**Kirish**

Ushbu analitik hisobot kichik IT kompaniyasida kiberxavfsizlik bo'yicha mutaxassis sifatida faoliyat yuritayotgan muallif tomonidan tayyorlangan bo'lib, elektron tijorat bilan shug'ullanuvchi mijozning yaqinda duch kelgan kiberhujumini tahlil qilishga bag'ishlangan. Hisobotning asosiy maqsadi hujumning mohiyatini aniqlash, potensial zaifliklarni ko'rib chiqish, himoyalanish va axborotni kafolatlash choralarini baholash, tashkilotning hodisalarga javob berish usullarini o'rganish hamda soha standartlari va qonuniy asoslarni tahlil qilishdan iborat.

Ssenariyga ko'ra, universitetni yaqinda tamomlagan kiberxavfsizlik mutaxassisi sifatida, muallif kompaniyaning mijozlaridan biri bo'lgan elektron tijorat korxonasining kiberhujumga uchrashi natijasida yuzaga kelgan vaziyatni o'rganib chiqadi. Hujum oqibatida mijozlarning shaxsiy ma'lumotlari, jumladan login va bank karta ma'lumotlari o'g'irlangan.

Ushbu hisobotda keltirilgan raqamli tahlil va xulosalar kompaniyaga kelgusida shunday xavflarning oldini olish va ularning oqibatlarini bartaraf etish bo'yicha amaliy tavsiyalar berishga qaratilgan.

Ushbu kirish qismi hisobotingizning boshlang'ich nuqtasi bo'ladi. Keyingi bo'limlarda har bir o'rganish maqsadini batafsil yoritib borishingiz mumkin.

**P1. Zararli va/yoki jinoiy kiber faoliyat turlarini ko'rib chiqish (LO1)**

Kiberjinoyatchilik va zararli kiber faoliyat turlari juda xilma-xil bo'lib, turli maqsadlar va usullar bilan amalga oshirilishi mumkin. Ushbu hujum kontekstida quyidagi faoliyat turlari ehtimolga yaqin:

* **Ma'lumotlar buzilishi (Data Breach):** Bu shaxsiy ma'lumotlar, moliyaviy ma'lumotlar yoki boshqa maxfiy ma'lumotlarning ruxsatsiz qo'lga kiritilishi, nusxalanishi, uzatilishi yoki foydalanishidir. Mijozning holatida login va bank karta ma'lumotlarining o'g'irlanishi aynan shu turga kiradi.
* **Fishing (Phishing):** Soxta elektron pochta xabarlari, SMS yoki veb-saytlar orqali foydalanuvchilarni aldab, ularning login, parollar va boshqa shaxsiy ma'lumotlarini qo'lga kiritishga qaratilgan usul. Bu hujum vektorlaridan biri bo'lishi mumkin.
* **Veb-saytga hujumlar:**
  + **SQL injeksiyasi:** Veb-saytning ma'lumotlar bazasiga zararli SQL kodini kiritish orqali ma'lumotlarni o'g'irlash yoki o'zgartirish.
  + **Cross-Site Scripting (XSS):** Zararli skriptlarni veb-saytga joylashtirish orqali boshqa foydalanuvchilarning brauzerida ishga tushirish va ularning ma'lumotlarini o'g'irlash.
  + **Denial of Service (DoS) va Distributed Denial of Service (DDoS) hujumlari:** Veb-sayt yoki onlayn xizmatni haddan tashqari yuklab qo'yish orqali uni qonuniy foydalanuvchilar uchun mavjud bo'lmay qolishiga olib kelish. (Bu holatda ma'lumot o'g'irlanmagan bo'lsa ham, biznesga zarar yetkazishi mumkin).
* **Zararli dasturlar (Malware):** Kompyuter tizimlariga zarar yetkazish, ma'lumotlarni o'g'irlash yoki tizimni boshqarishni qo'lga kiritish uchun yaratilgan dasturlar (viruslar, qurtlar, troyanlar, ransomware va boshqalar).
* **Ichki tahdidlar (Insider Threats):** Kompaniyaning ichki xodimlari tomonidan (intentional yoki accidental) qilingan zararli harakatlar.

**P2. Kiberjinoyatchilikning potentsial maqsadlarini oʻrganish (LO2)**

Kiberjinoyatchilikning maqsadlari turlicha bo'lishi mumkin, jumladan:

* **Moliyaviy daromad olish:** Kredit karta ma'lumotlarini sotish, to'lovlarni o'g'irlash, ransomware orqali pul talab qilish. Ushbu holatda o'g'irlangan bank karta ma'lumotlari moliyaviy motivni ko'rsatadi.
* **Shaxsiy ma'lumotlarni o'g'irlash (Identity Theft):** O'g'irlangan shaxsiy ma'lumotlardan noqonuniy maqsadlarda foydalanish (masalan, soxta hisoblar ochish, kredit olish).
* **Intellektual mulkni o'g'irlash:** Kompaniyaning sirli ma'lumotlari, texnologiyalari yoki boshqa qimmatli ma'lumotlarini raqobatchilarga sotish yoki o'z foydasiga ishlatish.
* **Siyosiy yoki ijtimoiy sabablar (Haktivizm):** Ma'lum bir tashkilotga yoki hukumatga norozilik bildirish maqsadida hujum qilish.
* **Raqobat:** Raqobatchining faoliyatini buzish yoki unga zarar yetkazish.
* **Kiber josuslik:** Davlatlar yoki tashkilotlar tomonidan boshqa davlatlar yoki tashkilotlar haqida ma'lumot to'plash.

Elektron tijorat korxonasiga qilingan bu hujumda asosiy maqsad, ehtimol, **moliyaviy daromad olish** va **shaxsiy ma'lumotlarni o'g'irlash** bo'lgan, chunki login va bank karta ma'lumotlari o'g'irlangan.

**M1. Raqamli tizimlar tushunchasini kiber xavfsizlik bilan bog'liq bo'lgan "maqsadlar" va "vositalar" deb tahlil qiling, haqiqiy dunyo misollarini keltiring (LO1 & LO2)**

Raqamli tizimlar kiberxavfsizlik nuqtai nazaridan ham "maqsadlar", ham "vositalar" sifatida qaralishi mumkin:

* **Raqamli tizimlar - Maqsadlar:**
  + **Ta'rif:** Raqamli tizimlar deganda kompyuterlar, serverlar, tarmoq uskunalari, mobil qurilmalar, veb-saytlar, ma'lumotlar bazalari va ular ishlaydigan dasturiy ta'minotlar majmui tushuniladi. Ushbu tizimlar tashkilotlar va shaxslar uchun muhim ma'lumotlarni saqlaydi, qayta ishlaydi va uzatadi.
  + **Kiberjinoyatchilikdagi roli:** Kiberjinoyatchilarning asosiy maqsadi ushbu tizimlarga ruxsatsiz kirish, ulardagi ma'lumotlarni o'g'irlash, o'zgartirish, yo'q qilish yoki ularning ishlashini buzishdir.
  + **Haqiqiy dunyo misollari:**
    - Elektron tijorat saytining ma'lumotlar bazasi (bizning ssenariyimizda login va karta ma'lumotlarining o'g'irlanishi).
    - Banklarning serverlari (pul mablag'larini o'g'irlashga urinishlar).
    - Kasalxonalarning ma'lumotlar bazasi (bemorlar haqidagi maxfiy ma'lumotlarning o'g'irlanishi).
    - Energetika kompaniyalarining boshqaruv tizimlari (infratuzilmaga zarar yetkazishga urinishlar).
* **Raqamli tizimlar - Vositalar:**
  + **Ta'rif:** Kiberjinoyatchilar o'z maqsadlariga erishish uchun mavjud raqamli tizimlardan foydalanishlari mumkin. Bunga zararli dasturlarni tarqatish, hujumlarni tashkil qilish yoki o'g'irlangan ma'lumotlarni sotish uchun ishlatiladigan tizimlar kiradi.
  + **Kiberjinoyatchilikdagi roli:** Kiberjinoyatchilar boshqa kompyuterlarni yoki serverlarni buzib kirib, ularni o'z hujumlarini amalga oshirish uchun "botnet" deb ataladigan tarmoqqa birlashtirishlari mumkin. Shuningdek, ular o'g'irlangan ma'lumotlarni sotish uchun internet platformalaridan foydalanadilar.
  + **Haqiqiy dunyo misollari:**
    - Botnetlar orqali uyushtirilgan DDoS hujumlari (ko'plab buzilgan kompyuterlar birgalikda bitta serverga hujum qiladi).
    - Fishing hujumlarida soxta elektron pochta xabarlarini yuborish uchun buzilgan elektron pochta serverlaridan foydalanish.
    - Ransomware dasturlarini tarqatish uchun buzilgan veb-saytlar yoki elektron pochta ilovalari.
    - O'g'irlangan ma'lumotlarni sotish uchun Dark Web platformalaridan foydalanish.

**D1. Zararli kiber faoliyat turlarini va kiber tahdid aktyorlarini neytrallashtirish uchun amalga oshirilishi mumkin bo'lgan choralarni baholash (LO1 & LO2)**

Zararli kiber faoliyat turlari va kiber tahdid aktyorlarini neytrallashtirish uchun keng qamrovli choralar majmuasi talab etiladi. Ushbu choralar texnik, tashkiliy va huquqiy yo'nalishlarni o'z ichiga olishi kerak:

* **Texnik choralar:**
  + **Kuchli xavfsizlik devorlari va kirishni aniqlash/oldini olish tizimlarini (IDS/IPS) joriy etish va sozlash:** Tarmoq trafigini filtrlash va zararli harakatlarni bloklash.
  + **Muntazam zaifliklarni skanerlash va bartaraf etish:** Tizimlardagi xavfsizlik kamchiliklarini aniqlash va ularni tuzatish.
  + **Dasturiy ta'minotni muntazam yangilab turish:** Dasturiy ta'minot ishlab chiquvchilari tomonidan chiqarilgan xavfsizlik patchlarini o'rnatish.
  + **Ma'lumotlarni shifrlash:** Maxfiy ma'lumotlarni ruxsatsiz kirishdan himoyalash.
  + **Ko'p faktorli autentifikatsiya (MFA)ni joriy etish:** Hisoblarga ruxsatsiz kirishni qiyinlashtirish.
  + **Zararli dasturlarga qarshi dasturlardan foydalanish va ularni muntazam yangilab turish.**
  + **Veb-sayt xavfsizligini ta'minlash uchun WAF (Web Application Firewall)dan foydalanish.**
  + **Ma'lumotlarni zaxiralash va tiklash tizimlarini joriy etish:** Hujum natijasida yo'qolgan ma'lumotlarni tiklash imkoniyatini yaratish.
  + **Hodisalarga javob berish uchun texnik vositalarni (masalan, loglarni tahlil qilish tizimlari) joriy etish.**
* **Tashkiliy choralar:**
  + **Kiberxavfsizlik siyosatini ishlab chiqish va joriy etish:** Barcha xodimlar uchun xavfsizlik qoidalarini belgilash.
  + **Xodimlarni kiberxavfsizlik bo'yicha muntazam ravishda o'qitish va xabardor qilish:** Fishing, kuchsiz parollar va boshqa xavflar haqida ma'lumot berish.
  + **Kuchli parollar siyosatini o'rnatish va majburiy qilish.**
  + **Ma'lumotlarga kirish huquqini cheklash (minimal zaruriyat prinsipi).**
  + **Muntazam xavfsizlik auditlarini o'tkazish (ichki va tashqi).**
  + **Hodisalarga javob berish rejasini ishlab chiqish, sinovdan o'tkazish va takomillashtirish.**
  + **Kiberxavfsizlik bo'yicha sug'urta qilish (agar zarur bo'lsa).**
* **Huquqiy choralar:**
  + **Huquqni muhofaza qilish organlari bilan hamkorlik qilish:** Kiberjinoyatlarni tergov qilish va aybdorlarni javobgarlikka tortish.
  + **Kiberjinoyatlarga qarshi kurashish bo'yicha milliy va xalqaro qonunchilikka rioya qilish.**
  + **Yetkazuvchilar va hamkorlar bilan kiberxavfsizlik bo'yicha kelishuvlarga erishish.**

Ushbu choralar birgalikda qo'llanilganda zararli kiber faoliyat va tahdid aktyorlarini neytrallashtirishda sezilarli ta'sir ko'rsatishi mumkin. Biroq, kiber tahdidlar doimiy ravishda rivojlanib borayotganini unutmaslik kerak, shuning uchun xavfsizlik choralarini muntazam ravishda yangilab va takomillashtirib turish zarur.

**P5. Axborotni kafolatlash tushunchalari ICT infrastrukturasidagi tahdid va zaifliklarni qanday yengillashtirishi mumkinligini tushuntirib bering, misollar keltiring.**

Axborotni kafolatlash (Information Assurance - IA) deganda axborot tizimlarining konfidentsialligini, butunligini va mavjudligini ta'minlashga qaratilgan kompleks choralar majmui tushuniladi. Ushbu tushunchalar ICT (Axborot-kommunikatsiya texnologiyalari) infratuzilmasidagi turli tahdid va zaifliklarni samarali ravishda yengillashtirishga yordam beradi. Keling, asosiy tushunchalarni va ularning amaliy misollarini ko'rib chiqamiz:

* **Konfidentsiallik (Confidentiality):** Ma'lumotlarga faqat vakolatli shaxslarning kirishini ta'minlash. Bu, ayniqsa, elektron tijorat sohasida mijozlarning shaxsiy va to'lov ma'lumotlari kabi sezgir axborotlarni himoya qilish uchun juda muhimdir.
  + **Yengillashtirish:** Shifrlash texnologiyalari ma'lumotlarni ruxsatsiz shaxslar uchun o'qib bo'lmaydigan formatga o'zgartirish orqali konfidentsiallikni ta'minlaydi. Kirishni boshqarish mexanizmlari (masalan, parollar, biometrik autentifikatsiya, smart-kartalar) faqat tasdiqlangan foydalanuvchilarga tizim va ma'lumotlarga kirishga ruxsat beradi. Tarmoq segmentatsiyasi esa, agar bir tizim buzib kirilgan bo'lsa ham, boshqa tizimlarga tarqalish xavfini cheklaydi.
  + **Misol:** Elektron tijorat veb-sayti HTTPS protokolini ishlatadi, bu esa mijozning brauzeri va veb-server o'rtasidagi ma'lumotlar almashinuvini shifrlaydi va MITM (o'rtadagi odam) hujumlaridan himoya qiladi. Mijozlarning bank karta ma'lumotlari esa ma'lumotlar bazasida kuchli shifrlash algoritmlari yordamida saqlanadi.
* **Butunlik (Integrity):** Ma'lumotlarning ruxsatsiz o'zgartirilishi, yo'q qilinishi yoki buzilishidan himoyalanganligini ta'minlash. Bu, ayniqsa, mahsulot kataloglari, narxlari va tranzaksiya yozuvlari kabi muhim biznes ma'lumotlari uchun juda muhimdir.
  + **Yengillashtirish:** Fayllarning xesh-funksiyalari yoki raqamli imzolari ma'lumotlarning o'zgartirilmaganligini tekshirish imkonini beradi. Versiyalarni boshqarish tizimlari ma'lumotlardagi har qanday o'zgarishlarni kuzatish va qaytarish imkoniyatini beradi. Kirishni boshqarish mexanizmlari faqat vakolatli foydalanuvchilarga ma'lumotlarni o'zgartirishga ruxsat beradi.
  + **Misol:** Elektron tijorat platformasidagi mahsulot narxlari ma'lumotlar bazasida saqlanadi va har qanday o'zgarish log qilinadi. Muhim biznes fayllari muntazam ravishda zaxiralanadi, shuning uchun buzilish yoki yo'qotish holatlarida ularni tiklash mumkin.
* **Mavjudlik (Availability):** Vakolatli foydalanuvchilarning ma'lumotlar va resurslarga kerakli vaqtda kirish imkoniyatiga ega bo'lishini ta'minlash. Bu elektron tijorat veb-saytining doimiy ravishda ishlashi va mijozlarga xizmat ko'rsatishi uchun juda muhimdir.
  + **Yengillashtirish:** Serverlarning ortiqchaligi (redundancy) va failover mexanizmlari server ishdan chiqqan taqdirda ham tizimning ishlashini davom ettirish imkoniyatini beradi. Yukni muvozanatlashtirish (load balancing) texnologiyalari serverlarga tushadigan yukni taqsimlaydi va ularning ortiqcha yuklanishining oldini oladi. DDoS hujumlaridan himoyalanish choralarini ko'rish veb-saytning ishdan chiqishining oldini oladi.
  + **Misol:** Elektron tijorat kompaniyasi o'zining veb-serverlarini bir nechta geografik joylarda joylashtiradi va yukni muvozanatlashtirish tizimini ishlatadi. Agar asosiy server ishdan chiqsa, trafik avtomatik ravishda boshqa serverga yo'naltiriladi.
* **Autentifikatsiya va Autorizatsiya:** Foydalanuvchining kimligini tasdiqlash (autentifikatsiya) va unga qanday resurslarga kirishga ruxsat berilganligini aniqlash (autorizatsiya) orqali ruxsatsiz kirish va harakatlarning oldini olish.
  + **Yengillashtirish:** Kuchli parollar siyosati, ko'p faktorli autentifikatsiya (MFA), biometrik autentifikatsiya kabi usullar autentifikatsiyaning ishonchliligini oshiradi. Rolga asoslangan kirishni boshqarish (RBAC) esa har bir foydalanuvchiga faqat o'z vazifalari uchun zarur bo'lgan resurslarga kirish huquqini beradi.
  + **Misol:** Elektron tijorat platformasida mijozlar o'z akkauntlariga kirish uchun login va parol bilan birga SMS orqali kelgan bir martalik kodni ham kiritishlari kerak (MFA). Administratorlar esa faqat o'z vazifalarini bajarish uchun zarur bo'lgan server konfiguratsiyalariga kirish huquqiga ega.

**M3. Axborotni kafolatlash ICT infratuzilmasining kiber o'zgaruvchanligini qanday oshirishi mumkinligini bahola.**

Axborotni kafolatlash konsepsiyalari ICT infratuzilmasining kiber o'zgaruvchanligini sezilarli darajada oshiradi. Kiber o'zgaruvchanlik deganda infratuzilmaning kiberhujumlar, nosozliklar yoki boshqa disruptiv voqealarga qaramay o'zining asosiy funksiyalarini bajarish, ulardan tezda tiklanish va moslashish qobiliyati tushuniladi.

* **Chidamlikni oshirish:** Konfidentsiallikni ta'minlash orqali ma'lumotlar buzib kirilgan taqdirda ham ularning qiymati kamayadi. Butunlikni ta'minlash orqali hujumchilarning tizimga zarar yetkazish yoki ma'lumotlarni o'zgartirish imkoniyati cheklanadi. Mavjudlikni ta'minlash orqali esa, hatto hujum sodir bo'lgan taqdirda ham xizmatlarning uzluksiz ishlashi kafolatlanadi. Autentifikatsiya va autorizatsiya ruxsatsiz kirishning oldini oladi va ichki tahdidlarni kamaytiradi.
* **Tez tiklanishni ta'minlash:** Axborotni kafolatlash doirasida amalga oshiriladigan muntazam zaxiralash va tiklash mexanizmlari hujum natijasida yo'qolgan ma'lumotlarni tezda qayta tiklash imkoniyatini beradi. Hodisalarga javob berish rejalari esa hujumga tez va samarali javob berish, uning tarqalishini cheklash va zararni minimallashtirishga yordam beradi.
* **Moslashuvchanlikni oshirish:** Axborotni kafolatlash doimiy ravishda yangilanib turishni talab qiladi. Yangi tahdidlar paydo bo'lishi bilan himoya choralarini takomillashtirish zarur. Tahdid razvedkasi orqali yangi tahdidlar haqida oldindan ma'lumot olish va proaktiv choralar ko'rish imkoniyati yaratiladi.

Umuman olganda, axborotni kafolatlash konsepsiyalari ICT infratuzilmasini nafaqat hujumlardan himoya qiladi, balki hujum sodir bo'lgan taqdirda ham uning barqaror ishlashini ta'minlaydi va tezda tiklanishiga yordam beradi, shu orqali kiber o'zgaruvchanlikni oshiradi.

**D2. Javoban turli tashkilotlar tomonidan kiber xavfsizlik tahdidlariga amalga oshirilgan javoblarni baholash.**

Turli tashkilotlar kiberxavfsizlik tahdidlariga turlicha javob berishlari mumkin, bu ularning hajmi, soha xususiyatlari, resurslari va xavfni boshqarish strategiyalariga bog'liq. Keling, turli tashkilotlar tomonidan amalga oshirilgan javoblarni baholaymiz:

* **Kichik va o'rta biznes (KOB):** Ko'pincha kiberxavfsizlikka yetarli e'tibor bermasliklari yoki bu sohada malakali mutaxassislarga ega bo'lmasliklari mumkin. Javoblar ko'pincha reaktiv bo'lib, hujum sodir bo'lganidan keyin yuzaga kelgan zararni bartaraf etishga qaratilgan bo'ladi. Byudjet cheklanganligi sababli, ular ko'pincha bepul yoki arzon xavfsizlik vositalaridan foydalanadilar.
  + **Baholash:** Bunday yondashuv KOBni jiddiy xavf ostida qoldirishi mumkin, chunki ular hujumlarning oldini olish va ularga samarali javob berish uchun yetarli resurslarga ega emaslar.
* **Yirik korporatsiyalar:** Kiberxavfsizlikka katta investitsiyalar kiritadilar va maxsus xavfsizlik bo'limlariga ega bo'ladilar. Ularning javoblari ko'pincha proaktiv bo'lib, doimiy monitoring, tahdid razvedkasi va hodisalarga javob berishning aniq rejalari mavjud. Ular zamonaviy xavfsizlik texnologiyalaridan foydalanadilar va muntazam ravishda xavfsizlik auditlarini o'tkazadilar.
  + **Baholash:** Yirik korporatsiyalar kiber tahdidlarga qarshi ancha yaxshi tayyorgarlikka ega bo'lsalar ham, ular ham murakkab va maqsadli hujumlarga duch kelishlari mumkin. Javoblarning samaradorligi ularning rejalari va resurslarining to'g'ri yo'naltirilganligiga bog'liq.
* **Davlat tashkilotlari:** Milliy xavfsizlik va muhim infratuzilmani himoya qilish kabi vazifalarga ega. Ularning javoblari ko'pincha koordinatsiyalashgan bo'lib, milliy darajada kiberxavfsizlik siyosatini ishlab chiqish va amalga oshirishni o'z ichiga oladi. Ular tahdid razvedkasi bilan faol shug'ullanadilar va boshqa davlatlar bilan hamkorlik qiladilar.
  + **Baholash:** Davlat tashkilotlari kiberxavfsizlikni ta'minlashda muhim rol o'ynaydi, ammo ularning byurokratik tuzilmalari va turli idoralar o'rtasidagi koordinatsiyaning murakkabligi ba'zan javoblarning tezkorligiga ta'sir qilishi mumkin.

**LO4: Kiber xavfsizlik tahdidlariga hodisalarga javob berish usullarini o'rganib chiqish.**

**P6. Xavfsizlik standartlari, qoidalari va ularning oqibatlarini kamida ikkita sektor bo'yicha tavsiflang.**

Turli sektorlarda kiberxavfsizlikni tartibga soluvchi ko'plab standartlar va qoidalar mavjud. Ularga rioya qilish tashkilotlar uchun muhim ahamiyatga ega.

* **Sektor 1: Moliya sektori**
  + **Standart/Qoida:** **PCI DSS (Payment Card Industry Data Security Standard)** - To'lov kartalari ma'lumotlarini qayta ishlash, saqlash va uzatish bilan shug'ullanuvchi barcha tashkilotlar uchun majburiy bo'lgan standart. Uning maqsadi karta egalarining ma'lumotlarini himoya qilishdir.
  + **Tavsif:** PCI DSS 12 ta asosiy talabdan iborat bo'lib, ular xavfsiz tarmoqni yaratish va saqlash, karta egalari ma'lumotlarini himoya qilish, zaifliklarni boshqarish, kuchli kirishni boshqarish choralarini joriy qilish, tarmoqni muntazam monitoring qilish va testlash, axborot xavfsizligi siyosatini yuritish kabi yo'nalishlarni qamrab oladi.
  + **Oqibatlar:** PCI DSSga rioya qilmaslik moliyaviy jarimalarga, to'lov tizimlari tomonidan xizmat ko'rsatishni to'xtatishga, reputatsiyaning buzilishiga va mijozlar ishonchini yo'qotishga olib kelishi mumkin. Bundan tashqari, ma'lumotlar buzilishi sodir bo'lgan taqdirda, tashkilot katta moliyaviy yo'qotishlarga duch kelishi mumkin.
* **Sektor 2: Sog'liqni saqlash sektori**
  + **Standart/Qoida:** **HIPAA (Health Insurance Portability and Accountability Act)** - AQShda bemorlarning sog'lig'i bilan bog'liq maxfiy ma'lumotlarni (Protected Health Information - PHI) himoya qilishni tartibga soluvchi qonun.
  + **Tavsif:** HIPAA qoidalarida PHIga ruxsatsiz kirish, uni oshkor qilish yoki noto'g'ri foydalanishga yo'l qo'ymaslik bo'yicha talablar belgilangan. U texnik, fizikaviy va ma'muriy xavfsizlik choralarini o'z ichiga oladi.
  + **Oqibatlar:** HIPAAga rioya qilmaslik jiddiy moliyaviy jarimalarga (bir buzilish uchun millionlab dollargacha), jinoiy javobgarlikka (qamoq jazosigacha) va bemorlarning ishonchini yo'qotishga olib kelishi mumkin.

**M4. Kiberjinoyatchilikni to'xtatishda jinoyat va boshqa qonunning rolini tahlil qilish.**

Jinoyat va boshqa qonunlar kiberjinoyatchilikni to'xtatishda muhim rol o'ynaydi, ammo bu sohada bir qator qiyinchiliklar ham mavjud.

* **Jinoiy qonun:** Kiberjinoyatlarni jinoiy javobgarlikka tortish uchun huquqiy asos yaratadi. Ko'pgina mamlakatlarda kompyuterga noqonuniy kirish, ma'lumotlarni o'g'irlash, zararli dasturlarni tarqatish, fishing va boshqa kiber faoliyatlar jinoyat hisoblanadi va tegishli jazo choralari belgilangan. Bu potentsial jinoyatchilarni to'xtatishga yordam berishi mumkin.
* **Boshqa qonunlar:** Shuningdek, shaxsiy ma'lumotlarni himoya qilish, intellektual mulkni himoya qilish va elektron tijoratni tartibga solishga qaratilgan qonunlar ham kiberjinoyatchilikka qarshi kurashishda muhim rol o'ynaydi. Masalan, GDPR (Yevropa Ittifoqi) kabi ma'lumotlarni himoya qilish qonunlari tashkilotlarni shaxsiy ma'lumotlarni himoya qilishga majbur qiladi va buzilish holatlarida jiddiy jarimalar belgilaydi.
* **Qiyinchiliklar:** Kiberjinoyatlarning transchegaraviy xususiyati, jinoyatchilarni aniqlash va ularni javobgarlikka tortishni murakkablashtiradi. Ko'pgina kiberhujumlar bir nechta mamlakatlar orqali amalga oshirilishi mumkin, bu esa huquqni muhofaza qilish organlari o'rtasida xalqaro hamkorlikni talab qiladi. Bundan tashqari, kiberjinoyatchilarning texnik jihatdan yuqori savodxonligi va doimiy ravishda yangi hujum usullarini ishlab chiqishi ularga qarshi kurashishni qiyinlashtiradi.
* **Xalqaro hamkorlik:** Kiberjinoyatchilikka qarshi kurashishda turli mamlakatlar o'rtasidagi hamkorlik juda muhimdir. Ma'lumot almashinuvi, qo'shma operatsiyalar va ekstraditsiya kabi mexanizmlar kiberjinoyatchilarni to'xtatishda va javobgarlikka tortishda yordam beradi.

**P7. Kiber xavfsizlik tahdidlariga javoban amalga oshirilgan javob turlarini tekshirish.**

Kiberxavfsizlik tahdidlariga javoban tashkilotlar tomonidan amalga oshiriladigan javob turlari xilma-xildir va hujumning turi, hajmi va tashkilotning imkoniyatlariga bog'liq bo'ladi. Asosiy javob turlarini ko'rib chiqamiz:

* **Texnik javoblar:**
  + **Ta'sirlangan tizimlarni izolyatsiya qilish:** Hujumning tarqalishini cheklash uchun ta'sirlangan kompyuterlar, serverlar yoki tarmoq segmentlarini ajratish.
  + **Zararli dasturlarni o'chirish:** Zararlangan tizimlardan viruslar, troyanlar, ranzomvar va boshqa zararli dasturlarni aniqlash va yo'q qilish.
  + **Tizimlarni tiklash:** Hujumdan oldingi holatga qaytarish uchun zaxira nusxalaridan foydalanish yoki zararlangan tizimlarni qayta qurish.
  + **Zaifliklarni bartaraf etish:** Hujumga olib kelgan xavfsizlik zaifliklarini aniqlash va ularni tuzatish uchun patchlar o'rnatish yoki konfiguratsiyalarni o'zgartirish.
  + **Kirish huquqlarini qayta ko'rib chiqish:** Hujum natijasida buzilgan bo'lishi mumkin bo'lgan kirish huquqlarini tekshirish va qayta tiklash.
* **Tashkiliy javoblar:**
  + **Hodisalarga javob berish rejasini ishga tushirish:** Oldindan ishlab chiqilgan hodisalarga javob berish protseduralarini amalga oshirish.
  + **Ichki va tashqi kommunikatsiyani yo'lga qo'yish:** Xodimlarni, mijozlarni, hamkorlarni va boshqa manfaatdor tomonlarni hujum haqida xabardor qilish.
  + **Huquqni muhofaza qilish organlariga xabar berish:** Jiddiy kiberjinoyat holatlarida politsiya yoki boshqa tegishli organlarga murojaat qilish.
  + **Regulyatorlarga xabar berish:** Ma'lumotlar buzilishi kabi holatlarda tegishli davlat organlariga xabar berish (qonunchilik talablariga muvofiq).
* **Huquqiy javoblar:**
  + **Yuristlar bilan maslahatlashish:** Hujumning huquqiy oqibatlarini baholash va zaruriy choralar ko'rish bo'yicha maslahat olish.
  + **Tergovga yordam berish:** Huquqni muhofaza qilish organlarining tergov ishlarida ishtirok etish va zarur bo'lgan ma'lumotlarni taqdim etish.
  + **Sudga murojaat qilish:** Hujumchilarga qarshi da'vo arizalari kiritish yoki etkazilgan zararni qoplashni talab qilish.
* **Ommaviy javoblar:**
  + **Jamoatchilik bilan aloqalar:** Ommaviy axborot vositalari orqali voqea haqida xabar berish va kompaniyaning harakatlarini tushuntirish.
  + **Mijozlarni qo'llab-quvvatlash:** Ta'sirlangan mijozlarga yordam ko'rsatish, maslahat berish va ularning xavfsizligini ta'minlash bo'yicha choralar ko'rish.
  + **Reputatsiyani tiklashga qaratilgan harakatlar:** Mijozlar ishonchini qaytarish va kompaniyaning obro'sini tiklash uchun marketing va PR kampaniyalarini o'tkazish.

**Xulosa**

Ushbu analitik hisobot elektron tijorat sohasidagi kichik bir IT kompaniyasining mijoziga qarshi sodir etilgan kiberhujumning har tomonlama tahlilini taqdim etdi. Hujumning potentsial turlari va uni amalga oshirgan tahdid aktyorlari, shuningdek, kompaniyaning AKT infratuzilmasidagi zaif nuqtalar va hujumning ehtimoliy nishonlari batafsil ko'rib chiqildi. Hisobotda himoyalanish va axborotni kafolatlash bo'yicha mavjud choralar, shuningdek, bunday holatlarda tashkilotning to'g'ri javob berish usullari tahlil qilindi. Kiberxavfsizlik sohasidagi amaldagi standartlar va qonuniy asoslar ham o'rganilib, ushbu sohada faoliyat yuritayotgan kompaniyalar uchun ularga rioya qilishning muhimligi ta'kidlandi. Yakuniy xulosa sifatida shuni aytish mumkinki, kiberxavfsizlikka etarli e'tibor qaratish, proaktiv himoya choralarini ko'rish va hodisalarga tayyor bo'lish har qanday tashkilot, ayniqsa elektron tijorat bilan shug'ullanuvchi korxonalar uchun hayotiy zaruratdir. Keltirilgan tavsiyalar kompaniya va uning mijozlariga kelgusida kiberxavfsizlik xavflarini minimallashtirish va agar hujum sodir bo'lsa, uning oqibatlarini tez va samarali tarzda bartaraf etishga yordam beradi.

References

1. Fowler, M., 2004. Inversion of Control Containers and the Dependency Injection pattern. [online] Available at: <https://martinfowler.com/articles/injection.html> [Accessed 30 May 2025].
2. Goodrich, B., 2016. *Python for Cybersecurity: Learn to use Python to Enhance your Cybersecurity Skills*. Syngress.
3. Vacca, J.R., 2019. *Computer and Information Security Handbook*. 3rd ed. Morgan Kaufmann.
4. Kshetri, N., 2017. Cybercrime and Cybersecurity in the Global Economy. *Journal of Global Information Management*, 25(1), pp. 72-94.
5. Weber, R.H. and Weber, R.H., 2010. The legal framework of cloud computing. *Computer Law & Security Review*, 26(6), pp. 585-591.
6. Stallings, W. and Brown, L., 2018. *Computer Security: Principles and Practice*. 4th ed. Pearson.
7. The European Parliament and the Council of the European Union, 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [online] Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [Accessed 30 May 2025].