KIBERJINOYATCHILIK VA ULARDAN HIMOYALANISH RAQAMLI XAVFSIZLIK VA HIMOYA STRATEGIYALARI

Mo‘minov Azamat Solijonovich
Namangan viloyati Ichki Ishlar Boshqarmasi Axborot-texnologiyalari sohasidagi jinoyatlarga qarshi kurashish boshqarmasi prognozlash guruhi, yetakchi mutaxassisi, podpolkovnik

KIRISH

Zamonaviy raqamli davr insoniyatga katta imkoniyatlar berdi: internet orqali dunyo bilan bog'lanish, onlayn xizmatlardan foydalanish, elektron tijorat va raqamli to'lovlar. Biroq, bu imkoniyatlar bilan birga yangi xavf – kiberjinoyatchilik ham paydo bo'ldi. Kiberjinoyatchilik – bu kompyuter tizimlari, tarmoqlar va raqamli ma'lumotlarga qarshi qonunbuzarlik faoliyati.

Kiberjinoyatlar yildan-yilga ko'payib bormoqda va ularning murakkabligi ham oshib bormoqda. Hujumchilar yangi usullar va texnologiyalardan foydalanib, shaxsiy ma'lumotlarni o'g'irlash, moliyaviy firibgarlik qilish, tizimlarni buzish va davlat infratuzilmasiga zarar yetkazishga harakat qilmoqdalar.

Ushbu tezisda kiberjinoyatchilik turlari, ularning qo'llanish usullari, jamiyat va iqtisodiyotga ta'siri hamda himoya choralari va xavfsizlik strategiyalari to'liq tahlil qilinadi.

1. Kiberjinoyatchilik turlari va tasnifi

1.1. Phishing (Firibgarlik xabarlari)

Phishing – bu hujumchilar o'zlarini ishonchli tashkilot (bank, pochta xizmati, davlat muassasasi) sifatida ko'rsatib, foydalanuvchilarni aldab shaxsiy ma'lumotlarini (parol, karta raqami, shaxsiy ma'lumotlar) o'g'irlash usuli.

Phishing hujumlari odatda elektron pochta, SMS (smishing) yoki ijtimoiy tarmoqlar orqali amalga oshiriladi. Xabar ishonchli ko'rinishda bo'lib, foydalanuvchini zararli havolani bosish yoki shaxsiy ma'lumotlarni kiritishga undaydi.

Masalan, foydalanuvchi bank nomidan kelgan xabar deb o'ylab, havola orqali soxta saytga kirib, karta ma'lumotlarini kiritishi mumkin. Hujumchilar bu ma'lumotlarni olganlaridan keyin foydalanuvchi hisobidan pul o'g'irlaydilar.

1.2. Ransomware (To'lov talab qiluvchi viruslar)

Ransomware – bu foydalanuvchi yoki tashkilot fayllarini shifrlash orqali ularga kirishni bloklash va shifrlash kalitini olish uchun to'lov (odatda kriptovalyuta) talab qiluvchi zararli dastur.

Ransomware hujumlari katta kompaniyalar, davlat muassasalari, kasalxonalar va ta'lim tashkilotlari uchun jiddiy tahdid hisoblanadi. WannaCry (2017) va NotPetya (2017)

kabi ransomware hujumlari dunyo bo'ylab millionlab kompyuterlarni zararladi va milliardlab dollar zarar keltirdi.

To'lov to'lansa ham, hujumchilar har doim fayllarni tiklamasligining kafolati yo'q. Shuning uchun muntazam zaxira nusxa (backup) saqlash juda muhim.

1.3. DDoS hujumlari (Distributed Denial of Service)

DDoS hujumlari – bu veb-sayt yoki onlayn xizmatni minglab yoki millionlab soxta so'rovlar bilan to'ldirib, uni ishdan chiqarish usuli. Natijada qonuniy foydalanuvchilar xizmatdan foydalana olmaydilar.

DDoS hujumlari odatda botnet tarmoqlari (yuqtirilgan kompyuterlar tarmog'i) orqali amalga oshiriladi. Hujumchilar minglab kompyuterni nazorat qilib, ularni bir vaqtda bitta nishonga hujum qilishga majburlaydilar.

2016-yilda Dyn kompaniyasiga qarshi DDoS hujumi Twitter, Netflix, PayPal va boshqa yirik xizmatlarni bir necha soatga to'xtatdi. Bu hujum IoT (Internet of Things) qurilmalarining zaifligidan foydalangan.

1.4. Identifikatsiya o'g'irlash (Identity Theft)

Identifikatsiya o'g'irlash – bu boshqa shaxsning shaxsiy ma'lumotlarini (ism, tug'ilgan sana, pasport ma'lumotlari, ijtimoiy sug'urta raqami) o'g'irlab, ularning nomidan moliyaviy operatsiyalar yoki boshqa huquqbuzarliklarni amalga oshirish.

Bu jinoyat qurbonlarga jiddiy moliyaviy va huquqiy muammolar keltirishi mumkin. Identifikatsiya o'g'irlash natijasida kreditlar olinishi, firibgarlik operatsiyalari amalga oshirilishi va qurbon nomidan jinoyatlar sodir etilishi mumkin.

1.5. Ijtimoiy muhandislik (Social Engineering)

Ijtimoiy muhandislik – bu texnologik zaifliklardan emas, balki insoniy psixologiyadan foydalanib, odamlarni aldash va maxfiy ma'lumotlarni olish usuli. Bu usul odamlarning ishonchli tabiati, qo'rquvlari yoki bilimdonligi etishmaganligidan foydalanadi.

Masalan, hujumchi kompaniya xodimi sifatida qo'ng'iroq qilib, texnik yordam xizmati nomidan parol so'rashi yoki ishonchli tashkilot vakili sifatida maxfiy hujjatlarni so'rashi mumkin.

Kevin Mitnick kabi mashhur xakerlar ijtimoiy muhandislik orqali eng xavfsiz tizimlarga ham kirishgan. Ular ko'pincha odamlarni aldash texnik bilimlardan ko'ra samaraliroq deb ta'kidlashgan.

1.6. Kreditka firibgarligi va onlayn to'lov hujumlari

Kreditka firibgarligi – bu boshqa shaxsning karta ma'lumotlarini o'g'irlab, ulardan ruxsatsiz foydalanish. Hujumchilar karta raqami, CVV kod va amal qilish muddatini turli usullar bilan olishadi.

Skimming (karta ma'lumotlarini nusxalash), veb-sayt buzish (data breach), phishing va zararli dasturlar orqali karta ma'lumotlari o'g'irlanishi mumkin. Bu ma'lumotlar keyinchalik qora bozorda sotiladi yoki to'g'ridan-to'g'ri firibgarlik uchun ishlatiladi.

1.7. Davlat darajasidagi kiberhujumlar (Cyber Warfare)

Davlat darajasidagi kiberhujumlar – bu bir davlat tomonidan boshqa davlatning kritik infratuzilmasiga (energetika tizimlari, transport, aloqa, harbiy tizimlar) qarshi hujumlar. Bu hujumlar siyosiy, harbiy yoki iqtisodiy maqsadlarda amalga oshiriladi.

2010-yilda Stuxnet virusi Eron yadro dasturining santrifugalarini buzish uchun ishlatildi. 2015-yilda Ukraina elektr tarmog'iga kiberhujum tashkil etilib, yuz minglab odam elektr ta'minotisiz qoldi.

Kiberhujumlar zamonaviy urushlarning yangi formasi hisoblanadi va ulardan himoyalanish milliy xavfsizlikning muhim qismi bo'lib qolmoqda.

2. Kiberjinoyatchilik usullari va texnikalari

2.1. Zaif parollardan foydalanish

Ko'pgina kiberhujumlar oddiy va takrorlanuvchi parollardan foydalanishdan kelib chiqadi. Hujumchilar brute force (qo'pol kuch) usuli bilan parollarni sinab ko'rishadi yoki dictionary attack (lug'at hujumi) orqali umumiy parollarni tekshirishadi.

'123456', 'password', 'qwerty', 'admin' kabi oddiy parollar daqiqalar ichida buzilishi mumkin. Shuningdek, bir xil parolni turli xizmatlarda ishlatish xavflidir – bir xizmat buzilganda, boshqa barcha hisoblar ham xavf ostida qoladi.

2.2. Dasturiy ta'minot zaifliklaridan foydalanish

Hujumchilar operatsion tizimlar, dasturlar va veb-saytlardagi xavfsizlik zaifliklaridan foydalanadilar. Yangilanmagan dasturlar, patch (tuzatish) o'rnatilmagan tizimlar va zero-day zaifliklar kiberhujumlar uchun eng qulay nishonlardir.

Zero-day zaiflik – bu ishlab chiqaruvchi hali tuzatmagan xavfsizlik muammosi. Hujumchilar bu zaifliklarni topib, ulardan tuzatish chiqishidan oldin foydalanishga harakat qilishadi.

2.3. SQL Injection va veb-hujumlar

SQL Injection – bu veb-saytning ma'lumotlar bazasiga zararli SQL buyruqlarni yuborish orqali ma'lumotlarni o'g'irlash, o'zgartirish yoki o'chirish usuli. Bu zaif kodlangan veb-saytlarga qarshi keng qo'llaniladigan hujum turi.

Cross-Site Scripting (XSS) va Cross-Site Request Forgery (CSRF) ham keng tarqalgan veb-hujumlardir. Ular foydalanuvchilarni aldash va ularning sessiyalarini o'g'irlash uchun ishlatiladi.

2.4. Man-in-the-Middle (MITM) hujumlari

MITM hujumi – bu hujumchi ikki tomon (masalan, foydalanuvchi va bank) o'rtasidagi aloqani to'xtatib, ularning o'zaro ma'lumotlarini o'qish yoki o'zgartirish usuli. Bu odatda xavfsiz bo'lmagan Wi-Fi tarmoqlari orqali amalga oshiriladi.

Hujumchi jamoat Wi-Fi nuqtasida foydalanuvchilar va internet o'rtasidagi aloqani kuzatib, login ma'lumotlari, karta raqamlari va boshqa maxfiy ma'lumotlarni olishi mumkin.

2.5. Zararli dasturlar va troyanlar

Troyanlar, keylogger (klaviatura bosishlarini qayd qiluvchi dasturlar), spyware (josuslik dasturlari) va backdoor (yashirin kirish yo'llari) yaratuvchi zararli dasturlar hujumchilar uchun asosiy vositalardir.

Ushbu dasturlar foydalanuvchi bilmasdan o'rnatiladi va fonda ishlaydi. Ular parollarni, bank ma'lumotlarini, shaxsiy fayllarni to'playdi va hujumchilarga yuboradi. Ba'zi troyanlar esa kompyuterni botnet tarmog'iga qo'shib, uni DDoS hujumlarida ishlatadi.

3. Kiberjinoyatlarning jamiyat va iqtisodiyotga ta'siri

3.1. Moliyaviy yo'qotishlar

Kiberjinoyatchilik jahon iqtisodiyotiga har yili trilionlab dollar zarar keltirmoqda. Cybersecurity Ventures ma'lumotlariga ko'ra, 2025-yilda kiberjinoyatlar oqibatida global zarar 10.5 trillion dollarga yetishi kutilmoqda.

Shaxslar uchun identifikatsiya o'g'irlash, karta firibgarligi va phishing hujumlari katta moliyaviy zararlarga olib kelishi mumkin. Kompaniyalar uchun esa ma'lumotlar buzilishi, ransomware to'lovlari va biznes to'xtatilishi milliardlab dollar yo'qotishga sabab bo'ladi.

3.2. Ishonch va obro'ning yo'qolishi

Kompaniyalar ma'lumotlar buzilishi (data breach) oqibatida mijozlarning ishonchini yo'qotadi. Equifax (2017), Yahoo (2013-2014), Facebook-Cambridge Analytica (2018) kabi skandallar bu kompaniyalarning obro'siga jiddiy zarar yetkazdi.

Mijozlar shaxsiy ma'lumotlarini himoya qilmaydigan kompaniyalardan voz kechishadi. Natijada kompaniya bozor qiymatini yo'qotadi va mijozlar soni kamayadi.

3.3. Davlat infratuzilmasiga zarar

Kiberhujumlar davlat infratuzilmasiga (elektr tarmoqlari, suv ta'minoti, transport tizimlari, aloqa tarmoqlari) jiddiy zarar yetkazishi mumkin. Bu xizmatlar to'xtashi millionlab odamlarni ta'sir qiladi va favqulodda vaziyatlarga olib kelishi mumkin.

2021-yilda Colonial Pipeline kompaniyasiga ransomware hujumi AQShda yoqilg'i ta'minoti tanqisligiga olib keldi. Kompaniya 4.4 million dollar to'lovni to'lashga majbur bo'ldi.

3.4. Shaxsiy hayot va maxfiylikka tahdid

Kiberjinoyatchilik shaxsiy ma'lumotlarning oshkor bo'lishiga olib keladi. Shaxsiy suratlar, xabarlar, moliyaviy ma'lumotlar va tibbiy tarix ochiqlanishi katta psixologik va ijtimoiy muammolarga sabab bo'lishi mumkin.

Deepfake texnologiyasi yolg'on video va audio yaratib, odamlarning obro'siga putur yetkazish, shantaj qilish yoki dezinformatsiya tarqatish uchun ishlatilmoqda.

3.5. Milliy xavfsizlik tahdidlari

Davlat darajasidagi kiberhujumlar milliy xavfsizlik uchun jiddiy tahdid hisoblanadi. Harbiy tizimlar, razvedka ma'lumotlari va davlat sirlari kiberhujumlar orqali o'g'irlanishi mumkin.

Shuningdek, saylovlarga aralashish, propaganda tarqatish va ijtimoiy bo'linish yaratish uchun ham kiberhujumlar qo'llanilmoqda. 2016-yilgi AQSH saylovlariga aralashish mojarosi buni aniq ko'rsatdi.

4. Kiberjinoyatchilikdan himoyalanish choralari

4.1. Kuchli parollar va ikki faktorli autentifikatsiya

Kuchli parol kamida 12 belgidan iborat bo'lib, katta va kichik harflar, raqamlar va maxsus belgilarni o'z ichiga olishi kerak. Har bir xizmat uchun noyob parol ishlatish muhimdir.

Ikki faktorli autentifikatsiya (2FA) qo'shimcha xavfsizlik qatlami qo'shadi. Faqat parol bilan emas, balki telefon orqali kod yoki autentifikatsiya ilovasi orqali tasdiqlash ham talab qilinadi.

Parol menejerlari (1Password, LastPass, Bitwarden) barcha parollarni xavfsiz saqlash va boshqarish imkonini beradi. Ular murakkab parollar yaratish va avtomatik to'ldirish funktsiyasiga ega.

4.2. Dasturiy ta'minotni muntazam yangilab turish

Operatsion tizim (Windows, macOS, Linux), brauzer, antivirus va boshqa dasturlarni muntazam yangilab turish xavfsizlik zaifliklarini yopishga yordam beradi.

Avtomatik yangilanishni yoqish tavsiya etiladi. Ishlab chiqaruvchilar xavfsizlik tuzatishlarini chiqargandan keyin imkon qadar tezda o'rnatish kerak.

4.3. Antivirus va xavfsizlik dasturlari

Ishonchli antivirus dasturini o'rnatish va uni muntazam yangilab turish asosiy himoya choralaridan biri. Zamonaviy antivirus dasturlari zararli dasturlarni aniqlash, blokirovka qilish va yo'q qilish qobiliyatiga ega.

Firewall (xavfsizlik devori), anti-malware, anti-spyware va boshqa xavfsizlik vositalari ham qo'shimcha himoya beradi. Korporativ tizimlar uchun EDR (Endpoint Detection and Response) va SIEM (Security Information and Event Management) tizimlari tavsiya etiladi.

4.4. Xavfsiz internet foydalanish odatlari

Shubhali elektron pochta xabarlaridagi havolalar va ilovalarni ochmang. Noma'lum manbalarga ishonmang va shoshilinch xabarlar bilan aldanmang.

Faqat ishonchli veb-saytlardan dastur va fayllarni yuklang. HTTPs protokoli bilan ishlaydigan saytlardan foydalaning (sayt manzilida qulf belgisi bo'lishi kerak).

Jamoat Wi-Fi tarmoqlaridan ehtiyot bo'ling. Maxfiy operatsiyalar (bank operatsiyalari, parol kirish) uchun VPN (Virtual Private Network) dan foydalaning.

4.5. Ma'lumotlarni zaxiralash va shifrlash

Muhim ma'lumotlarni muntazam ravishda tashqi qattiq diskka yoki bulut xizmatlariga zaxiralang. 3-2-1 qoidasini qo'llang: 3 nusxa (asl + 2 zaxira), 2 xil muhitda, 1 tasi internetda.

Maxfiy ma'lumotlarni shifrlash orqali himoya qiling. Full disk encryption (butun diskni shifrlash) va file encryption (fayl shifrlash) usullaridan foydalaning.

4.6. Xodimlarni o'qitish va xabardor qilish

Tashkilotlar uchun eng zaif halqa – odamlar. Xodimlarni kiberjinoyatchilik turlari, phishing hujumlari va xavfsiz internet foydalanish qoidalari haqida o'qitish muhimdir.

Muntazam xavfsizlik treninglari, simulatsion phishing testlari va hodisalarga javob berish mashqlari (incident response drills) tashkilot xavfsizligini sezilarli darajada oshiradi.

4.7. Tizim monitoringi va hodisalarga javob berish

Tarmoq faoliyatini doimiy monitoring qilish, g'ayritabiiy xatti-harakatlarni aniqlash va tezkor javob berish zarur. SIEM tizimlari barcha xavfsizlik hodisalarini to'playdi va tahlil qiladi.

Incident Response Plan (hodisalarga javob berish rejasi) tuzish va uni muntazam sinab ko'rish muhimdir. Kiberhujum sodir bo'lganda, tashkilot qanday harakat qilishini oldindan bilishi kerak.

4.8. Qonunchilik va tartibga solish

Davlatlar kiberjinoyatchilik bilan kurashish uchun qonunlar qabul qilmoqdalar. GDPR (Evropa), CCPA (Kaliforniya) va boshqa qonunlar ma'lumotlar himoyasini tartibga soladi va buzilganlik uchun katta jarimalar belgilaydi.

Xalqaro hamkorlik ham muhim. Kiberjinoyatchilik global muammo bo'lgani uchun, davlatlararo ma'lumot almashish, qonunchilik uyg'unligi va birgalikda tergov o'tkazish zarur.

Xulosa

Kiberjinoyatchilik zamonaviy raqamli dunyoning eng jiddiy muammolaridan biridir. U shaxslar, biznes va davlatlar uchun katta xavf tug'diradi. Moliyaviy yo'qotishlar, shaxsiy ma'lumotlar o'g'irlanishi, ishonchning yo'qolishi va milliy xavfsizlik tahdidlari – bularning barchasi kiberjinoyatchilik oqibatlaridir.

Hujumchilar doimiy ravishda yangi usullar va texnologiyalarni ishlab chiqmoqdalar. Shuning uchun himoyalanish ham doimiy jarayon bo'lishi kerak. Bir martalik choralar kifoya qilmaydi – doimiy monitoring, yangilanish va o'rganish zarur.

Kiberjinoyatchilikdan samarali himoyalanish uchun quyidagi choralar muhim:

- Kuchli parollar va ikki faktorli autentifikatsiya ishlatish;
- Dasturiy ta'minotni muntazam yangilab turish;
- Antivirus va xavfsizlik dasturlarini o'rnatish;
- Xavfsiz internet foydalanish odatlarini rivojlantirish;
- Ma'lumotlarni zaxiralash va shifrlash;
- Xodimlarni o'qitish va xabardor qilish;
- Tizim monitoringi va hodisalarga tezkor javob berish;
- Qonunchilik va tartibga solishni qo'llab-quvvatlash.

Esingizda bo'lsin: kiberjinoyatchilikdan himoyalanish faqat texnologiya masalasi emas – bu odamlar, jarayonlar va texnologiyalarning kombinatsiyasidir. Eng kuchli xavfsizlik tizimi ham insoniy xato tufayli buzilishi mumkin.

Shaxsiy xavfsizlik har bir foydalanuvchining mas'uliyatidir. Oddiy xavfsizlik qoidalariga rioya qilish ko'pgina hujumlardan himoya qilishi mumkin. Ehtiyotkorlik, bilim va to'g'ri amallar – raqamli xavfsizlikning kaliti.

Kelajakda kiberjinoyatchilik yanada murakkablashishi kutilmoqda. Sun'iy intellekt, kvant kompyuterlari va IoT qurilmalari yangi xavflar yaratmoqda. Shuning uchun doimiy ravishda o'rganish, moslashish va himoya strategiyalarini yangilab turish zarur.

Jamiyat sifatida biz raqamli xavfsizlikni jiddiy qabul qilishimiz va barcha darajada – shaxsiy, korporativ va davlat – samarali choralar ko'rishimiz kerak.

Faqat shunda raqamli dunyoning barcha imkoniyatlaridan xavfsiz va ishonchli foydalanishimiz mumkin bo'ladi.