TA'LIM JARAYONIDA AXBOROT XAVFSIZLIGI TUSHUNCHALARI

Jabborov Oybek Aminovich
Maxsus fan o'qituvchisi:
Turgunboyev Mirzabek Rustambek O'g'li
Maxsus fan o'qituvchisi

Annotatsiya: *Ushbu maqolada informatika fanining bir qismi bo'lgan "Axborot xavfsizligi" tushunchasi bo'yicha bir qancha tavsiyalar va tushunchalar berib o'tilgan.*

Kalit so'zlar: *Axborot xavfsizligi, kiberxavfsizlik, fishing, dastur, login, parol.*

Yaqin yillarda hayotimizga oldinlari ko'p ham e'tibor bermagan va ishlatmagan tushunchalar, yangi terminlar kirib keldi, ularni biz juda tez o'zlashtirmoqdamiz. Axborot xavfsizligi, kiberxavfsizlik, fishing, pentesting, botlar, shubhali havolalar va shunga o'xshash terminlar sanab o'tish maqsadga muvofiq.

Axborotlar, ma'lumot bazalari bizni shunchalik o'rab oldiki, u hatto yoshu-qarini o'ziga tez jalb qilmoqda. Oddiy telefon orqali biz ma'lumot bazasini ixtiyoriy yoshdagi insonni qo'lida turganini ko'rishimiz oddiy holga aylandi.

Axborotlar bilan ishlash jarayoni tezlashgani, texnikaning, dasturiy ta'minotning odamlarning istaklaridanda tezroq o'sib borayotgani bunga yaqqol misol. Sun'iy intellekt, sun'iy intellektning ham juda ko'p yo'nalishlari paydo bo'lmoqda, uni hozirda hamma sohada ko'rishimiz mumkin. Hamma narsaning ham ijobiy va salbiy jihatlari bo'lgani kabi, texnika yangiliklari, bizni bunday davrda yanaham ehtiyorkorroq, axborotlarni himoyalash usullaridan foydalanishga ko'proq chorlamoqda.

Chunki turli tarmoqlar orqali tez-tez kelib turgan shubhali havolalar, ulardan so'ng "fake" xabarlar deb keladigan bildirishnomalar va yana turli notanish insonlardan keladigan SMS xabarlari, turli ogohlantirishlar bizni bu axborotlar davrida axborot hurujlaridan ehtiyot bo'lishga chorlamoqda.

Axborot xavfsizligi (inglizcha: Information security) - axborotni ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o'zgartirish, tadqiq qilish, yozib olish yoki yo'q qilishning oldini olish amaliyotidir. Bu universal kontsepsiya ma'lumotlar qanday shaklda bo'lishidan qat'iy nazar amal qiladi. Axborot xavfsizligini ta'minlashning asosiy maqsadi, ma'lumotlarning konfidensialligi, yaxlitligi va mavjudligini muvozanatli qo'llashning maqsadga muvofiqligini hisobga olgan holda va tashkilot faoliyatiga hech qanday zarar yetkazmasdan himoya qilishdir.

Buning uchun birinchi navbatda, asosiy vositalar va nomoddiy aktivlar, tahdid manbalari, zaifliklar, potensial ta'sirlar va mavjud xavflarni boshqarish imkoniyatlarini aniqlaydigan ko'p bosqichli xavflarni boshqarish jarayoni orqali erishiladi.

Bu jarayon xavflarni boshqarish rejasining samaradorligini baholash bilan birga olib boriladi. Respublikamizda ham axborot xavfsizligini ta'minlash, kiberhujumlardan himoylanish, kiberxavfsizlikni rivojlantirish bo'yicha bir qancha ishlar qilinmoqda.

Kiberhujum - kompyuter axborot tizimlari, kompyuter tarmoqlari, infratuzilmalar yoki shaxsiy kompyuter qurilmalariga qaratilgan har qanday hujumkor manyovr.

Milliy kiberxavfsizlik strategiyasi, kiberxavfsizlik qonunchiligi, potensialni oshirish va ta'lim, aholini xabardor qilish kompaniyalari, hodisalarga javob berish va boshqalar. Ushbu qilinayotgan ishlar albatta, bizni, jamiyatimizni, axborotlar bilan ishlash xavfsizligimizni ta'minlash va oshirish uchun xizmat qilmoqda. Bu borada qilinayotgan ishlarga psixologik fishing, zararli dasturlardan foydalanmaslik va kiberxavfsizlik qoidalariga amal qilish kabilarni misol tariqasida keltirishimiz mumkin.

Hakkerlar haqida eshitganmisiz? Ularning ham yaxshisi (White hat), yomoni (Black hat) va o'rta darajalisi (Grey hat) bo'ladi. Black hat hakkerlar odamlarni aldash, ularni pulini o'marish va turli yomon maqsadlarda ishlasa, "White hat" hakkerlari esa axborotlar xafvsizligini buzishga qilinayotgan harakatlarni aniqlab, ularga nisbatan chora ko'rilishi, "Black hat" hakkerlarni topish bilan shug'ullanadilar. "Grey hat" hakkerlar esa, ular havaskor hakkerlar sanaladi, ular turli sayt va tarmoq xavfsizligini tekshirish, uning zaif tomonlarini topib, bu haqda xabar berish bilan shug'ullanadilar va shu orqali pul ishlaydilar.

Axborot xavfsizigini ta'minlash bo'yicha bir necha tushunchalar kiritilgan. Ularga axborotni muhofazalash, axborot xavfsizligi, ma'lumotni ochish, identifikatsiya, autentifikatsiya, avtorizatsiya kabilar.

Axborotni muhofazalash - bu ma'lumotlarni o'g'irlash, yo'qotish, soxtalashtirish, qalbakilashtirsh, ruxsatsiz foydalanish va ko'paytirishning oldini olishga yo'naltirilgan tadbirlar majmuasidan iborat.

Axborot xavfsizligi - foydalanish talablari asosida ma'lumotning yashirinligi, yaxlitligi va foydalanuvchanligini ta'minlashdan iborat.

Ma'lumotni ochish - tasodifan yoki xusumatli harakatlar natijasida begona shaxsga axborotning mazmuni ruxsatsiz oshkor etilishdir.

Identifikatsiya - foydalanuvchini tizimga o'zini tanitish jarayoni bo'lib, unda mijozning maxsus shaxsiy kartalaridan yoki uning biometrik xususiyatlaridan foydalaniladi.

Autentifikatsiya - foydalanuvchining to'g'riligini tekshiriladi va shundan so'ng tizimda faoliyat olib borishi mumkinligi yoki mumkin emasligini belgilaydi.

Avtorizatsiya - foydalanuvchiga tizim tomonidan berilgan huquqlar majmuasidir.

Informatika va axborot texnologiyalari fanini "Axborot xavfsizligi" bo'limini o'qitishda bir necha tavsiyalarni ko'rib chiqaylik:

Axborot xavfsizligini ta'minlashning eng sodda tushunchalaridan boshlaydigan bo'lsak, ixtiyoriy sayt, ijtimoiy tarmoqdan ro'yxatdan o'tish jarayonida login va parollarni ishlatilishiga ahamiyat berish. Bugungi kunda ro'yxatdan o'tish formalari parollariga bir qancha talablar qo'yilgan, shu talablarni to'liq bajarish, parol qo'yishda o'z shaxsiy ma'lumotlarimizdan foydalanmaslik, masalan tug'ilgan kunimiz, ism, familiya, yaqinlarimizning tug'ilgan kunlari, raqamlar va klaviaturadagi harflar ketma-ketligi kabilar. Bunday parol qo'yishdan juda ko'p insonlar foydalaniladilar va kombinatsiya qilish jarayonida juda tez parolni buzilishiga olib keladigan sanaladi.

Kompyuter, mobil yoki texnik qurilmaga turli sinovlardan o‘tmagan dasturlarni o‘rnatishdan saqlanish kerak. Reklamalar orqali keladigan tekin dasturlar o‘zi bilan birgalikda viruslarni olib kelishiga hech kim javob bermaydi, shuning uchun bu qilayotgan hatti-harakatimizni o‘ylab amalga oshirishimiz kerakligini bildiradi. Turli viruslar uchun esa, antivirus dasturlaridan foydalanish, Windows operatsion tizimi foydalanuvchilari uchun esa, Sistema bilan birga o‘rnatiladigan Windows Defender dasturidan foydalanish va operatsion sistema bilan birgalikda yangilanib turish rejimini yoqib qo‘yishimiz kerak bo‘ladi. Axborot ma’lumotlar bazalari o‘rab olgan dunyoda yashayotgan ekanmiz, eng ko‘p foydalanuvchilarga ega bo‘lgan messenjerlar, itimoiy tarmoq ilovalari (Instagramm, Telegram, Youtube, Tvitter...) da reklama qilinayotgan turli e’tiborni, qiziqishni uyg‘otayotgan xabarlardan ehtiyot bo‘lishimiz lozim. Hozirda xavaskor dasturchilarning ko‘payib borayotgani, pul ishlash maqsadida, turli reklamalar, videolarni ommaga taqdim etish, ishga tushuvchi virus dasturlarni yaratish kabi videolar, kodlar yozishni o‘rgatish yosh avlod bunday narsalardan himoylashimiz zarurligini anglatadi. Axborot xavfsizligi haqida ko‘proq ma’lumot berish, barcha manbalardan to‘g‘ri foydalanishni o‘rganishimiz va bu haqida o‘quvchilarga ko‘proq ma’lumot berishimiz kerak.

Axborotlarni himoyalashni yana bir sodda usulini ko‘rib chiqaylik. Har qanday texnikadan foydalanuvchi o‘z shaxsiy ma’lumotlarini boshqalardan himoyalashga, fayllarini parollashga urinadilar. Bunday usullardan eng osoni bu arxivlash dasturlari yordamida (Winrar, WinZip, 7zip) amalga oshirishdir.

Keling buni qanday amalga oshirish ketma-ketligini ko‘rib chiqaylik:

1. “Hujjatlar” deb yoki siz tomoningizdan ixtiyoriy nom bialn saqlangan fayl, papka tanlanadi.
2. Konteks menyu hosil qilinadi (sichqonchaning o‘ng tarafi bosiladi).
3. Hosil bo‘lgan “Имя и параметры архива” oynasidan “Обзор” tugmasi orqali saqlanadigan joyni ko‘rsatishimiz kerak bo‘ladi.
4. “Установить пароль” tugmasi orqali hujjatimizni shifrlaymiz.
5. Hosil bo‘lgan arxivlangan hujjatni ixtiyoriy vaqtda, parolni terib ishlatimishimiz mumkin.
6. Quyida qilinadigan amallar ketma-ketligi tasvirlarda ko‘rsatilgan.

XULOSA

Xulosa qilib shuni aytish mumkinki, axborotlarni saqlash va uzatish tizimlari bir tomondan takomillashib murakkablashgan va ikkinchi tomondan axborotlardan foydalanuvchilar uchun keng qulayliklar vujudga kelgan davrda, axborotlarni maqsadli boshqarishning qator muhim masalalari kelib chiqadi. Bunday masalalar qatoriga katta hajimdagi axborotlarning tez va sifatli uzatish hamda qabul qilish axborotlarni ishonchliligini ta’minlash, axborotlar tizimida axborotlarni begona shaxslardan (keng ma’noda) muhofaza qilish kabi ko’plab boshqa masalalar kiradi.

FOYDALANILGAN ADABIYOTLAR:

1. G’aniyev S. K. ,Karimov M. M., Tashev K. A. AXBOROT XAVFSIZLIGI Toshkent 07

2. S.S. Qosimov Axborot texnologiyalari xaqida o'quv qo'llanma Toshkent 07

3. G'aniyev S.K.Karimov M.M. Hisoblash tizimlari va tarmoqlarida axborot xavfsizligi TDTU 03

4. http://www.kaspersky.ru/

5. http://www.viruslist.ru/

8. http://www.osp.ru/lan/2001/03/024.htm/

9. www.nasa.gov/statistics/

10. www.security.uz