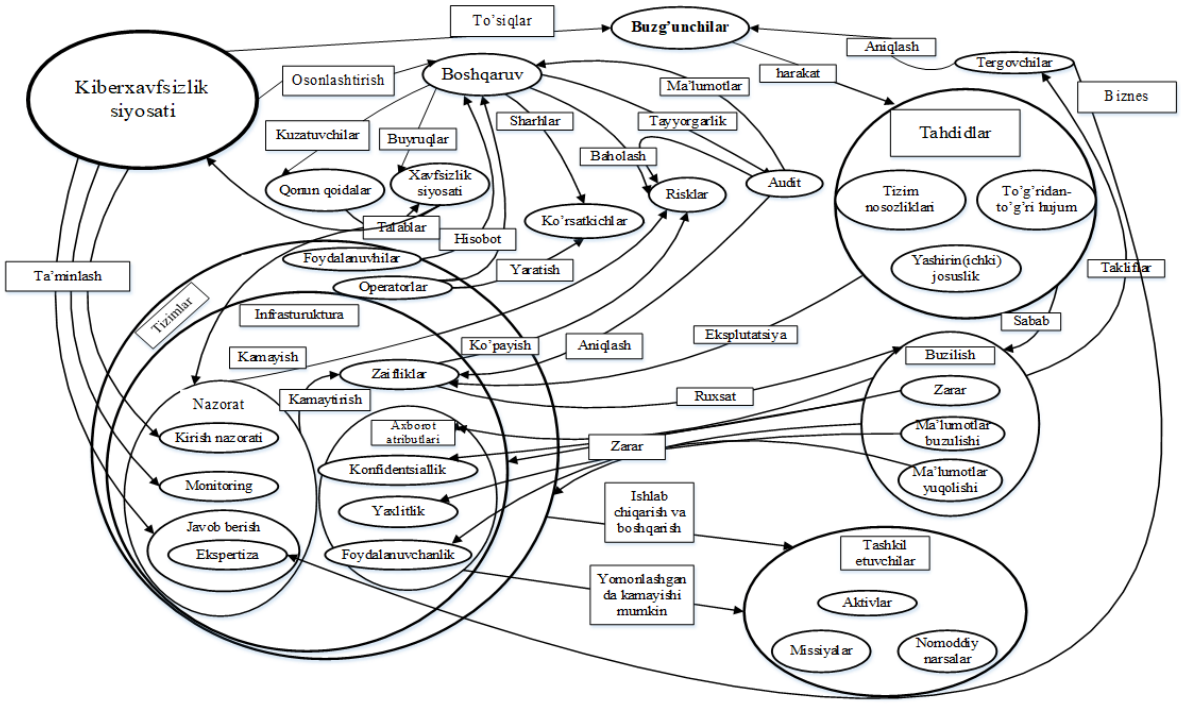


1-rasm. Kiberxavfsizlik sistemagrammasi.

Tizimning zaif qismlariga qarshi choralar qo‘llanildi va tizimlarga tahdidlar ularning barchasini amalga oshirishning umumiy natijasi bilan qoplanadi deb taxmin qilingan. 2-rasmda ushbu tushunchalar va ular o‘rtasidagi munosabatlar 1- rasmdagi sistemagrammaga qo‘shilgan holda ushbu yondashuv tasvirlangan.

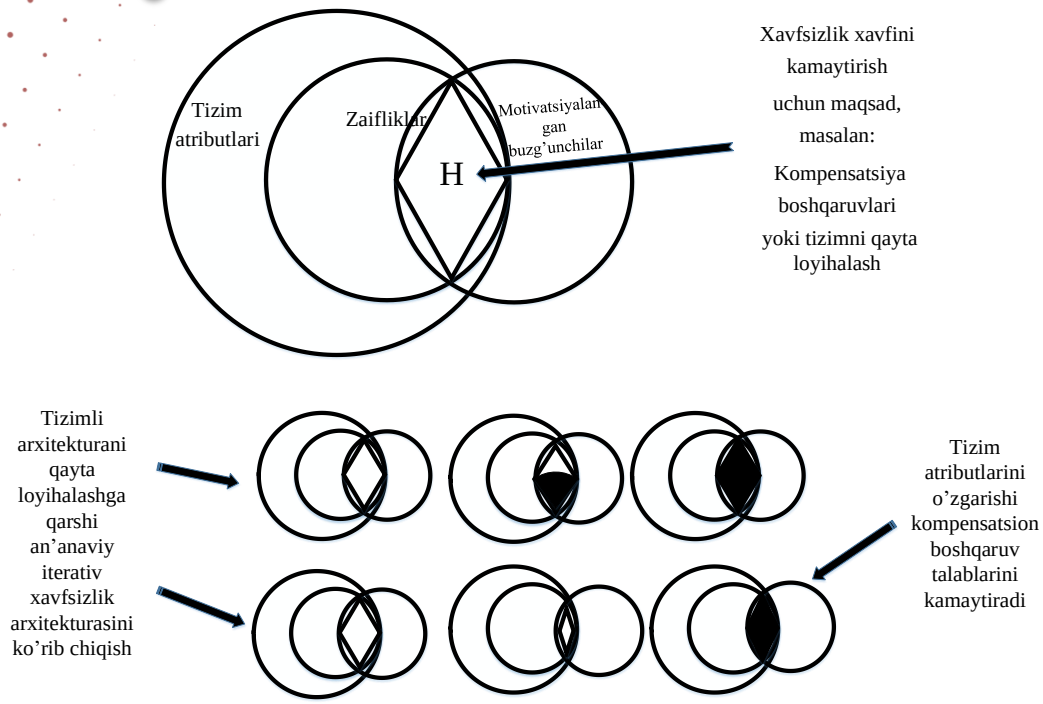
2-rasmda kiberxavfsizlik ko‘rsatkichlari, boshqaruv yondashuvlari, auditlar va tergov usullari xavfsizlik vositalari va usullariga asoslanganligini ko‘rsatadi.

Xavfsizlik maqsadlariga qarshi choralar texnologiyasi bilan erishilishi haqidagi konsensus tizim dizaynining bir qismi sifatida DBTlarga murojaat qilish hisobiga keladi. 3-rasmda xavfsizlik arxitekturasiga ushbu an’anaviy yondashuv va tizim darajasidagi yaxlit yondashuv o‘rtasidagi farq ko‘rsatilgan



2-rasm. To‘liq sistemagramma

Boltonlar, ta’rifiga ko‘ra, tizimning o‘ziga tegishli bo‘lmagan, masalan, 1-bobda tasvirlangan xavfsizlik devorlari bo‘lgan ishlov berish vositalaridir. 3-rasmning pastki qismida xavfsizlik muammolarini hal qilishda muruvatli yondashuv va xavfsizlik dizayni o‘rtasidagi ziddiyat tasvirlangan. zaiflikni yo‘q qilish yoki kamaytirish uchun tizim darajasidagi atributlarni o‘zgartirishi kutilayotgan yondashuv. Agar ushbu yondashuv birinchi bo‘lib sinab ko‘rilsa, xavfsizlikka oid kompensatsiya boshqaruvlari soni minimal bo‘lishi kerak. Shunga qaramay, 1-bobda ta’riflanganidek, xavfsizlik texnologiyalari ro‘yxati deyarli ongsiz ravishda qabul qilingan ko‘rinadi. Buning ta’siri shundaki, xavfsizlik maqsadlarining odatiy taqdimoti biznes sohasi va kompyuter operatsion tizimi tomonidan sanab o‘tilgan xavfsizlik texnologiyalarini joriy etish jarayonini ko‘rsatadi. 4-rasm odatiy misoldir. Odatda bu ko‘rsatkichga hamroh bo‘ladigan tahlilda marketing biznesi sohasi moliya sohasi kabi xavfsizlikka ega emasligi marketingning moliyaga nisbatan yuqori xavf-xatarlarga chidamliligi bilan izohlanishi mumkin.



3.3-rasm. Bolt bilan bog‘langan dizayn.
Xavfsizlikni boshqarish maqsadlari

Ko‘pgina rahbarlarda xavfsizlik uchun "Men xavfsiz bo‘lishni xohlayman" degan fikrdan boshqa aniq maqsad yo‘q. Bunday hollarda maqsadning shunday bir elementi borki, uni to‘liq ifodalash odatda shunday bo‘lishi mumkin: "Men o‘z tashkilotimga juda kam yoki umuman ta’sir qilmasdan xavfsiz bo‘lishni xohlayman". Ular ushbu ko‘rsatmani xavfsizlik bo‘yicha mutaxassislarga, xuddi shunday qilib, balans boshqaruvini buxgalteriya xodimlariga topshirib, “Men raqamlar aniq bo‘lishini xohlayman” deb berishadi. Huquqiy va me’yoriy hujjatlarga rioya qilish zarurati bilan bog‘liq ikkita kasbdagi o‘xshashliklarni chetga surib qo‘ysak, delegatsiya ijrochi delegatlar topshirilgan masalalarni tushunadigan va biznesdagi barcha odamlar bilan yaqindan hamkorlik qila olishiga ishonishadi. Ijro hokimiyati-maqsadiga erishish uchun topshirilgan funktsiyalardan manfaatdor tomonlar hisoblanadi.

Biroq, buxgalterlik kasbi bir necha ming yillik tarixga ega bo‘lib, uning ishonchni vaziyatlar va sanktsiyalar kombinatsiyasini o‘z ichiga olgan munosabatlar nuqtai nazaridan aniqlash qobiliyatini qo‘llab-quvvatlaydi.

(Ginnane 2005). Aksincha, kiberxavfsizlik kasbi atigi yarim asr yoki birinchi sanoat yoki milliy xavfsizlik standartlari paydo bo‘lganidan beri, xalqaro xavfsizlik standartlari paydo bo‘lganidan beri ancha kamroqdir (kichik namunaga DoD 1985; ISO/IEC 2005 a,b); FFIEC 2006; Ross, Katzke va boshq. 2007; PCI 2008). Bundan tashqari, har qanday kelishilgan sanoat standartidan ko‘ra, masalan, buxgalteriya hisobining umumiy kelishilgan buxgalteriya hisobi tamoyillari (GAAP), kiberxavfsizlikda juda ko‘p raqobatdosh standartlar

mavjudki, ularni kataloglash va taqqoslash uchun biznes tashkil etilgan (UCF davom etmoqda). Mahsulot elektron jadval yoki boshqa tuzilgan ma'lumotlar formatida yetkazib beriladi. U xavfsizlik ma'lumotlarini boshqarish (SIM) tizimiga import qilinishi uchun mo'ljallangan va u xavfsizlik menejeriga ularning barchasini o'qib chiqmasdan turib bir nechta standartlarga muvofiqligini ko'rsatish imkonini beradi. Normativ-huquqiy hujjatlarga muvofiqlik asosida ishlab chiqilgan xavfsizlik dasturlari xavfsizlik bo'yicha tashkiliy maqsadlarga erishish uchun maxsus ishlab chiqilmagan, balki xavfsizlikni boshqarish standartlariga muvofiqligini namoyish qilish uchun mo'ljallangan. Shunday qilib, standartlarning o'zi tashkilot chegaralarini kesib o'tuvchi de-fakto xavfsizlik ko'rsatkichlari taksonomiyalariga aylandi.

Amaliyotchilarga ko'pincha o'z ko'rsatkichlarini xavfsizlikni boshqarish standartlaridagi talablar atrofida tartibga solish tavsiya etiladi, ular tekshirilishi mumkin. Xavfsizlik ko'rsatkichlarini yaratish uchun xavfsizlikni boshqarish standartlaridan foydalanishning xalqaro standarti ham mavjud (ISO/IEC 2009b).

Xavfsizlikni boshqarishga yondashuvning bunday turining kamchiliklari shundaki, standartlarga muvofiqlik tafsilotlari xavfsizlik bo'yicha korporativ maqsadlarni aks ettirish uchun mo'ljallangan ko'rsatkich kartasidan farqli o'laroq, oldindan o'rnatilgan ko'rsatkichlar kartasiga solishtiriladigan izolyatsiya qilingan texnologiya konfiguratsiyasi sifatida ko'riladi.

Ushbu standartlarning hech biri tahdidlarni bartaraf etishda erishish nuqtai nazaridan xavfsizlikni bevosita o'lchashning umumiy qabul qilingan usulini o'z ichiga olmaydi (King 2010). Ular odatda xavfsizlikni ta'minlashi kerak bo'lgan faoliyatni o'rnatishda rahbariyatning tegishli sinchkovlik bilan harakat qilganligini ta'minlash uchun ishlatiladi, bu faoliyat samarali bo'lganligini o'lchash uchun emas. Buni oddiy odamlarning xavfsizlikka nisbatan qarashlari bilan taqqoslang. Masalan, ish joyini o'zgartirgan shaxslar ba'zan eski va yangi firmalardagi xavfsizlikni muhim ma'lumotlar va ma'lumotlarga mahalliy va masofadan kirish qiyinligi darajasiga qarab o'lchaydilar. Misol uchun, ular ofisdagi mijozlar ma'lumotlariga kirish uchun uyda ish stollaridan foydalanishlari kerak bo'lgan parollar sonini aniqlashlari va ularni ko'proq autentifikatsiya qilish omillaridan foydalanishga majbur qiladigan firma xavfsizroq ekanligiga qaror qilishlari mumkin. 4-rasmda tizim xavfsizligining ushbu turdagi qatlamli mudofaa tasviri ko'rsatilgan. Bunday qatlam ko'pincha chuqurlikdagi mudofaa deb ataladi. Bu atama xavfsizlik boshqaruvlari qatlamli va ortiqcha bo'lgan arxitekturani anglatadi va tizimning bir qismidagi zaiflik boshqasi tomonidan qoplanadi.

Ya'ni, hech bir boshqaruv elementi bitta nosozlik nuqtasini ko'rsatmasligi kerak, chunki buzg'unchi kirishi uchun kamida ikkita boshqaruv elementi sinishi kerak. Diagrammaning markaziy pastki qismida tasvirlanganidek, u bir nechta xavfsizlik "qatlamlariga" ega. Diagrammaning yuqori qismida "Masofadan foydalanish" foydalanuvchisi korxona tomonidan boshqarilishi yoki bo'lmasligi mumkin bo'lgan ish stantsiyasini autentifikatsiya qilish uchun zarur bo'lganligi tasvirlangan.

Keyin foydalanuvchi Internet orqali korporativ tarmoqqa autentifikatsiya qiladi. Tarmoqqa kirish nuqtasidan masofaviy foydalanuvchi ichki tarmoqdagi boshqa qatlamlarning istalganiga to'g'ridan-to'g'ri autentifikatsiya qilishi mumkin. Shuning uchun masofaviy kirish odatda yuqori darajadagi xavfsizlikni talab qiladi, chunki ichki tarmoqqa kirgandan so'ng platformaga kirish uchun turli xil variantlar mavjud.

Ushbu masofaviy kirish yo'li 4-rasmda veb-ilovaga kirish yo'liga qarama-qarshidir. Veb-ilovaga kelsak, qatlamlarning mavjudligi aslida chuqur himoyani tashkil etmaydi. Buning sababi shundaki, Internetga kirish mumkin bo'lgan bunday ilovalar odatda bitta tizimga kirish orqali mavjud.

Veb-ilova yo'li shuni ko'rsatadiki, Internet foydalanuvchilari odatda korxona tomonidan boshqarilmaydigan o'zlarining ish stantsiyalariga autentifikatsiya qiladilar. Keyin foydalanuvchi tarmoqqa autentifikatsiya qilmasdan dasturga kirishi mumkin, chunki xavfsizlik devori Internetdagi har bir kishiga veb-serverdagi ilovaning kirish ekraniga to'g'ridan-to'g'ri kirish imkonini beradi.

Shuningdek, serverning operatsion tizimida autentifikatsiya qilishning hojati yo'q. Ilova ichida bir marta ma'lumotlar autentifikatsiya qatlami foydalanuvchiga ko'rsatilmaydi; ilova avtomatik ravishda foydalanuvchi nomidan unga ulanadi. Ushbu qulayliklar rasmda masofaviy foydalanuvchi o'tish uchun autentifikatsiya qilishi kerak bo'lgan qatlamlar orqali ko'priklar sifatida tasvirlangan, ammo dastur foydalanuvchisi buni qilmaydi. Demak, bu ishda mudofaa atamasini chuqur qo'llash noto'g'ri bo'ladi. Zarur bo'lgan texnologiyani har bir qatlamdagi har bir qulf kaliti bo'lmagani uchun aslida yopiq bo'lishini ta'minlash uchun bir nechta qurilmalar muvofiqlashtirilgan holda sozlanishi kerakligi aniq. Shunday qilib, xavfsizlik ko'rsatkichlari bo'yicha ko'plab adabiyotlarda maqsad ushbu qatlamlarning barchasini to'g'ri konfiguratsiya qilish deb taxmin qilinadi (Hayden 2010). Biroq, bu taxminga qaramay, xavfsizlik ko'rsatkichlari uchun standart taksonomiya mavjud emas.

Bunday tasniflashda foydalaniladigan tamoyillar turli tadqiqotchilar tomonidan tadqiq qilingan va bu izlanishlar turli natijalar bergan.

Xulosa

Xulosa o'rnida shuni ta'kidlash kerakki, zamonaviy virtual olamda kiberxavfsizlik tushunchasiga bo'lgan e'tibor kundan-kunga ortib bormoqda. Bunga nafaqat bir foydalanuvchining kibermakondagi xavfsizligi, balki biror-bir korxona yoki tashkilot va hattoki, butun davlat miqyosidagi kiberxavfsizlik ham kiradi. Internet olamida xavfsizlikni taminlash foydalanuvchi va virtual makon orqasidagi har bir vosita bilan o'zaro kombinatsion tarzda bog'liq hisoblanadi. Bu bog'liqliklarning mukammal sistemagarammasini o'rgangan holda kiberxafsizlikni taminlash kerakdir.

FOYDALANILGAN ADABIYOTLAR:

- S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma. – T.: «Aloqachi», 2020, 221 bet.
- Cyber Security Policy Guidebook
- Jennifer L. Bayuk Independent Cyber Security Governance Consultant Industry Professor at Stevens Institute of Technology, Hoboken
- NJ Jason Healey Director of the Cyber Statecraft Initiative Atlantic Council of the United States, Washington
- D.C. Paul Rohmeyer Information Systems Program Director Howe School of Technology Management Stevens Institute of Technology, Hoboken