SIMSIZ TARMOQ XAVFSIZLIGI

Mòsinjonova Aygiza

Farġona Davlat universiteti

axborot tizimlari va texnalogiyalari yònalishi

2 kurs talabasi bòladimi

ANNOTATSIYA : *Ushbu tezisda simsiz tarmoq tizimlari hamda simsiz tarmoq xavsizligi haqida so'z boradi. Simsiz tarmoq tuzilmasi va himoyasi xususida ham ma'lumot berilgan.*

Kalit so'zlar: *tarmoq himoyasi, simsiz aloqa, identifikatorlar, serverlar, simsiz lokal tarmoq.*

АННОТАЦИЯ: *Эта диссертация посвящена системам беспроводных сетей и безопасности беспроводных сетей. Также предоставляется информация об архитектуре и безопасности беспроводной сети.*

Ключевые слова: *сетевая безопасность, беспроводная связь, идентификаторы, серверы, беспроводная локальная сеть.*

ANNOTATION: *This thesis deals with wireless network systems and wireless network security. Information on wireless network architecture and security is also provided.*

Key words: *network security, wireless communication, identifiers, servers, wireless local area network.*

Simsiz tarmoqlarning qulayligi, biroq narxiga bog'liq. Simli tarmoqdan foydalanishni nazorat qilish mumkin, chunki ma'lumotlar kompyuterni kalitga ulaydigan kabelda joylashgan. Simsiz tarmoq bilan kompyuter va kalit o'rtasida "kabel" ("kabel") "havo" deb ataladi, bu doirada har qanday qurilma potensial kirish imkoniyatiga ega bo'ladi. Agar foydalanuvchi 300 metr masofada simsiz ulanish nuqtasi bilan bog'lana oladigan bo'lsa, nazariy jihatdan simsiz kirish nuqtasining 300 metrlik radiusi ichida boshqalar ham shunday bo'lishi mumkin.

Simsiz tarmoq xavfsizligiga tahdid

Rog'un GESlari - Sizning korxonangiz rasman tasdiqlangan simsiz tarmoqqa ega bo'ladimi yoki yo'qmi, simsiz routerlar nisbatan arzon va shuhratli foydalanuvchilar tarmoqqa ruxsatsiz uskunalarni ulashi mumkin. Ushbu noqonuniy simsiz tarmoqlar ishonchsiz yoki noto'g'ri kafolatlangan bo'lishi mumkin va tarmoq uchun katta xavf tug'dirishi mumkin.

Spoofing Internal Communications - Tarmoq tashqarisidan qilingan hujum, odatda, bu kabi aniqlanishi mumkin. Agar buzg'unchilikchi sizning WLAN-ga ulanishi mumkin bo'lsa, ular ichki domenlardan keladigan ko'rinishda aloqa o'rnatishlari mumkin. Foydalanuvchilar ishonchli va ichki aloqa bilan aloqa qilishda ko'proq harakat qilishlari mumkin.

Tarmoq resurslarini o'g'irlash - Agar sizning kompyuteringizga hujum qilmasa yoki ma'lumotlarni uzib qo'ymasangiz ham, ular WLAN-ga ulanish va tarmoqni Internetga chiqish uchun tarmog'ingizni kengaytirishi mumkin. Ular sizning qimmatbaho tarmoq resurslaridan foydalanib va qonuniy foydalanuvchilar uchun tarmoq ishiga ta'sir qilish uchun musiqa va video kliplarni yuklab olish uchun ko'plab korporativ tarmoqlarda topilgan yuqori tarmoqli kengligidan foydalanishi mumkin.

Tarmog'ingizni WLAN-dan himoya qilish

Yaxshilangan xavfsizlik - WLAN-ni o'z VLAN-da o'rnatish uchun juda yaxshi sababdir. Barcha simsiz qurilmalarning WLAN-ga ulanishiga ruxsat berishingiz mumkin, ammo sizning ichki tarmog'ingizni qolgan qismini simsiz tarmoq orqali yuzaga keladigan har qanday muammolar yoki hujumlardan himoyalashingiz mumkin.

Faervol yoki ACL yo'riqchisidan foydalanish (kirishni boshqarish ro'yxatlarini) siz WLAN va boshqa tarmoq o'rtasidagi aloqani cheklashingiz mumkin. WLAN-ni veb-proksi yoki VPN orqali ichki tarmoqqa ulasangiz, hatto ular faqatgina Internetga kira olishlari uchun yoki faqat ma'lum papkalarga yoki ilovalarga kirishga ruxsat beradigan simsiz qurilmalar tomonidan kirishni cheklashingiz mumkin.

Simsiz shifrlash

Ruxsatsiz foydalanuvchilarning sizning simsiz tarmoqingizda quloq solmaslik usullaridan biri simsiz ma'lumotingizni shifrlashdir. Original shifrlash usuli, WEP

(simli ekvivalentlik maxfiyligi), asosan, nuqsonli deb topildi. WEP kirishni cheklash uchun umumiy kalit yoki parolga asoslangan. WEP kalitini biladigan har qanday kishi simsiz tarmoqqa qo'shilishlari mumkin. WEPga kalitni avtomatik ravishda o'zgartirish uchun hech qanday mexanizm yo'q edi va WEP kalitini bir necha daqiqada yorib yuboradigan vositalar mavjud, shuning uchun buzg'unchiga WEP-shifrlangan simsiz tarmoqqa kirish uchun uzoq vaqt talab qilinmaydi.

WEPni ishlatishda hech qanday shifrlashdan ko'ra biroz yaxshiroq bo'lishi mumkin, korporativ tarmoqni himoya qilish uchun etarli emas. WPA (Wi-Fi Protect Access) shifrlashning yangi avlodi 802.1X-mos keluvchi autentifikatsiya serveridan foydalanish uchun mo'ljallangan, lekin PSK (Pre-Shared Key) rejimida WEPga o'xshash ishlarni bajarish mumkin. WEPdan WPAga bo'lgan asosiy yondashuv TKIP (Temporal Key Integrity Protocol) qo'llanilishidir, bu WEP shifrlashni buzish uchun ishlatiladigan yorilish texnikasining oldini olish uchun kalitni dinamik ravishda o'zgartiradi.

Hatto WPA ham guruh yordami yondashuvi edi. WPA, simsiz qurilmalar va dasturiy ta'minot ishlab chiqaruvchilari tomonidan rasmiy 802.11i standartini kutib, etarli darajada himoya qilishni talab qildi. Shifrlashning eng dolzarb shakli - WPA2. WPA2 shifrlash AES shifrlash algoritmiga asoslangan CCMP, shu jumladan yanada murakkab va xavfsiz mexanizmlarni taqdim etadi.

Simsiz ma'lumotlarni uzib qo'ymaslik va simsiz tarmog'ingizga ruxsatsiz kirishni oldini olish uchun, WLAN-dan kamida WPA shifrlash va WPA2 shifrlash afzalroq bo'lishi kerak.

Simsiz haqiqiylikni tekshirish

Simsiz ma'lumotni shifrlashdan tashqari, WPA 802.1X yoki RADIUS autentifikatsiya serverlari bilan WLAN-ga kirishni boshqarishning yanada xavfsiz usulini ta'minlashi mumkin. PSK rejimida WEP yoki WPA mavjud bo'lsa, 802.1X yoki RADIUS autentifikatsiyasi to'g'ri kalit yoki parolga ega bo'lganlarga deyarli noma'lum kirishni ta'minlaydi. Foydalanuvchilarda joriy foydalanuvchi nomi va parol hisobga olish ma'lumotlari yoki simsiz tarmoqqa kirish uchun haqiqiy sertifikat bo'lishi kerak.

WLAN-ga autentifikatsiya qilishni talab qilish kirishni cheklab, xavfsizlikni oshiradi, biroq u shubhali narsalar borligini tekshirish uchun jurnalga yozilish va sud-huquqiy izlanishni ta'minlaydi. Umumiy kalitlarga asoslangan simsiz tarmoq MAC yoki IP manzillarini qayd etishi mumkin bo'lsa-da, bu muammo muammoning ildiz sababini aniqlashda juda foydali emas. Tegishli maxfiylik va yaxlitlik, agar kerak bo'lmasa, ko'pchilik xavfsizlik talablariga javob berishi uchun tavsiya etiladi.

WPA / WPA2 va 802.1X yoki RADIUS autentifikatsiya serverlari yordamida tashkilotlar Kerberos, MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) yoki TLS (Transport Layer Security) kabi bir qator autentifikatsiya protokollaridan foydalanishi va foydalanuvchi nomi / parollar, sertifikatlar, biometrik autentifikatsiya yoki bir martalik parollar kabi hisob ma'lumotlari autentifikatsiya qilish usullari.

Simsiz tarmoqlar samaradorlikni oshirishi, hosildorlikni oshirishi va tarmoqni yanada arzonlashtirishi mumkin, ammo agar ular to'g'ri qo'llanilmasa, ular sizning tarmoq xavfsizligingizning Axilles to'pig'i bo'lishi mumkin va sizning barcha tashkilotingizdan kelishuvga yo‘l qo'yishi mumkin. Xatarlarni tushunish uchun vaqt ajratib oling va sizning simsiz tarmog'ingizni qanday qilib xavfsiz qilishingiz mumkin, shunday qilib tashkilotingiz simsiz aloqa qulayligini xavfsizlik buzmasligi uchun imkoniyat yaratmasdan foydalanishi mumkin.

Xulosa o’rnida aytish joizki, bugungi kunda ayniqsa simsiz tarmoqlar xavfsizligiga katta e'tibor berilsa maqsadga muvofiq bo’ladi. Simsiz qurilmalarning tez o'sishi bilan ularni tasniflash, boshqarish va himoya qilish uchun yanada samarali strategiyalar talab qilinadi. Shu bilan birga, biz tarmoqdagi yashirin qurilmalarni aniqlashni o'rganishni davom ettirish birgalikdagi ishimiz simsiz tarmoqlar va qurilmalar xavfsizligi bo'yicha keyingi tadqiqotlar olib borish muhim hisoblanadi.

FOYDALANILGAN ADABIYOTLAR

1. Tojimamatov, I. (2023). KOMPYUTERNING STATIK VA DINAMIK OPERATIV XOTIRALARI. Current approaches and new research in modern sciences, 2(12), 133-139.

2. Tojimamatov, I. (2023). VAKUUM NAYCHALARIDAN KREMNIY CHIPLARIGACHA: KOMPYUTER TEXNIKASI EVOLYUTSIYASINI KUZATISH. Development and innovations in science, 2(12), 121-131.

3. Goyibova, G. G., & Tojimamatov, I. N. (2023). ZAMONAVIY KAMPYUTERLARNING DASTURIY TA'MINOTI VA ULARNING RIVOJLANISH TENDENSIYALARI. Solution of social problems in management and economy, 2(13), 209-214.

4. Онаркулов, М. К. (2023). ГЛУБОКИЕ НЕЙРОННЫЕ СЕТИ В ЗАДАЧАХ РАСПОЗНАВАНИЯ РЕЧИ. INNOVATIVE DEVELOPMENTS AND RESEARCH IN EDUCATION, 2(18), 248-250.

5. Onarqulov, M., Yaqubjonov, A., & Yusupov, M. (2022). Computer networks and learning from them opportunities to use. Models and methods in modern science, 1(13), 59-62.

6. Karimberdiyevich, O. M., & Mahamadamin o'g'li, Y. A. (2023). BASHORATLI TAHLILLAR UCHUN MASHINALI O‟ QITISH ALGORITMLARI. QIYOSIY QARASHLAR. THE JOURNAL OF INTEGRATED EDUCATION AND RESEARCH, 130.

7. Karimberdiyevich, O. M., & Axmedovna, X. M. (2023). NEYRONLAR HARAKATINING MATEMATIK MODELI. Finland International Scientific Journal of Education, Social Science & Humanities, 11(1), 515-518.

8. Ибрагимов, Ш. (2023). Реализация цифровизации образования: пути развития и проблемы. Информатика и инженерные технологии, 1(2), 273-278.

9. Karimberdiyevich, O. M., Mahamadamin o'g'li, Y. A., & Abdulaziz o'g'li, Y. M. (2023). MASHINALI O'QITISH ALGORITMLARI ASOSIDA BASHORAT QILISH USULLARINI YARATISH. Journal of new century innovations, 22(2), 165-167.

10. Karimberdiyevich, O. M., & Axmedovna, X. M. (2023). MARKAZLASHTIRILMAGAN BOSHQARUV TIZIMLARI UCHUN NEYRON

TARMOG ‘INI MATEMATIK MODELINI YARATISH. Scientific Impulse, 1(10), 1378-1381.

11. Ibragimov, S. M. (2020). IMPROVING THE EFFECTIVENESS OF TEACHING INFORMATION TECHNOLOGY IN UNIVERSITIES USING THE METHOD OF INDIVIDUALIZATION. Экономика и социум, (11), 127-130.

12. Mamirovich, I. S., Revkatovich, I. E., Rustamjon o‘g, H. O. K., & Yigitali o'g'li, R. J. (2023). IJTIMOIY TARMOQLARDA BIG DATA TEXNOLOGIYASIDAN FOYDALANISH TAHLILI. " RUSSIAN" ИННОВАЦИОННЫЕ ПОДХОДЫ В СОВРЕМЕННОЙ НАУКЕ, 9(1).

13. Tojimamatov, I. N., Mamalatipov, O. M., & Karimova, N. A. (2022). SUN’IY NEYRON TARMOQLARINI O ‘QITISH USULLARI.

14. Tojimamatov, I., Mirkomil, M. M., & Saidmurod, S. (2023). BIG DATANING TURLI SOHALARDA QO ‘LLANILISHI. ОБРАЗОВАНИЕ НАУКА И ИННОВАЦИОННЫЕ ИДЕИ В МИРЕ, 18(6), 61-65.

15. Tojimamatov, I. N., Topvoldiyeva, H., Karimova, N., & Inomova, G. (2023). GRAFIK MA'LUMOTLAR BAZASI. Евразийский журнал технологий и инноваций, 1(4), 75-84.

16. Tojimamatov, I. N., Mamalatipov, O., Rahmatjonov, M., & Farhodjonov, S. (2023). NEYRON TARMOQLAR. Наука и инновация, 1(1), 4-12.