# AXBOROT XAVFSIZLIGI TALABLARI BO'YICHA KORPORATIV TARMOQLARDA KIBERXAVFSIZLIKNI TA'MINLASH

**Odilov Ozodbek Raxmatillo o'g'li**
*Toshkent axborot texnologiyalari unversiteti*

**Annotatsiya**: *Ushbu maqolada kiberxavfsizlikni ta'minlash uchun xavfsizlikni bartaraf etadigan virus turlari haqida ogohlik o'rgatilgan , asl va qalbaki saytlardan ogoh bo'lish va insonning xissiyotlari orqali xujum qiladigan buzg'unchi va saytlardan xabardor bo'lish o'rgatilgan.*

**Kalit so'zlar**: *Yolg'on saytlar, asosiy maqsadlar, malware , DNS Spoofing, ransomware, fishing , spear fishing, parol tekshirish, Domain Name System,*
Brute Force.

Korparativ tarmoqlarga suqilib kirish usullari

Fishing hujumi, elektron pochta yoki boshqa kommunikatsiya vositalari orqali foydalanuvchilarni jalb qilish va ularning shaxsiy axborotlarini olish uchun qo'llaniladigan o'zgaruvchan va odatda zararli taktika hisoblanadi. Ushbu hujum turini o'rganish, har qanday korporatsiyani taqib qilib, xavfsizlikni ta'minlash va xodimlarni ma'lumotlarni himoya qilish uchun juda muhimdir. Quyidagi xususiyatlar Fishing hujumlari to'g'risida ko'proq malumot beradi:

Hujum Usullari. Fishing hujumlari elektron pochta xabarlari, messaging tizimlari (masalan, WhatsApp yoki Telegram), ijtimoiy tarmoqlar, forumlar va boshqa kommunikatsiya vositalari orqali amalga oshiriladi. Ushbu xabarlarda odatda kompaniya nomi, logotipi yoki rasmiy shakli qo'llaniladi, shuningdek, eng ko'p mijozlar talablari, hisobni tiklash yoki boshqa aktivliklarni amalga oshirish uchun ilova yoki havolalar orqali ishlatiladi.

Fishing xabarlari ko'rsatkichlari odatda xavfsizlikning yuqori darajada bo'lishi uchun foydalanuvchilarni urg'utib qo'yadi. Ular, kompaniyaga qarshi shubha yaratish uchun qiyin o'zlashtirilgan, urg'uli qismlar orqali yuboriladi. Bundan tashqari, ularning ko'rsatkichlarida maqbul kompaniya nomi, logotipi yoki boshqa tashqi ko'rinishlari mavjud bo'ladi.

Yolg'on saytlar. Hujumchilar xavfsizlikning yoki ilova tashxisi bo'yicha yolg'on saytlar ochish orqali foydalanuvchilarni jalb qilishga urinadilar. Ular, asosiy kompaniya saytlari bilan o'xshash yoki juda qiyinlikda tushuncha beradigan domen nomlarini o'z ichiga oladilar.

Fishing xabarlari va saytlari odatda tezroq o'qilib chiqarilgan yoki tez o'chirilgan sahifalarda joylashgan bo'ladi. Bu, foydalanuvchilar tomonidan yuqori ko'rsatkich sifatida aniqlanishi mumkin.

Asosiy maqsadlar. Fishing hujumlari asosan shaxsiy axborotlarni olish, xavfsizlik kalitlari yoki kirish ma'lumotlarini olish, yoki malwareni tizimga kiritish uchun qo'llaniladi. Ushbu hujumlar odatda qarindoshlarning yoki kompaniyadagi ishchilar yoki xodimlar tomonidan qo'llaniladi.

Farming hujumi, hujumchilar tomonidan olib borilgan ushbu taktika tizimga kirishga urinishni o‘z ichiga oladi. Asosan, farming, g‘alati saytlarga olib borilgan foydalanuvchilarning tarmoqni o‘z ichiga olganligini va ularning shaxsiy axborotlarini olish imkoniyatiga ega bo‘ladi. Bu hujum turini o‘rganish, kompaniya tarmoqlarini himoya qilish va xavfsizlikni ta’minlash uchun juda muhimdir. Quyidagi xususiyatlar Farming hujumlari to‘g‘risida ko‘proq malumot beradi:

DNS Spoofing. Farming hujumchilari, g‘alati DNS (Domain Name System) xizmatlaridan foydalanib, kompaniyaga oid domen nomlarini va IP manzillarini almashtirishadi. Bunday qilib, foydalanuvchilar g‘alati saytlarga o‘tishlarini kutib olishadi, ammo haqiqiy kompaniya saytiga o‘tishlari kerak bo‘lgan joylarda.

Farming va fishing hujumlari ko‘proq avj bo‘lishi mumkin. Bir nechta tarmoq xavfsizlik ko‘rsatki bo‘lmasa, hujumchilar foydalanuvchilarni g‘alati saytlarga olib borishga chaqirish uchun fishing amaliyotlaridan foydalanishi mumkin.

Mijozlar uchun g‘alati saytlar yaratish. Farming hujumchilari, asosiy kompaniya sayti bilan o‘xshash domen nomini olish orqali g‘alati saytlar yaratishadi. Ular, shaxsiy axborotlarni olish uchun yuqori darajada shubha yaratishga urinishadi.

Farming hujumlariga qarshi kurashish uchun, kompaniyalar DNS xavfsizligini kuchaytirish, SSL/TLS kengaytmasi bilan xavfsizlikni ta’minlash va foydalanuvchilarga g‘alati saytlardan qayta kirish orqali xavfsizlikni ta’minlash, shuningdek, xavfsizlik bilan bog‘liq ta’limlar berish kerak.

Malware va Ransomware, korporativ tarmoqlarga suqilib kirishda juda ommalashgan zararli dasturlar va viruslar turlaridir. Bu hujumlar kompaniyalar uchun katta xavf va zararlarga sabab bo‘lishi mumkin. Quyidagi xususiyatlar Malware va Ransomware hujumlari haqida ko‘proq malumot beradi:

Malware. Malware, zararli dasturlarning umumiy nomi hisoblanadi va tarmoqlarga kirish uchun ko‘p turdagi zararli dasturlarni o‘z ichiga oladi. Ular viruslar, trojanlar, kripterlar, spywarelar va boshqa zararli dasturlar shaklida bo‘lishi mumkin. Malware, tarmoq tizimlarida ko‘p xavfsizlik muammolari va ma’lumotlarning yo‘qolishiga olib kelishi mumkin.

Ransomware. Ransomware, kompaniyalar uchun maxfiylik muammolari va ma’lumotlarni yo‘qolishga olib keladigan xavfsizlik hujumlarining xususiy turidir. Ushbu hujumda, xavfsizlikni buzish uchun virus tarmoqni qarshiligi maqsadida, hujumchilar kompaniyadagi ma’lumotlarni shifrlash uchun xavfsizlik kalitini yoki kodini olishadi. Keyin, ular ruxsat berish uchun pul so‘raydigan shifrlangan ma’lumotlarni etkazib berishadi.

Tizimlar va ma’lumotlar yo‘qotilishi. Malware va Ransomware, tarmoq tizimlarini buzish, ma’lumotlarni yo‘qotish yoki nazoratini o‘z ichiga oladi. Bu hujumlar kompaniya faoliyatlarini to‘xtatishi va katta miqdorda ma’lumot yo‘qolishi bilan qandaydir kompaniyalarga katta zarar yetkazishi mumkin.

Fishing va Spear Fishing orqali o‘tkazilishi: Malware va Ransomware viruslarining juda ko‘pini fishing va spear fishing hujumlaridan foydalanib, foydalanuvchilarning foydalanishga kiritishini olish uchun o‘rnatiladi. Bu hujumlar, foydalanuvchilarning faqatgina xavfsizlik tavsiflarini kiritishlari bilan amalga oshiriladi.

Boshqaruv va ta'minotning qo'llash imkoniyatini yo'qotish: Ransomware hujumlari tarmoq tizimlarini, serverlarni, ma'lumotlar bazalarini yoki boshqa ma'lumotlarni shifrlash orqali kompaniyadagi faoliyatni to'xtatish va ma'lumot yo'qotish imkonini ta'minlashadi. Bu xavfsizlik hujumlari tarmoq tizimlarini, kompaniya ma'lumotlarini va faoliyatini buzish orqali katta zararlarni keltirishi mumkin.

Ijtimoiy muhandislik (Social engineering) insonlarni shubha yaratish, g'alati maqbul shaxslar sifatida ko'rinadigan axborotlarni olish va kompaniya tarmoqlariga suqilib kirishga urinishdir. Bu hujum usuli, odatda xavfsizlik tizimlarini o'tkazish orqali o'tkaziladi va foydalanuvchilarning kuzatish muhim ahamiyatga ega. Quyidagi xususiyatlar Social Engineering hujumlari to'g'risida ko'proq malumot beradi:

Hujumchilar, elektron pochta, telefon qo'ng'iroqlari yoki messaging tizimlari orqali xodimlarni yoki korporativ foydalanuvchilarni jalb qilish uchun shubhali xabarlar yuborishadi. Bu xabarlar odatda qarindoshlar yoki kompaniyadagi ishchilar sifatida ko'rinadi va xavfsizlik so'roqlarini yoki boshqa axborotlarni talab qiladi.

Yolg'on (Fake) identifikatsiya va ma'lumotlar. Hujumchilar, axborot olish uchun yolg'on identifikatsiya va ma'lumotlar foydalanishadi. Ular o'zlarining boshqa insonlar yoki kompaniyadagi ishchilar sifatida ta'riflanishlari, shuningdek, shubhali axborotlarni olish uchun qo'llaniladi.

Fishing. Ijtimoiy muhandislik hujumchilari odatda fishing xabarlari orqali foydalanuvchilarni g'alati saytlarga olib borishga qo'llaniladi. Ular elektron pochtalar yoki messaging tizimlari orqali g'alati saytlarga olib borish uchun havolalar yuborishadi, shuningdek, foydalanuvchilarni shaxsiy axborotlarni kiritish uchun o'zlarining ma'qullangan saytlarga o'tishiga shubha yaratishadi.

Spear Fishing. Ijtimoiy muhandislik hujumchilari, aynan ma'lum bir shaxs yoki guruhga qaratilgan fishing xabarlari orqali biron bir tarmoqga olish uchun yaxshi samarali fishing xabarlari yuborishadi. Ular, foydalanuvchilarning xavfsizlik hisobini ochish uchun g'alati saytlarga o'tish uchun boshqa qo'llanishni qo'llanishadi.

Brute Force hujumi ya'ni qulaylik bilan amalga oshirilgan biron-bir kirish kalitini topish uchun avtomatik dastur yordamida qo'llaniladi. Bu hujum turining asosiy maqsadi, parol yoki kirish kalitini aniqlash va undan foydalanib tizimga kirishga urinishdir. Quyidagi xususiyatlar Brute Force hujumlari haqida ko'proq malumot beradi:

Parolga kirish uchun Brute Force hujum dasturi, avvalgi bilgan parollarni ishlatib, keyinchalik kirish kalitini aniqlab chiqib, u parolni topish uchun yuzlab, millionlar va hatta milliardlar darajadagi imkoniyatlarni sinovlab chiqadi.

Dastlabki hujum. Brute Force hujumi asosan dastlabki hujumnini olish uchun qo'llaniladi. Agar foydalanuvchi yoki tarmoq tizimi kuchli, katta hajmli parollarga ega bo'lmasa, hujumchilar uning parolini qo'llab-quvvatlash uchun kichikroq qobiliyatdagi parollarni aniqlashga urinishadi.

Brute Force hujum dasturi, parolni topish uchun yuzlab, millionlar va hatta milliardlar darajadagi imkoniyatlarni sinovlab chiqadi, ammo bundan tashqari, ushbu dastur yuzlablar va minglab urinishni tezda ishlab chiqib berishi mumkin.

Parol tekshirish. Brute Force hujum dasturlari, kirish kalitlarini tekshirish va parolni topish uchun o'zgaruvchan bo'lishi mumkin. Ushbu dasturlar, qat'iy qaror kabil parolni aniqlab chiqish orqali tizimga kirishga urinishadi.

Xavfsizlikni buzish. Brute Force hujumlari, agar parol kengaytmasi va kirish kalitlarini cheklangan yo'llar bo'lmasa, tarmoq tizimlariga kirish uchun xavfsizlikni buzish imkonini berishi mumkin. Hujumchilar tizimga kirib o'tish uchun parol topishga o'zgaruvchan imkoniyatni sinovlay oladilar.

Xizmatni rad etish (DoS) va Tarqatilgan xizmatni rad etish (DDoS) hujumlari, yoki xizmatdan mahrum etish hujumlari, kompaniyalar uchun katta xavfsizlik muammolarini yaratadigan hujum turlaridan biri. Bu hujumlar tarmoq tizimlarini yo'qotish, katta trafik oqimi yoki resurslarni sarflash orqali tizimga kirish vaqtimizni cheklash orqali olib boriladi. Quyidagi xususiyatlar DoS va DDoS hujumlari haqida ko'proq malumot beradi:

Xizmatni rad etish (DoS) hujumi. Bu hujum turi, tizimga kirishni vaqtida ta'minlash vaqtini cheklash orqali foydalanuvchilarni xizmatdan mahrum qilishni maqsad qiladi. Hujumchilar odatda kompaniya serverlariga yoki tarmoq tizimiga yolg'on trafikni yuborish orqali tizimni buzishga urinishadi. Bu hujum turi tarmoq tizimlarini bo'shatadi va faol ishlashlarini to'xtatadi.

Tarqatilgan xizmatni rad etish (DDoS) hujumi. DDoS hujumi, DoS hujumining kuchaytirilgan variantidir. Bu hujumda, hujumchilar ko'p qurilmalar (botnet) yoki ko'plab xavfsizlik tizimlarini (zombie tarmoqlar) ishlatadilar, shu sababli hujumni amalga oshirish uchun yuqori darajadagi trafik yuborish imkonini oshirishadi. Bu, tarmoq tizimlarini sarflashga olib kelsa, ularni ishlab chiqarish va qo'llash imkoniyatlarini buzishi mumkin.

Botnet ishlatish. DDoS hujumlarida, hujumchilar ko'p qurilmalar yoki botnet deb nomlangan kuchaytirilgan kompyuter tarmoqlarini ishlatishadi. Bu kompyuterlar hujumchilarning buyurtmasi asosida katta trafikni kompaniya serverlariga yuborish uchun qo'llaniladi.

DoS va DDoS hujumlarida, hujumchilar protokollarni sarflash, serverlar va tarmoq tizimlari resurslarini sarflash orqali foydalanuvchilarni xizmatdan mahrum qilish uchun harakat qiladi. Ular kompaniya serverlarini ishdan chiqaradi va tarmoq tizimlarini qo'llash imkoniyatlarini cheklash uchun o'zlarining maqsadlariga erishishadi.

DoS va DDoS hujumlari, foydalanuvchilar uchun axborotlar almashishni yoki foydalanuvchilar bilan interaksiya qilishni to'xtatishi mumkin. Bu hujumlar kompaniya tarmoqlarini xavfsizlik muammolari va ma'lumot yo'qotish muammolari bilan muholif bo'lish uchun katta xavfsizlik choralarini oshirish lozim.

Ichki tahdidlar (Insider Threats) hujumi, kompaniya ichidagi xodimlar yoki tizim administratorlari tomonidan amalga oshirilgan hujum turlaridan biridir. Bu hujumlar tarmoq tizimlariga kirish uchun maslahat olish, ma'lumotlarni o'zgartirish yoki yo'qotish, yoki xavfsizlik hisoblarini ishlatish orqali olib boriladi. Quyidagi xususiyatlar Ichki tahdidlar hujumlari haqida ko'proq malumot beradi:

Ichki tahdidlar hujumlari ma'lumot yo'qotish, yo'qotilganligi yoki o'zgartirilganligi yoki uni qarindosh hujumchilarga taqdim etish orqali amalga oshirilishi mumkin. Bu hujumlar kompaniya ichidagi sirli axborotlarni yo'qotish, kompaniya xavfsizligini buzish, yoki ma'lumotlarni o'zgartirishni maqsad qiladi.

Ichki tahdidlar hujumchilari, korporativ tarmoq tizimlariga kirish uchun o'zlarining ma'lumotlari yoki ma'lumotlarni o'zgartirish uchun foydalanadigan tarmoq tizimi xavfsizlikni buzish uchun korporativ resurslardan foydalanishi mumkin.

Ichki tahdidlar hujumlari, tizim administratorlari, xodimlar yoki boshqa korporativ tizimlarga kirishga ega bo'lgan shaxslar tomonidan amalga oshirilishi mumkin. Ular, o'zlarining huquqiy ruxsatlari orqali kompaniya ichidagi axborotlarga kirib, ularni yo'qotish yoki o'zgartirish imkoniyatiga ega bo'lishlari mumkin.

Ichki tahdidlar hujumlari, kompaniya ichidagi xodimlar yoki tizim administratorlari tomonidan korporativ resurslarni yoki ma'lumotlarni korruptsiya qilish, o'zgartirish yoki yo'qotish orqali tizimga kirish uchun amalga oshirilishi mumkin.

Ichki tahdidlar hujumchilari o'zlarining huquqiy ruxsatlari orqali kompaniya ichidagi axborotlarga kirishga urinishadi. Ular, o'zlarining ma'lumotlari orqali foydalanuvchilarning parollarini olish, ma'lumotlarni yo'qotish yoki o'zgartirish uchun ruxsatlar ishlatishi mumkin.

Ichki tahdidlar hujumlari o'zlarining ruxsatlari orqali kompaniya ichidagi axborotlarga kirishga urinishadi. Bu, kompaniyada qat'iy xavfsizlik choralarini buzishi, korporativ tarmoq tizimlarini buzish, yoki kompaniya xavfsizligini buzishga olib kelishi mumkin.

## FOYDALANILGAN ADABIYOTLAR

1. S.K.Ganiev, T.A.Kuchkarov. Tarmoq xavfsizligi (Mobil tarmoq xavfsizligi). O'quv qo'llanma. –T.: «Aloqachi», 2019, 140 b.
2. S.K.Ganiev, M.M.Karimov, Z.T.Xudoyqulov, M.M.Kadirov. Axborot xavfsizligi bo'yicha atama va tushunchalarning rus, o'zbek va ingliz tillaridagi izohli lug'ati. –T.: «Iqtisod-moliya», - 2017, 480 bet.
3. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –T.: «Fan va texnologiya», 2016, 372 bet.
4. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, -P. – 606.
5. Марков А. С., Барабанов А. В., Дорофеев А. В., Цирлов В.Л. Семь безопасных информационных технологий / под ред. А.С.Маркова. –М.: ДМК Пресс, - 2017. – 224с.
6. D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtoyeva. Kriptografiyaning matematik asoslari. O'quv qo'llanma. –T.: «Aloqachi», 2019, 192 bet.
7. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с.
8. Raef Meeuwisse. Cybersecurity for Beginners (2nd. ed.). Cyber Simplicity Ltd, London, England, 2017, - 224 p.
9. Manjikian M. Cybersecurity ethics: an introduction.– Routledge, 2017, -328 p.

10. Kostopoulos G. Cyberspace and cybersecurity. – CRC Press, 2017, -316 r.
11. Christen M., Gordijn B., Loi M. The Ethics of Cybersecurity.– Springer Nature, 2020. – S. 384.
12. Pande J. Introduction to Cyber Security. Uttarakhand Open University, 2017, -152 p.
13. Cybersecurity Fundamentals Study Guide, ISACA 2015, -196p.
14. Easttom C. Computer security fundamentals. – Pearson IT Certification, 2019, -447 p.
15. Введение в информационную безопасность автоматизированных систем: учебное пособие / В. В. Бондарев. — Москва : Издательство МГТУ им. Н. Э. Баумана, 2016. — 250 с.

## INTERNET MANBALARI

1. Analysis of Intrusion Detection Systems (IDS) https://ukdiss.com/examples/hujumlar-prevention-security.php
2. Comparative study and analysis of network hujumlar detection tools | Semantic Scholar https://www.semanticscholar.org/paper/Comparative-study-and-analysis-of-network-hujumlar-Bhosale-Mane/e9ee6ba38bc03b51c8fa54e3cf0db9de7582e2fd
3. https://www.sdtek.net/8-common-ways-hackers-break-into-computer-systems
4. https://www.memcyco.com/home/threat-detection-techniques/
5. https://www.neumetric.com/host-hujumlar-detection-system/
6. https://www.stamus-networks.com/ids-detection-types
7. https://www.intechopen.com/chapters/88343#B4
8. https://corelight.com/resources/glossary/signature-based-detection
9. https://www.upguard.com/blog/hujumlar-detection-system
10. https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-hujumlar-detection-open-source-tools#install-suricata