KIBER-XAVFSIZLIK. INTERNETDAGI MAXFIY MA'LUMOTLAR, KIBER-HUJUMLAR VA ULARNI OLDINI OLISH USULLARI

Sunnatov Zafar Ubaydullaevich
Axborot texnologiyalari va menejment universiteti rektori

Annotatsiya: *Kiber-xavfsizlik, bugungi eng muhim muddatlardan biri bo'lib chiqib, internet dunyosida ma'lumotlarni himoya qilish, ularga hujumlar bilan kurashish va kiber-tahdidlarga qarshi turishni o'z ichiga olgan texnologiyalardan biridir. Bu maqolada, kiber-xavfsizlikning asosiy xususiyatlari, muammolar, va ularni oldini olish usullari haqida gaplashamiz.*

Kalit so‘zlar: *kiber-xavfsizlik, internet, asosiy xususiyatlari, muammolar, teknologik rivojlanish, veb saytlar, nazorat qilish.*

Kiber-xavfsizlikning asosiy xususiyatlari.

Maxfiylik: Kiber-xavfsizlikning asosiy maqsadi, ma'lumotlarni maxfiy va himoya qilishdir. Bu, shaxsiy ma'lumotlar, kompaniya sirli ma'lumotlari, moliyaviy ma'lumotlar kabi muhim axborotlar uchun juda muhimdir.

Xavfsizlikni ta'minlash: Xavfsizlikni ta'minlash, tarmoqda foydalanuvchilarga xavfsizlik yechimlarini berishni, shu jumladan, xavfsiz parollar, yorliq yoki biometrik identifikatsiya muvozanatlarini ta'minlashni o'z ichiga oladi.

Kiber-hujumlar bilan kurashish: Kiber-xavfsizlik, kiber-hujumlar, masalan, viruslar, trojanlar, foydalanuvchining ma'lumotlarini olish uchun qo'shimcha usullar kabi muammolarga qarshi kurashishda juda muhim rol o'ynaydi.

Kiber-xavfsizlikning muammolari.

Foydalanuvchilarning noyobligi: Foydalanuvchilar ko'plab muhim axborotlarga ega bo'lishi mumkinligi sababli, ularning xavfsizligini ta'minlash juda muhimdir. Foydalanuvchilar o'zlarining ma'lumotlarini himoya qilish, xavfsiz parollar yaratish, va eng yangi xavfsizlik texnologiyalaridan foydalanishga e'tibor bermoqda.

Kiber-tahdidlar: Kiber-tahdidlar, saytni qo'llab-quvvatlovchilardan, kiber-jinoyatchilardan yoki hujum yaratuvchilardan kelib chiqishi mumkin. Bu tahdidlar, saytni yo'lga qo'yish, ma'lumotlarni olish, yoki tarmoq xavfsizligini buzishga olib keladi.

Teknologik rivojlanish: Teknologik rivojlanish, xavfsizlik sohasidagi muammo va xalqaro kiber-jinoyat risklarini oshiradi. Masalan, IoT (internetga ulangan jihozlar) muhitdagi vositalar, xavfsizlikni ta'minlash uchun yangi qo'shimcha muammo va hujumlar yaratishi mumkin.

Kiber-xavfsizlikning oldini olish usullari

Xavfsiz ta'minot protokollari: Foydalanuvchilar va kompaniyalar uchun xavfsiz ta'minot protokollari, masalan, HTTPS, VPN (Virtual Private Network), va SSH (Secure Shell) kabi usullar, internetda axborot almashish va o'zaro aloqalarni xavfsizligini ta'minlashda yordam beradi.

Xavfsiz ta'minot protokollari, foydalanuvchilar va kompaniyalar uchun internetda axborot almashish va o'zaro aloqalarni xavfsizligini ta'minlashda muhim bo'lgan vositalardir. Quyidagi ta'minot protokollari kiber-xavfsizlikni ta'minlashda katta ahamiyatga ega:

HTTPS (HyperText Transfer Protocol Secure): HTTPS, veb saytlarda ma'lumot almashish va uzatish protokolining maxfiy va xavfsiz versiyasidir. Ushbu protokol ma'lumotlarni shifrlaydi va ularga maxfiylikni ta'minlaydi, shuningdek, saytning kimlikni tasdiqlash uchun sertifikatlar ishlatadi. Bu protokol orqali sayt foydalanuvchilari va serverlar orasidagi aloqalarni xavfsiz ravishda o'tkazish mumkin.

VPN (Virtual Private Network): VPN, internetda foydalanuvchilar uchun xavfsiz va maxfiy aloqalarni ta'minlashda o'zaro tarmoqni ishlatadi. Bu tarmoq orqali ma'lumotlar shifrlanadi va foydalanuvchi IP manzili, geolokatsiyasi, va internet faoliyati maxfiy ravishda o'zgaradi. VPN, xavfsizlik ta'minoti bo'lgan qo'llab-quvvatlovchilar, kompaniyalar, va shaxsiy foydalanuvchilar uchun muhim bir vositadir.

SSH (Secure Shell): SSH, serverlar bilan ishlashda maxfiylikni ta'minlash uchun ishlatiladigan protokoldir. Ushbu protokol yordamida foydalanuvchilar maxfiy shifrlashni va xavfsiz aloqalarni ta'minlashadi. SSH, ma'lumot almashish va boshqaruv jarayonlarida kiber-xavfsizlikni oshirishda keng qo'llaniladi.

Bu protokollar kiber-xavfsizlik sohasida qo'llab-quvvatlovchilar uchun katta ahamiyatga ega. Foydalanuvchilar va kompaniyalar, internetda axborot almashish va o'zaro aloqalarni xavfsiz ravishda o'tkazish uchun bu protokollardan foydalanishadi. Xavfsiz ta'minot protokollari orqali ma'lumot almashish va uzatish jarayonlari maxfiy va xavfsiz bo'ladi, shuningdek, kiber-xavfsizlikni oshirishga yordam beradi.

Kiber-xavfsizlik tizimlari va dasturlar: Kiber-xavfsizlik tizimlari va dasturlari, hujumni aniqlash, undan oldinini olganda qo'llab-quvvatlovchilar uchun xavfsizlikni ta'minlashda juda muhimdir. Bu tizimlar va dasturlar, ma'lumotlar bazalarini himoya qilish, hujumni to'xtatish yoki qo'llab-quvvatlovchilar uchun xavfsizlik shakllarini taqdim etish imkonini beradi.

Kiber-xavfsizlik tizimlari: Bu tizimlar va dasturlar, tarmoqda yuz beradigan kiber-xavfsizlik hujumlarini aniqlash va uchraydigan nuqtalarini identifikatsiya qilish uchun ishlaydi. Kiber-monitoring va alarm tizimlari, hujum shakllarini oldinini olish jarayonlarini avtomatlashtirishga yordam beradi.

Antivirus va antimalware dasturlari: Bu dasturlar kompyuterlarga o'rnatiladi va kompyuterlarni kiber-xavfsizlik hujumlari, viruslar, trojanlar, va boshqa zararli dasturlar qarshi himoya qilishda yordam beradi. Antivirus va antimalware dasturlari, sistemni skan qilish, zararli fayllarni aniqlash va ularni yo'q qilish imkonini beradi.

Firewall tizimlari: Firewall tizimlari, tarmoqni himoya qilish uchun qo'llaniladi va hujumlarni oldini olishda katta ahamiyatga ega. Ular, tarmoq trafikini tekshirish va geymerlarni aniqlash, maxfiylik siyosatlarini amalga oshirish, va taqiqlanmagan kirishlarni bloklash imkonini beradi.

Intrusion detection systems (IDS) va intrusion prevention systems (IPS): Bu tizimlar hujum va xavfsizlik haqida yo'qotishlarni aniqlash uchun ishlaydi. IDS tizimi hujumni aniqlashda yordam beradi, va IPS tizimi hujumni to'xtatish yoki oldini olish uchun ishlaydi.

Access control dasturlari: Bu dasturlar, ma'lumotlarga kirishni tartibga solish uchun ishlatiladi. Foydalanuvchilar va sistem operatorlarining faqat kerakli ma'lumotlarga kirishini ta'minlash va maxfiylik sozlamalarini boshqarish imkonini beradi.

Encryption dasturlari: Ma'lumotlarni shifrlash va de-shifrlashda qo'llaniladigan dasturlar. Ular, ma'lumotlarni maxfiy ravishda almashish uchun xavfsizlik klyuchlari va shifrlash algoritmlarini taqdim etadi.

Kiber-xavfsizlik tizimlari va dasturlari, kompaniyalar, hukumatlar va shaxsiy foydalanuvchilar uchun kiber-xavfsizlikni oshirishda katta rol o'ynaydi. Ular, hujumlarni aniqlash, ma'lumotlarni himoya qilish, va xavfsizlik sozlamalarini amalga oshirish imkonini beradi, shuningdek, potentsial xavfli holatlarda yadrogi chiqishlarni to'xtatish uchun katta qo'llaniladi.

Ma'lumotni nazorat qilish va ta'lim berish: Ma'lumotni nazorat qilish va ta'lim berish, foydalanuvchilarga kiber-xavfsizlikning ahamiyatini tushuntirish, xavfsizlikni ta'minlash usullarini o'rgatish, va muammolarni aniqlash va oldini olishga yordam berish uchun juda muhimdir.

Kiber-xavfsizlikni tushunish: Foydalanuvchilarga kiber-xavfsizlikning ahamiyatini o'rgatish juda muhimdir. Bu, ularni shaxsiy ma'lumotlarni maxfiy saqlash, xavfsizlik sozlamalarini o'rganish va saytlarda to'g'ri bo'lish kabi amallar bilan tanishtiradi.

Xavfsizlikni ta'minlash usullarini o'rganish: Foydalanuvchilarga xavfsizlikni ta'minlash usullarini o'rganish, masalan, yangi xavfsiz parollar yaratish, foydalanuvchi to'g'risida maxfiy ma'lumotlarni olishga qo'yilgan cheksiz kirishlar yoki veb saytlarda "HTTPS" ni tekshirish imkoniyatlarini ta'lim etish.

Ma'lumotni himoya qilishning asosiy tamoyillari: Ma'lumotlarni nazorat qilishning asosiy tamoyillari va maxfiylikning asosiy prinsiplari, masalan, maxfiylik siyosatlarini amalga oshirish, ma'lumotlarni reglamentlash, va maxfiylikni ta'minlashning asosiy qoidalari bilan foydalanuvchilarni ta'lim etish.

Muammolarni Aniqlash va Oldini Olish: Foydalanuvchilarga kiber-xavfsizlik muammolarini aniqlash, masalan, foydalanuvchi hisobining hacklanishi, zararli dasturlar yoki hujumlar bilan uchrashish kabi muammolar haqida o'rganish va ularga qanday yordam bera olishlarini o'rgatish.

Vazirlik va yondashuv sohalarini o'rganish: Foydalanuvchilarga, ma'lumotlarni maxfiy ravishda saqlash uchun zarur vazirlik va yondashuv sohalarini o'rganish va ularga qanday murojaat qilishlarini o'rgatish.

**Dastlabki yordam: **Xavfsizlik savdo tuzilmasi, hujum tahlillarini yuborish, va muammolar uchun yordam olishning oldini olish uchun foydalanuvchilarni yo'q qilish, shuningdek, maslahatlar berish.

Bu usullar kiber-xavfsizlikni oshirishda katta yordam beradi va foydalanuvchilarga kiber-xavfsizlik bilimini oshirishda katta rol o'ynaydi. Ta'lim berish va ma'lumotni nazorat qilish, kiber-xavfsizlikning rivojlanishi va faol ko'rish uchun zarurdir.

Bu kiber-xavfsizlik muhim bo'lgan bir mavzu bo'lib, foydalanuvchilar, kompaniyalar, va hukumatlar uchun katta ahamiyatga ega. Kiber-xavfsizlikning muammo va oldini olish usullari, doimiy ravishda rivojlanib, yangi muammoni oldini olish va maxfiylikni ta'minlash uchun yangi texnologiyalar va usullar ishlab chiqilmoqda.

FOYDALANILGAN ADABIYOTLAR:

1. Ganiyev S.K. “Kiberxavfsizlik asoslari”. O’quv qo’llanma.
2. https://uz.wikipedia.org/wiki/Axborot_xavfsizligi
3. https://uzpedia.uz/pedia/kiberxavfsizlik