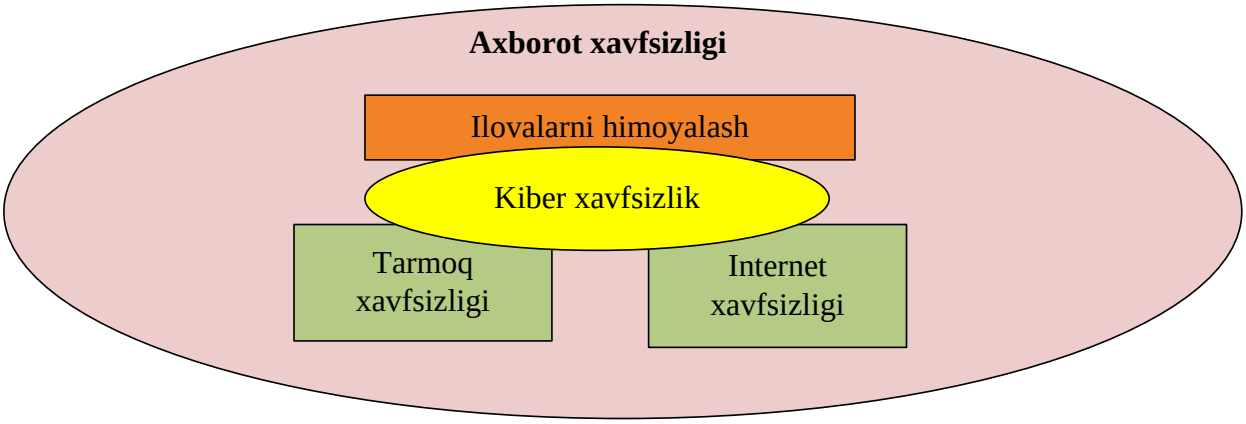
2-TOM, 5-SON

AXBOROTNI HIMOYALASHNING REAKTIV VA PROAKTIV TEXNOLOGIYALARI

Jumayev Ulug'bek
Termiz davlat universiteti Kompyuter tizimlari va ularning dasturiy ta'minoti 1-kurs magistranti

Axborot-kommunikantsion tarmoqlarda saqlanadigan, qayta ishlanadigan va uzatiladigan axborotlarning xavfsizligini ta'minlash dolzarb masalalardan hisoblanadi. Ularning xavfsizligini ta'minlashda dastlab axborotni himoyalash texnologiyalarini to'g'ri tanlashga asoslanadi. Muhim obyektlarda axborot xavfsizligining tashkil etuvchilari quyidagi rasmda keltirilgan bo'lib, u to'laligicha axborot xavfsizligini ta'minlashga qaratilgan.



Muhim obyektlarda axborot xavfsizligining tashkil etuvchilari

Axborotni himoyalashning ikki turdagi texnologiyasi mavjud: *proaktiv va reaktiv*.

Proaktiv himoya texnologiyalari. Odatda antivirus texnologiyalarida qo'llaniladi. Uning asosiy maqsadi foydalanuvchi kompyuterlari va axborot tizimini zararlanishdan himoyalash. Reaktiv himoyalash texnologiyasidan asosiy farqi ham aynan mana shu holatda, ya'ni u tizimdan zararkunanda dasturlar va ilovalarni qidirishga qaratilmagan. So'rov tizimga qaratilgan va uni buzishga doir harakatlari mavjudligi aniqlansa, unga qarshi choralarni ko'radi. Uning kamchiliklari sifatida qonuniy dasturiy ulanishlarni yolg'ondan xabarlari orqali bloklashi hisoblanadi. Proaktiv himoya texnologiyalari quyidagi usullar asosida amalga oshiriladi:

Evristik analiz: ushbu usul dasturiy ta'minotning kodi, skripti va makrorlarini o'rganish asosida unda tahdid holatlari mavjudligi tekshiriladi. Analizatorning sezuvchanlik qobiliyatiga bog'liq holda yolg'ondan zararkunanda deb toppish holatlari ko'p uchraydi.

Bundan tashqari, buzg'unchilar tomonidan evristik tahlilni aylanib o'tish yo'llari ishlab chiqilgan.

Kodni emulyatsiyalash: dasturiy ta'minot emulyatsiya sohasida ishga tushiriladi. Emulyatsiya sohasi operatsion tizimdan ajratilgan xavfsiz joy hisoblanadi. Dastur dastlab emulyatsiya sohasida ishga tushiriladi va unda buzg'unchilik holatlari mavjud emasligi tekshiriladi. Uning asosiy kamchiligi hisoblash mashinalaridan ko'p eneregiya va resurs talab qiladi. Zamonaviy zararkunanda dasturlar emulyatsiya sohasini aniqlash imkoniyatlariga ega va ushbu sohada o'z faoliyatini to'xtatib turadi.

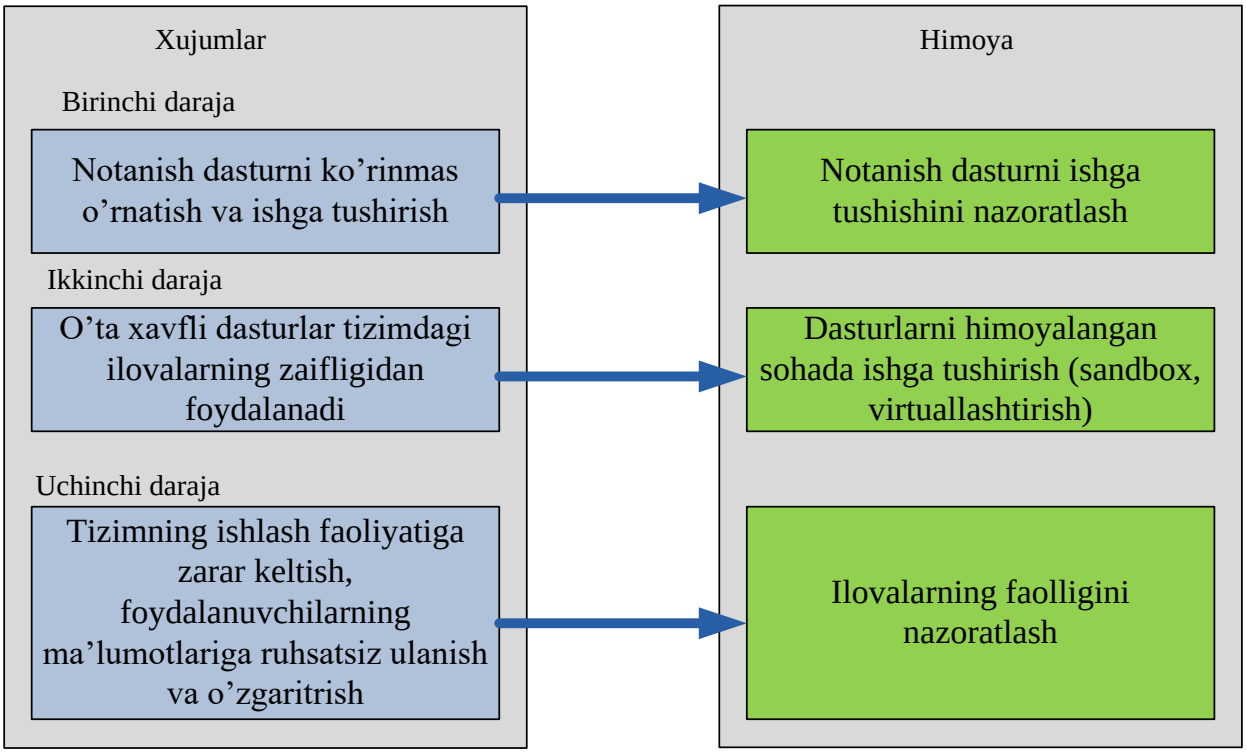
Harakatlarni tahlillash: tizimda ishlayotgan barcha jarayonlarni ushlab qoladi va uning hususiyatidan kelib chiqib harakatlarini tahlo qiladi. U yagona tahlil bo'lmay dasturning oldingi, hozirgi va keyingi harakatlarini tahlillash natijasida zanjiriy xulosani qabul qiladi. Uning bu usuli zararkunanda hoalatlarni aniqlash va bartaraf etishga qaratilgan. Harakatlarni tahlillashga asoslangan bloklash daturlaridan HIPS — Host-based Intrusion Systems ni keltirish mumkin.

Bajarish huquqlarini cheklash (Sandboxing): dasturlarning ishlashi davomida zararkunanda holatlari aniqlansa, uni ish faoliyati tezda to'xtatiladi. Unda dastur o'z huquqidan kelib chiqib foydalanishi mumkin bo'lgan fayllari, kutubxonalari, tizimli kataloglari tekshiriladi. Uning ruhsati mavjud fayllari ro'yhati tekshiriladi, agar ruhsatsiz foydalanish holatlari yuzaga kelsa, tezda uning ishlash faoliyati to'xtatiladi. Sandboxing dasturlari zamonaviy zararkunanda dastularni oldini olishda samarali vosita hisoblanadi, ammo foydalanuvchidan axborot xavfsizligi bilimlarini talab etadi. Chunki dastur qonuniy holatlarni ham noto'g'ri deb topishi mumkin.

Ish sohasini virtuallashtirish: operatsion tizimning tizimli fayllaridan foydalangan holda, qattiq diskdan uning boshqa sohasiga o'tishi mumkin bo'lmagan alohida qism ajratadi. Hattoki foydalanuvchining o'zi ham zararkunda dasturlarni ushbu sohada ishga tushirib, testlashi mumkin. Bunda barcha zarar holatlari virtual sohada yuzaga keladi. Asosiy xotira va tizimga zarar tegmaydi. Uning asosiy kamchiligi o'qish huquqini beruvchi zararkunanda dasturlardan yetarli himoyani ta'minlay olmaydi. Chunki virtual sohadan qattiq diskka fayllarni o'qish uchun murajaatni amalga oshirish mumkin. Bu esa, konfidensial axborotlarga zarar keltiradi.

Ushbu himoya texnologiyalari ko'pchilik zararkunanda dasturlarni aniqlash qurilmalari – antiviruslarda mavjud va asosiy himoya yo'nalishlaridan hisoblanadi. Antivirus dasturlari bir vaqtning o'zida bir nechta proaktiv himoyalash texnolgoiyalaridan foydalanishi mumkin. Masalan: evristik tahlil va kodlarni emulyatsiyalash. Bu esa, yangi va xavfli zararkunanda dasturlarni aniqlashga ko'mak berishi bilan farqlanadi. Antivurslardan

o'rnatilgan bajarish huquqlarini cheklash texnologiyasi dasturlarning harakati asosida zararli holatlarni aniqlab, foydalanuvchiga xabarlar chiqaradi.



Proaktiv himoya texnologiyasining sxemasi

Reaktiv yoki signaturali himoyalash texnologiyalari: ko'pchilik antivirus va buzg'unchiliklarni aniqlash tizimlarida qo'llaniladi. Zararkunanda holatlar mavjud fayllar va paketlar dasturiy ta'minot egasi tomonidan to'planadi va tizimga kirib kelgan fayl va paketlar tizimda mavjudlari bilan tahlillanadi. Taqqoslash zararkunanda dasturlarda qo'llaniladigan kalit so'zlarga asoslanadi. Dastur tomonidan aniqlangan zararkunanda fayllarga nisbatan quyidagi harakatlar amalga oshiriladi:

– zararli va zararlangan faylni o'chirish;

– faylni karantinga jo'natish (ushbu fayl mavjud dastur o'z ishini davom ettira olmaydi. Foydalanuvchining qarori asosida u o'chirilishi yoki qayta tiklanishi mumkin);

– fayl tarkibidan zararli kodlarni tozalab, uni qayta tiklash.

Faylni tekshirish e-mail pochtalar va boshqa xabarlarni almashish tizimlari orqali kelgan fayllarni tahlillashga asoslanadi. Fayl operatsion tizimda ishga tushirilishidan oldin uning tarkibi zararkunanda dasturlarning lug'ati yordamida tekshiriladi.

Foydalanilgan adabiyotlar ro'yhati

1. O'zbekiston Respublikasi Prezidentining farmoni. O'zbekiston Respublikasini yanada rivojlantirish bo'yicha Harakatlar strategiyasi to'g'risida. 2017 yil.

2. Villeneuve N., Bennett J. Detecting apt activity with network traffic analysis //Trend Micro Incorporated Research Paper. – 2012. – С. 1-13.

3. Vargas J. F. et al. Off-line signature verification based on grey level information using texture features //Pattern Recognition. – 2011. – Т. 44. – №. 2. – С. 375-385.

4. Stallings W. et al. Computer security: principles and practice. – Upper Saddle River (NJ : Pearson Education, 2012. – С. 978-0.

5. Uskov A. V. Information security of IPsec-based mobile VPN: Authentication and encryption algorithms performance //2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. – IEEE, 2012. – С. 1042-1048.

6. Fan K., Li H., Wang Y. Security analysis of the Chap protocol using BAN logic //2009 Fifth International Conference on Information Assurance and Security. – IEEE, 2009. – Т. 2. – С. 467-470.

7. Peltier T. R. Information security fundamentals. – CRC press, 2013.