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

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

Annotatsiya: *Ushbu maqolada korporativ tarmoqlarni tug'lishi mumkin bo'lgan risklarni oldini olish va xavf soluvchi potensial risklar haqida xodimlarni xabardor qilish , xavfsizlikni ta'minlash va kuchaytirish o'rganilgan*

Kalit so'zlar: *Xavfsizlik devorlari , ko'p faktorli autentifikatsiya , xodimlarni o'qitish , ma'lumotlarni shifrlash, doimiy dasturiy ta'minotni tuzatish , xavfsizlik choralari.*

Korporativ tarmoqlarda kiberxavfsizlikni ta'minlash.

Korporativ tarmoqning xavfsizligi maxfiy ma'lumotlarni himoya qilish va barcha o'lchamdagi tashkilotlarning uzluksiz ishlashini ta'minlash uchun juda muhimdir. Masofaviy ishlashning kuchayishi, zamonaviy muhitlarning murakkabligi va yanada rivojlangan kiber tahdidlarning paydo bo'lishi bilan korxonalar o'z tarmoqlarini, nozik ma'lumotlarini va asosiy tizimlarini himoya qilishlari har qachongidan ham muhimroqdir.

Tashkilotlar o'z tarmoqlari, tizimlari va foydalanuvchilarini bir qancha asosiy kiberxavfsizlik tahdidlaridan himoya qilishlari kerak. Masalan, Verizon 2020 DBIR quyidagilarni aniqladi:

- Huquqbuzarliklarning 70 foizi begonalar tomonidan sodir etilgan
- 45% xakerlik bilan shug'ullangan
- 86% moddiy rag'batlantirildi
- 17% zararli dasturlarning ba'zi shakllari bilan bog'liq va
- 22% fishing yoki ijtimoiy muhandislik bilan shug'ullangan

Kompaniyalar o'zlarining kiberxavfsizlik holatini mustahkamlashga va tarmoq xavfsizligini yaxshilashga intilayotganda, biz taklif qiladigan birinchi narsa odatda zaiflikni baholashdir - ayniqsa oxirgi audit yoki baholashdan keyin biroz vaqt o'tgan bo'lsa. Korporativ tarmog'ingizga tahdid solishi mumkin bo'lgan zaifliklarni aniqlash uchun ish joyingiz texnologiyasi, jarayonlari va siyosatlarining davriy xavfsizlik auditini o'tkazish kerak. Kiberxavfsizlikni baholash texnologik muhitda tuzatishni talab qiladigan har qanday zaifliklarni aniqlash uchun asosiy apparat va tarmoq infratuzilmasi, veb-saytlar, xavfsizlik devori va ilovalarni skanerlaydi.

Korporativ tarmog'i xavfsizligi nuqtai nazaridan , xavfsizlik tekshiruvlari tarmoq portlari va protokollaridagi cheklovlar va boshqaruvlarni, boshqaruv imtiyozlarini ko'rib chiqadi, tarmoqqa ulangan qurilmalarni skanerlaydi va boshqa asosiy xavfsizlik choralari bilan birga xavfsizlik devori konfiguratsiyasini ko'rib chiqadi.

Xavfsizlik devorlari va kirishni oldini olish tizimlari (IPS). Kiruvchi va chiquvchi trafikni boshqarish uchun xavfsizlik devorlarini qo'llaniladi. Firewallar juda ko'p imkoniyatlar, murakkablik va konfiguratsiyalarga ega. Korxona va ichki resurslariga mos keladigan tarmoqni yetarli darajada himoya qilish uchun xavfsizlik devorlarining to'g'ri turini tanlash

ba'zi korxonalar uchun qiyin bo'lishi mumkin. Ular kerakli tarmoq trafigiga to'sqinlik qilmasdan kiber tahdidlarning oldini olish uchun muntazam texnik xizmat ko'rsatish va tuzatishlarni talab qiladi. Agar ichki xavfsizlik devorini saqlash ko'nikmalariga ega bo'lmagan korxonalar boshqariladigan xavfsizlik devori xizmatlaridan foydalanadi.

Kirish nazorati va ko'p faktorli autentifikatsiya (MFA). Foydalanuvchilarning kuchli, noyob parollar yaratishini ta'minlash va asosiy ilovalar va platformalarda ko'p faktorli autentifikatsiyani (MFA) yoqishni ko'rib chiqish uchun siyosatlar o'rnatiladi. TIV parolga asoslangan zaifliklar xavfini sezilarli darajada kamaytiradi va korxonalar o'zlarini himoya qilish uchun foydalanishi mumkin bo'lgan arzonroq xavfsizlik choralaridan biridir va kompaniya tarmog'i va tizimlariga xavfsizroq masofadan kirish imkonini beradi.

Ish rollari va mas'uliyatlari asosida nozik ma'lumotlarga kirishni cheklash. Ushbu hududlarga xavfni cheklash uchun guruhlar ma'lumotlar, tizimlar va umumiy joylarga kirishlari mumkin bo'lgan aniq arxitektura yaratiladi. Xodimlarning ketishi, kelishi va turli guruhlar o'rtasida o'tkazilganda ruxsatni o'zgartirish qoidalariga rioya qilinganligiga ishonch hosil qilish kerak. Ushbu o'zgarishlar asosida kirishni qayta ko'rib chiqish kerak.

Xodimlarni o'qitish va xabardor qilish. Xodimlarni fishing elektron pochta xabarlarini aniqlash va maxfiy ma'lumotlarni himoya qilish kabi xavfsizlikning eng yaxshi amaliyotlari bo'yicha o'rgatiladi. Xavfsizlikdan xabardorlik dasturlarini ishga tushirish uchun litsenziya olinadigan bir nechta platformalar mavjud, jumladan, ta'lim, simulyatsiya qilingan fishing mashqlari va xodimlarni fishing, SMSfishing va boshqalar kabi tahdidlarga qanchalik duchor bo'lish ehtimoli haqida boshlang'ich ma'lumot olish uchun xodimlarni sinovdan o'tkazish kerak.

Xavfsizlik bo'yicha xabardorlik sohasidagi taniqli kompaniya KnowBe4, xavfsizlik bo'yicha o'qitish uchun byudjet yaratish xodimlarning xatti-harakatlarini o'zgartirishda samarali ekanligini va xavfsizlik bilan bog'liq xavflarni 45 dan 70 foizgacha kamaytirishini xabar qiladi.

Ma'lumotlarni shifrlash. SSL/TLS kabi protokollar yordamida tranzitdagi ma'lumotlarni shifrlanadi. Nozik ma'lumotlarni, ayniqsa, portativ qurilmalarda shifrlanadi. Bu, ayniqsa, shaxsiy, moliyaviy va sog'liq haqidagi nozik ma'lumotlar bilan shug'ullanadigan korxonalar uchun juda muhimdir. Ofisda ham, masofaviy xodimlar uchun ham ma'lumotlar buzilishining oldini olish uchun kompaniya telefonlari, noutbuklari va bulutli ilovalaridagi ma'lumotlarni shifrlash uchun bir nechta vositalar, protokollar va jarayonlar kuchga kirishi mumkin.

Shifrlash tarmoqning turli qatlamlariga, jumladan ma'lumotlarga, aloqa kanallariga, qurilmalar va so'nggi nuqtalarga qo'llanilishi mumkin. Qaysi qatlamda shifrlash va shifrlashni qanday boshqarishga strategik korporativ talablaringiz va texnologiya to'plami asosida yondashish kerak.

Doimiy dasturiy ta'minotni tuzatish va yangilash. Ma'lum zaifliklarni bartaraf etish uchun operatsion tizimlar, ilovalar va xavfsizlik dasturlarini yangilab turiladi. Dasturiy ta'minotni tuzatish va yangilash tarmoq xavfsizligi va umumiy kiberxavfsizlik holatini yaxshilashda hal qiluvchi rol o'ynaydi .

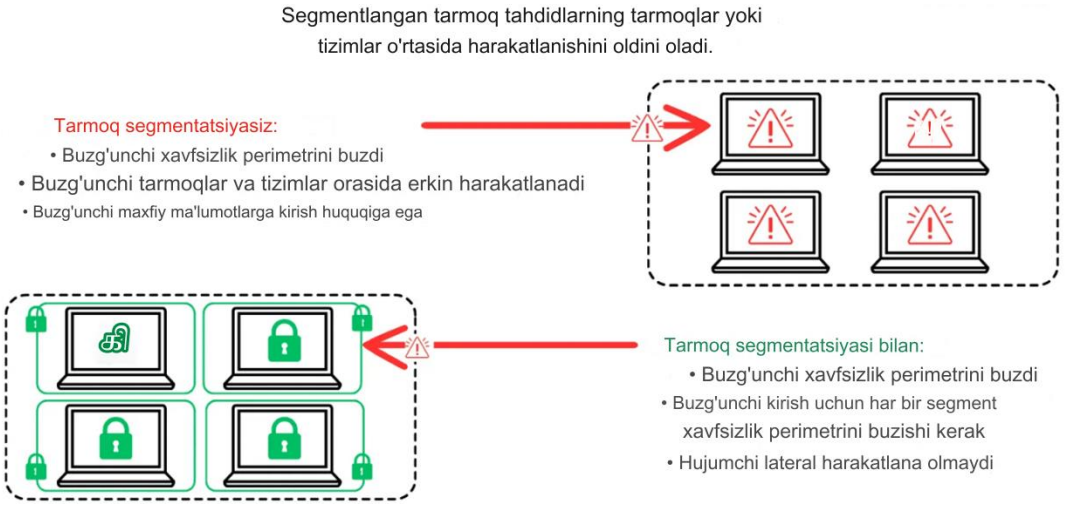
Muntazam tuzatishlar va yangilanishlar quyidagi usullarda yordam beradi:

- Korporativ tarmoqga ta'sir qilishdan oldin zaifliklarni tuzatish
- Ruxsatsiz kirish, buzilgan tizimlar va ma'lumotlar buzilishiga olib kelishi mumkin bo'lgan ekspluatatsiyalarning oldini olish
- Muvofiqlik va barqarorlikni oshirish
- Muvofiqlikni saqlash
- Hujum yuzasini kamaytirish va nol kunlik hujumlarga ta'sir qilish

Tarmoq xavfsizligi uchun tarmoq segmentatsiyasi. Xavfsizlik buzilishining ta'sirini cheklash va maxfiy ma'lumotlarga kirishni nazorat qilish uchun tarmoqni segmentlarga bo'linadi. Har bir segment boshqalardan ajratilgan bo'lib, kirish va xavfsizlik siyosatini yanada batafsil nazorat qilish imkonini beradi.

Korporativ tarmoq uchun tarmoq segmentatsiyasining tarmoq xavfsizligi afzalliklaridan tashqari , u qo'shimcha yaxshilanishlarga ham olib kelishi mumkin, masalan:

- Tarmoq unumdorligi ortdi
- Havflarni cheklash
- Muvofiqlik va me'yoriy talablarga erishish
- Segment talablari bo'yicha optimallashtirilgan resurslar taqsimoti



1.1-rasm. Segmentlangan va segmentlanmagan tarmoqlar farqi

VLAN yoki pastki tarmoqlar ko'pincha korporativ tarmoqlarini segmentlash va tarmoqni foydalanuvchilarni virtual bog'laydigan kichikroq segmentlarga bo'lish uchun ishlatiladi.

Bosqinlarni aniqlash tizimlari (IDS). Bosqinlarni aniqlash tizimlari (IDS) shubhali harakatlar yoki xavfsizlik hodisalari uchun tarmoq trafigini kuzatish va tahlil qilish orqali tarmoq xavfsizligida hal qiluvchi rol o'ynaydi. IDS tarmoq uchun potentsial tahdid sifatida belgilanishi uchun ma'lum imzolar, anomaliyalar va boshqa shubhali harakatlar uchun trafikni kuzatib boradi. IDS shuningdek, ruxsatsiz o'zgartirishlarni aniqlash uchun fayllar va tizim konfiguratsiyasidagi o'zgarishlarni kuzatadi.

Yaxshi sozlangan IDS-ni o'rnatish orqali tashkilotlar o'zlarining korporativ tarmoqlari xavfsizligini yaxshilashlari va keng doiradagi kiber tahdidlardan yaxshiroq himoyalanishlari mumkin.

Ma'lumotlarni zaxiralash va zaxira nusxadan tiklash: Muntazam ravishda muhim ma'lumotlarni zaxiralash va ularni xavfsiz joyda yoki bulutda saqlash kerak.

Hujjatlashtirilgan va amalda qo'llanilgan ofatlarni tiklash strategiyasi ishlamay qolish vaqtini qisqartirishga, tiklanishni tezlashtirishga va korporativ tarmoq operatsiyalarida halokatli uzilishlar va muhim ma'lumotlarni yo'qotish xavfini kamaytirishga yordam beradi.

Xavfsizlik siyosati va tartiblari: Barcha xodimlar amal qilishi kerak bo'lgan aniq xavfsizlik siyosati va tartiblarini belgilanadi. Ushbu xavfsizlik siyosatlari yangi xodimlarni ishga qabul qilish, xodimlarning ketishi yoki o'zgarishlari, texnologiyani tuzatish va yangilash va boshqalar paytida qanday choralar ko'rish kerakligini ko'rsatishi kerak. Xodim tashkilotni tark etganda kirish huquqlarini bekor qilish va kompaniyaga tegishli qurilmalarni yig'ish bo'yicha yaxshi hujjatlashtirilgan jarayonning mavjudligi korxonalarga foyda keltiradi. Bu ruxsatsiz kirish bilan bog'liq muammolarni kamaytirishga, shuningdek, offboarding jarayonlarini tezlashtirishga yordam beradi.

Boshqa tarmoq xavfsizligi siyosatlari quyidagilarni o'z ichiga olishi mumkin:

- Ko'p faktorli autentifikatsiyani amalga oshirish
- Parol siyosati va boshqaruvi
- Masofaviy kirish qoidalari va xavfsiz VPN orqali kompaniya tarmog'iga ulanish
- Tegishli kirish darajasi va ruxsatlardan foydalanish
- Xavfsizlik devori konfiguratsiyasi va qoidalari
- Xavfsiz Wi-Fi-dan foydalanish bo'yicha ko'rsatmalar
- Dasturiy ta'minotni yangilab turish va xavfsizlik yamoqlarini zudlik bilan qo'llash
- Kompaniya qurilmalari va tarmoqlaridan foydalanish

Monitoring va ro'yxatga olish. Tarmoq va tizim jurnallarini noodatiy harakatlar uchun kuzatib boriladi. Potentsial xavfsizlik havflari uchun ogohlantirishlarni o'rnatiladi. Monitoring va jurnallar tarmoq darajasida, operatsion tizimlar, ilovalar, qurilmalar, xavfsizlik devorlari va tarmoqqa ulangan har bir so'nggi nuqtada yoqilishi mumkin, bu sizning tarmog'ingizga xavf tug'dirishi mumkin. Bulutli yechimlardan foydalanadigan kompaniyalar o'zlarining monitoringini bulutli muhitlar va platformalarga kengaytirishlari kerak.

Korporativ tarmog'i xavfsizligi uchun jismoniy xavfsizlik choralari. Ko'pgina tarmoq xavfsizligi tahdidlari raqamli bo'lsada, kimdir korporativ tarmog'i uskunalariga bevosita kirishi mumkin bo'lgan jismoniy, shaxsiy tahdid mavjud. Ushbu xavfni kamaytirish uchun jismoniy tarmoq xavfsizligining bir nechta eng yaxshi amaliyotlariga rioya qilish kerak:

Ruxsatsiz buzg'unchilikni oldini olish uchun tayinlangan xodimlarga berilgan kalit karta bilan serverlar va tarmoq uskunalariga jismoniy kirishni ta'minlash kerak.

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 // JohnWiley & 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. Pande J. Introduction to Cyber Security. Uttarakhand Open University, 2017, -152 p.

10. Curricula Cybersecurity. Curriculum guidelines for post- secondary degree programs in cybersecurity. – 2017.

11. Zlatanov N. Hard Disk Drive and Disk Encryption, 2015, DOI: 10.13140/RG.2.1.1228.9681.

12. Ganiev S.K., Khudoykulov Z.T., Islomov Sh.Z., Selection suitable biometrics for cryptographic key generators // TUIT BULLETIN,Tashkent, 2016, №4 (40), – P. 80-92

13. Report to Congress on Breaches of Unsecured ProtectedHealth Information For Calendar Years 2015, 2016, and 2017. U.S. Department of Health and Human Services Office for Civil Rights. https://www.hhs.gov/sites/default/files/breach-report-to-congress-2015- 2016-2017.pdf

14. Fundamentals of General Ecology, Life Safety and Environment Protection. Mark D Goldfein, Alexei V Ivanov, Nikolaj Kozhevnikov, V Kozhevnikov. Nova Science Publishers, Inc. (April 25, 2013).

15. Life safety and environmental management (in terms, concepts, facts and figures): textbook / A. Nigmatov, Sh. Mukhamedov, N. Khasanova. T.: Navroz, 2014. 199 6.

16. Sapaev M.. Kadyrov F.M. "Life Safety and Ecology", Tashkent-2019. 276 v.

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