VII ШЎЪБА. АХБОРОТ ХАВФСИЗЛИГИ. INFORMATION SECURITY.

PYTHON DASTURLASH TILI ORQALI AXBOROT XAVSIZLIGINI TAMINLASH.

Adizova Z.M., Davletov J. K.

Buxoro davlat universiteti, Buxoro, O'zbekiston

Kompyuterlar va biznes tarmoqlaridagi texnik muammolarni bartaraf etish uchun Keylogger dasturlari ishlatiladi. U tarmoqdan foydalanishni kuzatish uchun ham ishlatilishi mumkin, lekin ko'pincha parollarni o'g'irlash kabi zararli maqsadlarda foydalaniladi.

Keylogger virus emas, lekin shunga qaramay u foydalanuvchilar uchun katta xavf tug‘diradi, chunki u tajovuzkorga foydalanuvchining ishini kuzatish imkonini beradi va maxfiy ma’lumotlarni, jumladan, foydalanuvchi parollarini o‘g‘irlashda foydalanishi mumkin.

Siz bunday xavfdan xabardor bo'lishingiz va uni aniqlay olishingiz kerak. Ayg'oqchi dasturlarga qarshi kurashda birinchi qadam FireFox, Safari, Opera va boshqalar kabi muqobil brauzerdan foydalanish bo'ladi. Agar biron sababga ko'ra buni amalga oshirishning iloji bo'lmasa, tizimingizni doimiy ravishda oldini olish, aniqlash uchun choralar ko'rishingiz kerak. va keyloggerlarni olib tashlang. RootKit texnologiyasi bilan birlashganda keylogger tahdidi sezilarli darajada oshishi mumkin, bu sizga keylogger mavjudligini yashirish imkonini beradi. Bundan ham xavflisi troyan yoki keyloggerni o'z ichiga olgan backdoor dasturidir - uning mavjudligi troyan funksiyalarini sezilarli darajada kengaytiradi va foydalanuvchi uchun u xavfli.

Pythonda Windows uchun Keyloggerni loyihalash va avtomatik ishga tushirish uchun kod yoziladi va Keylogger.py nomi bilan C diskka saqlanadi. Keylogger fonda ishga tushadi va barcha ma'lumotlarni "c:\output.txt" jurnali faylida saqlaydi.

Keylogger tayyor bo’lgandan so’ng, biz keyloggerni foydalanuvchidan yashirin va avtomatik ravishda ishga tushirishimiz kerak:

- Windows-ni yuklash...

Bu turli yo'llar bilan amalga oshirilishi mumkin. Masalan, buni bat-fayl yordamida, keyloggerni ishga tushirishni biron bir dasturga bog'lash yoki uni ishga tushirish uchun yozish orqali amalga oshirish mumkin.

Amaliyot shuni ko'rsatadiki, zararli dasturlarni ishlab chiquvchilar (viruslar, troyanlar, josuslik dasturlari) tobora ko'proq RootKit texnologiyalaridan foydalanishni boshlaydilar, bu esa ular yaratgan zararli dasturlarni aniqlash va o'chirishni sezilarli darajada murakkablashtiradi. Ko'pincha foydalanuvchi rejimida funktsiyalarni ushlab turish usullari qo'llaniladi, ammo yaqinda drayverlar yordamida juda samarali dasturlar paydo bo'ldi.

Ma'lumki, bugungi kunda apparat klaviaturalarini chetlab o'tishga imkon beruvchi universal va ishonchli texnika mavjud - bu ekran klaviaturasidan foydalanish va klaviaturadan foydalanmasdan ma'lumotlarni kiritishning boshqa usullari. Shuni ta'kidlash kerakki, eng zamonaviy

Ushbu maqsadlar uchun anti-keyloggerlar o'zlarining o'rnatilgan ekran klaviaturasini o'z ichiga oladi.Uskuna kalitloggerlarini topish, albatta, axborot xavfsizligi xodimlarining ish majburiyatlariga kiritilishi kerak. Shu bilan birga, albatta, apparat keyloggerini o'rnatish ehtimoli ish joyida kiritilgan ma'lumotlarning qiymatiga to'g'ridan-to'g'ri proportsional ekanligini yodda tutish kerak.

XODIMLARNI FACE ID YORDAMIDA BIOMETRIK AVTORIZATSIYADAN O‘TKAZISH AXBOROT TIZIMINI TASHKIL ETISHNING TEXNIK TALABLARI

Eshonqulov Sh.

Buxoro davlat universiteti, Buxoro, O'zbekiston

eshonqulov5474@gmail.com

Foydalanuvchining shaxsini tasdiqlash uchun biometrik xavfsizlik tizimlari tabiatan insonga tegishli bo‘lgan narsalardan – yuzning matematik modeli, retinal tomirlar, barmoq izlari, kaft, qo‘l yozuvi, ovoz va boshqalardan foydalanadi. Ushbu ma'lumotlarni kiritish odatiy parol o'rnini bosadi. Face ID bu qo'shimcha modul bo'lib, u kadrdagi yuzni aniqlay oladi va uni foydalanuvchi kartasidan ma'lumotlar bazasidan olingan fotosurat bilan solishtiradi.

Ko'p sonli xodimlarga ega bo'lgan kompaniyalar uchun asosiy biznes talablaridan biri axborot va ichki perimetrlarga kirishni nazorat qilishning tez va ishonchli mexanizmi hisoblanadi. Yuzni tanish ko'p faktorli autentifikatsiya protsedurasini tizimga kirishdan oldin foydalanuvchining shaxsini tasdiqlovchi kuchli parol himoyasi omili sifatida to'ldiradi[1].

Biz Face ID-ni yuzni tanish texnologiyasiga asoslangan ishonchli va yuqori aniqlikdagi biometrik identifikatsiya xizmati sifatida qarashimiz mumkin. Onlayn shaxsni aniqlash funksiyasi tufayli siz kameraning narigi tomonida boshqa odamlarning ma'lumotlaridan foydalanadigan firibgar emas, balki haqiqiy odam borligiga doimo amin bo'lasiz.

Face ID yordamida avtorizatsiyan o'tishning afzalliklari:

- Yuzni tanib olish qo'shimcha identifikatsiya darajasi sifatida ishlatiladi. Bu hududga/binoga boshqa birovning yoki soxta chiptalar bilan kirish, bir kartadan foydalangan holda bir nechta odamning kirish xavfini cheklaydi. Bu xodimlarning o'zlari uchun ham qulay: siz bilan "kalit" bo'lishi shart emas;
- vaqtni kuzatish: biometrik avtorizatsiya tizimi xodimlarning ishdan kelish va ketish vaqtlarini aniq qayd etish va bu ma'lumotlarni hisobxona tizimlari bilan sinxronlashtirish imkonini beradi;
- yuqori darajadagi himoyalangan ob'ektlarni nazorat qilish: yuzni tanish terminali faqat maxsus ro'yxatga kiritilgan va kirish huquqiga ega bo'lgan xodimlarga ruxsat beradi;
- ish joyini autentifikatsiya qilish. Korporativ tizimlaringizni himoya qilish darajasini oshiradi, parollarni uchinchi shaxslarga o'tkazish imkoniyatini yo'q qiladi;
- kameradan qat'iy nazar turli qurilmalarda ishlaydi (kompyuter yoki smartfonning web-kamerasi);
- shaxsni video selfi (tabassum orqali) bilan tekshirish foydalanuvchi uchun ishonchli himoya va ijobiy tajribani ta'minlaydi;
- xodimning orqasidan ekranni ko'rish yoki suratga olish orqali maxfiy ma'lumotlarni o'g'irlashdan himoya qilish;
- xizmat xodim nomidan saqlangan ma'lumotlarning u tomonidan kiritilishini ta'minlaydi.

Face ID yordamida korxona va tashkilot xodimlarini biometrik avtorizatsiyadan o'tkazish jarayonlarini tashkil etish uchun texnik ta'minotni amalga oshirish kerak. Buning uchun:

- tashkilot perimetri bo'yicha kameralarni optimal o'rnatilishi uchun loyiha ishlab chiqish;
- kirib chiqish yo'laklarida kameralarni optimal o'rnatilishi uchun loyiha ishlab chiqish;
- texnik qurilmalar ro'yxatini shakllantirish (kamera, tok manbalari, kerakli o'rnatiluvchi kronshteynlar va hk.)
- loyiha asosida kameralarni o'rnatish va texnik qo'llab quvvatlash xizmatini tashkil etish;

Hozirda Buxoro davlat universitetining barcha kirish/chiqish yo'laklari va universitet perimetri bo'yicha maxsus video kameralar o'rnatib chiqilgan bo'lib, texnik qo'llab quvvatlash universitet Raqamli ta'lim texnologiyalar markazi xodimlari tomonidan amalga oshirib kelinmoqda.

ADABIYOTLAR

1. *Lulov Yovi* Biometric face recognition // Научни трудове на Съюза на учените – Пловдив. Серия А: Обществени науки, изкуство и култура. 2017. №. URL: https://cyberleninka.ru/article/n/biometric-face-recognition (дата обращения: 24.04.2022).

2. *Улендеева Н. И.* Особенности использования технических средств охраны и контроля в деятельности УИС // Новые импульсы развития: вопросы научных исследований. 2020. №6.

KIRUVCHI VA CHIQUVCHI TARMOQ TRAFIGINI TEKSHIRISH VA BOSHQARISHNING ILG'OR USULLARI

[1]Matyakubov A.S., [2]Tadjiev R.N., [1]Komilov R.K.

[1]O'zbekiston Milliy universiteti, Toshkent, O'zbekiston

[2]O'zbekiston Milliy universiteti huzuridagi Biofizika va biokimyo instituti, Toshkent, O'zbekiston

ruhillo@mail.ru

Deep Packet Inspection (DPI) - Tarmoq trafigini tekshirish va boshqarishning ilg'or usuli. DPI tizimida paketlarni aniq ma'lumot yoki foydali yo'l bilan aniqlaydigan, tasniflaydigan, qayta yo'naltiradigan yoki bloklaydigan paketlarni filtrlash shakli va tarmoq orqali o'tadigan barcha paketlarni teran tahlil qiladi. "Teran" atamasi standart port raqamlari bilan emas, balki OSI modelining yuqori darajalarida paketni tahlil qilishni nazarda tutadi.

Paketlarning teran tekshiruvi xabarlarning mazmunini tekshirishi, kelgan mahsus dastur yoki xizmatni aniqlash va filtrlar tarmoq trafigini IP manzil (internet protokol tarmoqlar aro protokol) manzillaridan qayta yo'naltirish uchun dasturlashtirilishi mumkin.

Paketlarni teran tekshirish, maxfiy faylni elektron pochta orqali yuborishda vujudga keladigan ma'lumotlarning tarqalishini oldini olishga yordam beradi. Masalan faylni muvaffaqiyatli yuklash o'rniga foydalanuvchiga kerakli ruxsatni qanday olish va uni yuklash uchun ruxsat olish haqida ma'lumot beriladi [1].