AXBOROT XAVFSILIGIGA TAHDID TUSHUNCHASI

Akbarova Sayyora Odiljonova

Marg'ilon 1-son politexnikumi maxsus fan kata o'qituvchi

ANNOTATSIYA: *'Mazkur maqola texniumining o'qituvchi va o'quvchilariga mo'ljallangan. uslubiy ishlanmasi TTS-tarmoq ta'lim standarti talablaridan kelib chiqqan holda tayyorlanadi.kadrlar tayyorlash barcha bosqichlarida uning samaradorligini oshirish o'quv amaliyotiga oid bilimlarining salmog'iga bog'liq.Shu sababli o'quvchilarning ushbu amaliyotdan egallashi lozim bo'lgan ko'nikma va malakalarini shakllantirishga asosiy e'tibor qaratilgan.*

Ta'lim oluvchilar uchun mavzu bo'yicha muhim ahamiyatga ega bo'lgan texnik shartlar texnologik talablar va yo'l -yo'riqli xarita yoritilgan bugungi kun talablari uchun bo'yicha zaruriy qo'llanma bo'lib xizmat qiladi.

Tarmoq texnologiyalari rivojining boshlang'ich bosqichida viruslar va kompyuter xujumlarining boshqa turlari ta'siridagi zarar kam edi, chunki u davrda dunyo iqtisodining axborot texnologiyalariga bog'liqligi katta emas edi. Hozirda, xujumlar sonining doimo o'sishi hamda biznesning axborotdan foydalanish va almashishning elektron vositalariga bog'liqligi sharoitida mashina vaqtining yo'qolishiga olib keluvchi hatto ozgina xujumdan kelgan zarar juda katta raqamlar orqali hisoblanadi.

Misol tariqasida keltirish mumkinki, faqat 2003 yilning birinchi choragida dunyo miqyosidagi yo'qotishlar 2002 yildagi barcha yo'qotishlar yig'indisining 50%ini tashkil etgan, yoki bo'lmasa 2006 yilning o'zida Rossiya Federeatsiyasida 14 mingdan ortiq kompyuter jinoyatchiligi holatlari qayd etilgan.

Korporativ tarmoqlarda ishlanadigan axborot, ayniqsa, zaif bo'ladi. Hozirda ruxsatsiz foydalanishga yoki axborotni modifikatsiyalashga, yolg'on axborotning muomalaga kirishi imkonining jiddiy oshishiga quyidagilar sabab bo'ladi:

- kompyuterda ishlanadigan, uzatiladigan va saqlanadigan axborot hajmining oshishi;
- ma'lumotlar bazasida muhimlik va mahfiylik darajasi turli bo'lgan axborotlarning to'planishi;
- ma'lumotlar bazasida saqlanayotgan axborotdan va hisoblash tarmoq resurlaridan foydalanuvchilar doirasining kengayishi;
- masofadagi ishchi joylar soninig oshishi;
- foydalanuvchilarni bog'lash uchun Internet global tarmog'ini va aloqaning turli kanallarini keng ishlatish;
- foydaluvchilar kompyuterlari o'rtasida axborot almashinuvining avtomatlashtirilishi.

Axborot xavfsizligiga tahdid deganda axborotning buzilishi yoki yo'qotilishi xavfiga olib keluvchi himoyalanuvchi ob'ektga qarshi qilingan harakatlar tushuniladi. Oldindan shuni aytish mumkinki, so'z barcha axborot xususida emas, balki uning faqat, mulk egasi fikricha, kommertsiya qiymatiga ega bo'lgan qismi xususida ketyapti.

Zamonaviy korporativ tarmoqlar va tizimlar duchor bo'ladigan keng tarqalgan tahdidlarni tahlillaymiz. Hisobga olish lozimki, xavfsizlikka tahdid manbalari korporativ axborot tizimining ichida (ichki manba) va uning tashqarisida (tashqi

manba) bo'lishi mumkin. Bunday ajratish to'g'ri, chunki bitta tahdid uchun (masalan, o'g'irlash) tashqi va ichki manbalarga qarshi harakat usullari turlicha bo'ladi. Bo'lishi mumkin bo'lgan tahdidlarni hamda korporativ axborot tizimining zaif joylarini bilish xavfsizlikni ta'minlovchi eng samarali vositalarni tanlash uchun zarur hisoblanadi.

Tez-tez bo'ladigan va xavfli (zarar o'lchami nuqtai nazaridan) tahdidlarga foydalanuvchilarning, operatorlarning, ma'murlarning va korporativ axborot tizimlariga xizmat ko'rsatuvchi boshqa shaxslarning atayin qilmagan xatoliklari kiradi. Ba'zida bunday xatoliklar (noto'g'ri kiritilgan ma'lumotlar, dasturdagi xatoliklar sabab bo'lgan tizimning to'xtashi yoki bo'zilishi) to'g'ridan to'g'ri zararga olib keladi. Ba'zida ular niyati buzuq odamlar foydalanishi mumkin bo'lgan nozik joylarni paydo bo'lishiga sabab bo'ladi. Global axborot tarmog'ida ishlash ushbu omilning yetarlicha dolzarb qiladi. Bunda zarar manbai tashkilotning foydalanuvchisi ham, tarmoq foydalanuvchisi ham bo'lishi mumkin, oxirgisi ayniqsa xavfli.

Zarar o'lchami bo'yicha ikkinchi o'rinni o'g'irlashlar va soxtalashtirishlar egallaydi. Tekshirilgan holatlarning aksariyatida ishlash rejimlari va himoyalash choralari bilan a'lo darajada tanish bo'lgan tashkilot shtatidagi xodimlar aybdor bo'lib chiqdilar. Global tarmoqlar bilan bog'langan quvvatli axborot kanalining mavjudligida, uning ishlashi ustidan yetarlicha nazorat yo'qligi bunday faoliyatga qo'shimcha imkon yaratadi.

Xafa bo'lgan xodimlar (hatto sobiqlari) tashkilotdagi tartib bilan tanish va juda samara bilan ziyon yetkazishlari mumkin. Xodim ishdan bo'shaganida uning axborot resurslaridan foydalanish xuquqi bekor qilinishi nazoratga olinishi shart.

Hozirda tashqi kommunikatsiya orqali ruxsatsiz foydalanishga atayin qilingan urinishlar bo'lishi mumkin bo'lgan barcha buzilishlarning 10%ini tashkil etadi. Bu kattalik anchagina bo'lib tuyulmasa ham, Internetda ishlash tajribasi ko'rsatadiki, qariyb har bir Internet-server kuniga bir necha marta suqilib kirish urinishlariga

duchor bo'lar ekan. Xavf-xatarlar taxlil qilinganida tashkilot korporativ yoki lokal tarmog'i kompyuterlarining xujumlarga qarshi turishi yoki bo'lmaganida axborot xavfsizligi buzilishi faktlarini qayd etish uchun yetarlicha himoyalanmaganligini hisobga olish zarur. Masalan, axborot tizimlarini himoyalash Agentligining (AQSH) testlari ko'rsatadiki, 88% kompyuterlar axborot xavfsizligi nuqtai nazaridan nozik joylarga egaki, ular ruxsatsiz foydalanish uchun faol ishlatishlari mumkin. Tashkilot axborot tuzilmasidan sasofadan foydalanish xollari alohida ko'rilishi lozim.

Himoya siyosatini tuzishdan avval tashkilotda kompyuter muhiti duchor bo'ladigan xavf-xatar baholanishi va zarur choralar ko'rilishi zarur. Ravshanki, himoyaga tahdidni nazoratlash va zarur choralarni ko'rish uchun tashkilotning sarf-harajati tashkilotda aktivlar va resurslarni himoyalash bo'yicha hech qanday choralar ko'rilmaganida kutiladigan yo'qotishlardan oshib ketmasligi shart.

Umuman olganda, tashkilotning kompyuter muhiti ikki xil xavf-xatarga duchor bo'ladi:

1. Ma'lumotlarni yo'qotilishi yoki o'zgartirilishi.

2. Servisning to'xtatilishi.

Tahdidlarning manbalarini aniqlash oson emas. Ular niyati buzuq odamlarning bostirib kirishidan to kompyuter viruslarigacha turlanishi mumkin.

Bunda inson xatoliklari xavfsizlikka jiddiy tahdid hisoblanadi. 1.1-rasmda korporativ axborot tizimida xavfsizlikning buzilish manbalari bo'yicha statistik ma'lumotlarni tasvirlovchi aylanma diagramma keltirilgan.

Statistik ma'lumotlar tashkilot ma'muriyatiga va xodimlariga korporativ tarmoq va tizimi xavfsizligiga tahdidlarni samarali kamaytirish uchun xarakatlarni qaerga yo'naltirishlari zarurligini aytib berishi mumkin. Albatta, fizik xavfsizlik muammolari bilan shug'ullanish va inson xatoliklarining xavfsizlikka salbiy ta'sirini kamaytirish bo'yicha choralar ko'rilishi zarur. Shu bilan bir qatorda korporativ tarmoq va tizimga ham tashqaridan, ham ichkaridan bo'ladigan

xujumlarni oldini olish bo'yicha tarmoq xavfsizligi masalasini yechishga jiddiy e'tiborni qaratish zarur.

Viruslarga qashi ximoya tizimini qurish.

Hozirgi kunda 80000 dan ortiq kompyuter viruslari mavjud bo'lib, ular kompyuterda ma'lumotlarning ishonchli saqlanishiga xavf soladi va kompyuter ishlashi jarayonida turli muammolar kelib chiqishiga sabab bo'ladi. Shu bois, kompyuter viruslari, ularning turlari, etkazadigan zararlari hamda ulardan himoyalanish uchun ko'riladigan choralar bilan tanish bo'lish muhim.

Kompyuter viruslari va ularni davolash.

Kompyuter virusi o'lchami bo'yicha katta bo'lmagan, maxsus yozilgan dasturdan iborat bo'lib, u o'zini boshqa dasturlarga "yozib qo'yishi", shuningdek, kompyuterda turli noxush amallarni bajara olishi mumkin. Bunday dastur ishlashni boshlaganda dastlab boshqaruvini virus oladi. Virus boshqa dasturlarni topadi va unga "yuqadi", shuningdek, qandaydir zararli amallarni (masalan, diskdagi fayl yoki fayllarning joylashish jadvalini buzadi, tezkor xotirani "ifloslaydi" va h.k.) bajaradi. Virus o'ziga tegishli amallarni bajarib bo'lgandan so'ng boshqaruvini o'zi joylashgan dasturga uzatadi. Virus joylashgan dastur odatdagidek ishini davom ettiradi. Tashqaridan dasturning "kasallanganligi" bilinmaydi.

Ko'p turdagi viruslar shunday tuzilganki, kasallangan dasturni ishga tushirganda virus kompyuter xotirasida doimiy qoladiva vaqt-vaqgi bilan dasturlarni kasallaydi va kompyuterda zararli amallarni bajaradi. Virusning barcha amallari etarlicha tez va hech qanday ma'lumot e'lon qilmasdan bajariladi. Shuning uchun foydalanuvchi kompyuterda qanday jarayonlar amalga oshayotganligini bilishi qiyin.

Kompyuterdagi dasturlarning kamchilik qismi kasallangan bo'lsa, virus borligi umuman bilinmaydi. Lekin aniq vaqg o'tgandan so'ng kompyuterda qiziq

holatlar paydo bo'la boshlaydi. Masalan, ba'zi dasturlar ishlamay qoladi yoki noto'g'ri ishlaydi, ekranga begona ma'lumotlar yoki belgilar chiqariladi, kompyuterning ishlash tezligi sezilarli darajada pasayadi, ba'zi fayllar buzilib qoladi va hokazo.

Shu paytgacha kompyuterdagi anchagina dasturlar, ba'zi boshqa turdagi fayllarishdan chiqadi. Bundan tashhari, virus, disk yoki lokal hisoblash tarmoq orqali boshqa kompyuterlarga o'tishi ham mumkin.

Shuning uchun virusdan himoyalanmasa yoki yuqishining oldi olinmasa juda katta noxushliklarga olib kelishi mumkin. Masalan, 1989 yil amerikalik student Morris yozgan virus bilan bir necha ming kompyuter, jumladan AQSh mudofaa vazirligining kompyuterlari kasallangan va ishdan chiqqan. Oqibatida, virus muallifi 3 oy ozodlikdan mahrum qilinib, unga 270 ming dollar jarima solingan.

Virus dasturi ko'rinmaydigan bo'lishi uchun u juda kichik bo'lishi kerak. Shuning uchun ham ularning ko'pchiligi assembler tilida yoziladi.

Viruslarning paydo bo'lishiga dastlabki mualliflarning "shumligi" va o'zlari tushunmagan holda kimnidir "tuzlashni" maqsad qilib qo'yishlari sabab bo'lgan. Oqibatining bu darajada yomonlashuvi ularning xayoliga kelmagan bo'lsa kerak.

Hozirgi kunda 80000 dan ortiq kompyuter viruslari kompyuter tizimlari va ma'lumotlari ishi uchun asosiy xavfni tashkil etadi. Bunda, asosan, zarar ko'radiganlar litsey, institut, universitetlar va boshqa tashkilotlardir. Bunday muassasa kompyuterlarida ma'lumotlardan foydalanish ochiq va chegarasiz bo'lganligi uchun viruslarning qurboni bo'linadi va katta moddiy talafot ko'riladi. Shu bois, kompyuter ishini nazoratga olish muhimdir.

Kompyuter ishini nazoratga olish deganda nima tushuniladi? Unga quyidagilar kiradi:

1) litsenziyasiz dasturiy ta'minotdan foydalanmaslik;

2) tashqaridan kiritiladigan viruslarning oldini olish;

3) tizimga sanktsiyasiz kiruvchi xakerlarga imkon bermaslik.

Axborot va dasturlar xavfsizligini ta'minlash uchun quyidagilar zarur bo'ladi: birinchidan, litsenziyalangan dasturiy ta'minotni ishlatish; ikkinchidan, tashqi tarmoqlarga ulanishda filtr cheklovchilar o'rnatish (viruslardan himoyalanish va sanktsiyasiz foydalanishni cheklash).

Albatta, bunday himoya vositalari uzluksiz rivojlanib takomillashib bormoqda.

Kompyuter viruslarini quyidagi guruhlarga ajratish mumkin:

- diskning yuklanish sektorlarini buzadigan yuklanish viruslari;
- bajariladigan fayllar - com, exe, sys, bat fayllarini buzuvchi fayl viruslari;
- diskning yuklanish sektori va bajariladigan fayllarni buzadigan yuklanish fayli viruslari;
- stels (stelth) - ko'rinmas viruslar;
- Microsoft Word muharriri yordamida hosil qilingan ma'lumotli fayllarni yozuvchi makrobuyruq viruslari.

Bundan tashhari, boshqa turdagi viruslar ham mavjud. Viruslardan himoyalanishda axborotni himoya qilishning umumiy vositalaridan foydalanish kifoya qilmaydi. Buning uchun maxsus dasturlardan foydalanish zarur bo'ladi. Bu dasturlarni bir necha turga ajratish mumkin: detektorlar, vaktsinalar (immunizatorlar), doktorlar, revizorlar (fayl va disklarning tizimli sohalaridagi o'zgarishlarni nazorat qiluvchi dasturlar), doktor - revizorlar va filtrlar (virusdan himoyalanish uchun mo'ljallan-gan rezident dasturlar). Ularning xususiyatlarini ko'rib chiqamiz

R e v i z o r d a s t u r l a r - dastlab dastur va diskning tizimli sohasi haqidagi ma'lumotlarni xotiraga oladi, so'ngra ularni dastlabkisi bilan solishtiradi. Mos kelmagan hollar haqida foydalanuvchiga ma'lum qiladi. Masalan, CRCLIST va CRCTEST dasturlar.

Doktor revizorlar- revizor va doktorning aralashmasi, boshqacha aytganda, fayl va diskning tizimli sohasidagi o'zgarishlarni nafaqat aniq payqaydigan, balki o'zgargan holda ularni dastlabki holatga qaytarishi mumkin bo'lgan dasturlardir.

Filtr dasturlar yoki rezident dasturlar kompyuterning tezkor xotirasida rezidentday joylanadi va viruslar tomonidan zararni ko'paytirish va ziyon etkazish maqsadida operatsion tizimga qilinayotgan murojaatlarni ushlab qolib, ular haqida foydalanuvchiga ma'lum qiladi. Foydalanuvchi ushbu amalni bajarish yoki bajarmaslikka ko'rsatma beradi. Masalan, Flushot Plus va Antirus dasturlari.

Virusga qarshi dasturlar quvvatiga qarab bir necha turga bo'linadi. Quyida eng ko'p tarqalgani virusga qarshi Dsav 2.0 ("Dialog-nauka A.B.") kompleksi bilan tanishamiz. Uning tarkibiga quyidagilar kiradi:

1.AIDSTEST - viruslarni aniqlashi va yo’qotish uchun mo'ljallangan virusga qarshi ko'p qirralari dastur (har haftada yangilanib turadi).

2. Doctor WEB (Dr web) - yangidan yaratilgan, ma'lum va noma'lum viruslarni aniqlashi va yo’qotish uchun ishlatiladigan virusga qarshi dastur. U arxivlangan va vaktsiyalangan fayllarda ham viruslarni aniqlay oladi (har oyda o'rtacha 2 marta yangilanadi).

3. ADINF - diskdagi barcha o'zgarishlarni nazorat qiluvchii, disklarning virusga qarshi revizor dasturi (bir yilda bir necha marta yangilanadi). Diskdagi barcha dasturlarning fizik kamchiliklarini nazorat qiladi. Diskning tizimli sohasini va fayllar holatini eslab qoladi va qayta yuklashda diskdagi o'zgarishlarni aniqlaydi, agar biror xavfli o'zgarishlar aniqdansa, foydalanuvchiga bu haqda xabar beradi.

4. ADINF CURE MODVLE - ADINF disklar revizoridagi davolash moduli bo'lib, revizor tomonidan zararlanganligi aniqlangan fayllarni avtomatik holatda tiklaydi (yiliga bir necha marta yangilanadi).

5. SHERIF – qattiq diskdagi operatsion tizim, dasturlar va ma'lumotlar faylini 100% kafolat bilan himoyalovchi rezident dastur.

Bu dasturlar asosan MS DOS muhitida ishlatiladi (ularni Windows muhitiga moslash ham mumkin).

Amalda yuqoridagilarning bittasidan foydalanish maqsadga muvofiq. Biror dasturni o'rnatib, uni doimiy ravishda yangilab borilsa, foydaliroq bo'ladi.

Kompyuterlarga virus yuqqanda (yoki yuqqanlik haqida gumon bo'lsa) quyidagi qoidalarni esda tutish va qo'llash lozim:

1. Dastlab, qarshi kurash qarorlarini qabul qilishga shoshmaslik kerak. O'ylamasdan qilingan harakatlar tiklash mumkin bo'lgan fayllarning bir qismini yo'qotishgina emas, balki kompyuterni yana qayta kasallantirishga olib kelishi mumkin.

2. Virus o'zining buzg'unchiligini davom ettirmasligi uchun kompyuterni o'chirish lozim.

3. Kompyuter kasallanishi va davolash ko'rinishini aniqlashga mo'ljallangan barcha amallarni yozishdan himoyalangan operatsion tizimli disk bilan kompyuterni ishga tushirish orqaligina bajarish mumkin.

Тавсия этиладиган адабиётлар рўйхати:

1. Ахборот технологияси. Ахборотларни криптографик мухофазаси. Маълумотларни шифрлаш алгоритми" Ўзбекистон Давлат стандарти. O'zDSt 1105:2006

2. С.К.Еаниев, М.М. Каримов. Хисоблаш системалари ва тармокларида информация химояси. - Тошкент Давлат техника университети, 2003.

3. В.И. Завгородний. Комплексная защита информации в компьютерных системах: Учебное пособие. -М: Логос; ПБОЮЛ Н.А.Егоров, 2001.

4. Г.Н. Устинов. Основы Информационной безопасности систем и сетей передачи данных. Учебное пособие. Серия "Безопасность". - М.: СИНТЕГ, 2000.

5. Мерит Максим, Девид Поллино. Безопасность беспроводных сетей. Информационные технологии для инженеров. -Москва. 2004.

Интернет манбалари:

1. http://metalcandy.ru/documentation-centos

2. Книга Fedora Linux Toolbox. Автор: Negus Ch. 2007

3. http://xbb.uz/FOSS/Distributiv-Linux-CentOS

4. http://openwiki.ru/wiki/CentOS

5. http://metalcandy.ru/how-to-forge-centos/361-installing-webmin-on-centos-55

6. http://www.stealthsettings.com/ru/instalare-si-configurare-centos-5-6-pe-virtualbox-windows-7-vista-windows-xp.html

7. www.security.uz

8. www.cert.uz

9. www.uzinfocom.uz

10. http://sebeadmin.ru/

11. http://pc-rep.ru/