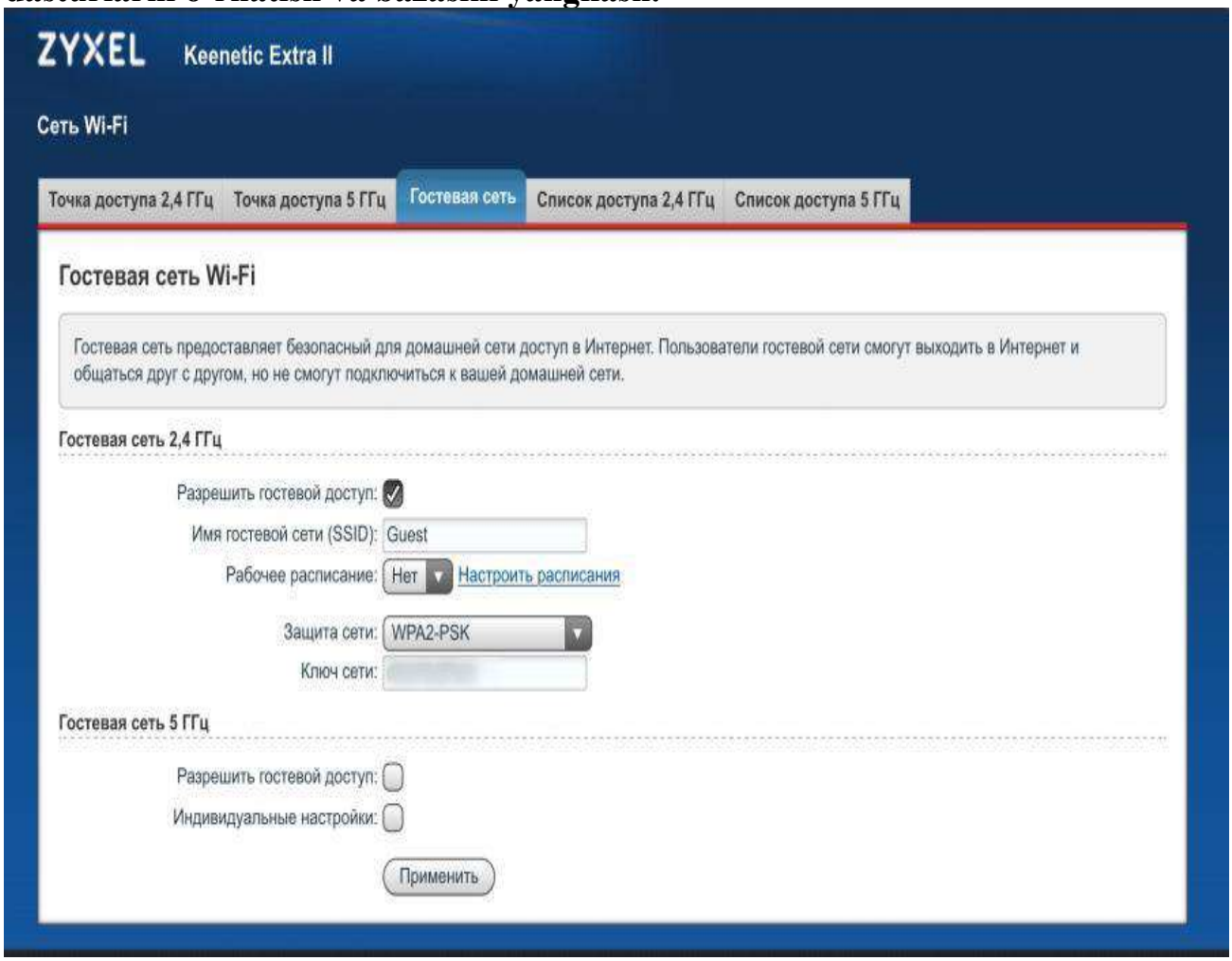
23-MAVZU. TARMOQDA AXBOROT XAVFSIZLIGI VA AXBOROTLARNI HIMOYALASH USULLARI

Reja:

23.1.Axborot xavfsizligi tushunchasi, axborot xavfsizligini siyosati. Axborotlarni ximoyalash vositalari. Kompyuterda va tarmoqlarda axborot xavfsizligi. Axborot xavfsizligining tashkiliy, texnik, dasturiy choralari.

23.2. Kompyuter tarmoqlariga ruxsatsiz kirishning oldini olish. Kompyuter viruslari va viruslardan ximoyalanish usullari.

23.3.Virus turlari, Antivirus dasturlar va ularning turlari. Antivirus dasturlarni o‘rnatish va bazasini yangilash.



Bugungi kunda deyarli har bir xonadonda statsionar kompyuterlar, noutbuklar, ma'lumotlarni saqlash (NAS), media pleerlar, aqlli televizorlar, shuningdek, smartfonlar, planshetlar va boshqa kiyiladigan moslamalarni ulaydigan uy tarmog'i mavjud. Simli (Ethernet) yoki simsiz (Wi-Fi) ulanishlar va TCP / IP protokollaridan foydalaniladi. "Internet Internet" texnologiyalari rivojlanishi bilan maishiy texnika - muzlatgichlar, kofe qaynatgichlar, konditsionerlar va hattoki elektr uzatish uskunalari tarmoqqa kirdi. "Aqlli uy" echimlari tufayli biz yorug'lik yorqinligini boshqarishimiz, ichki iqlimni

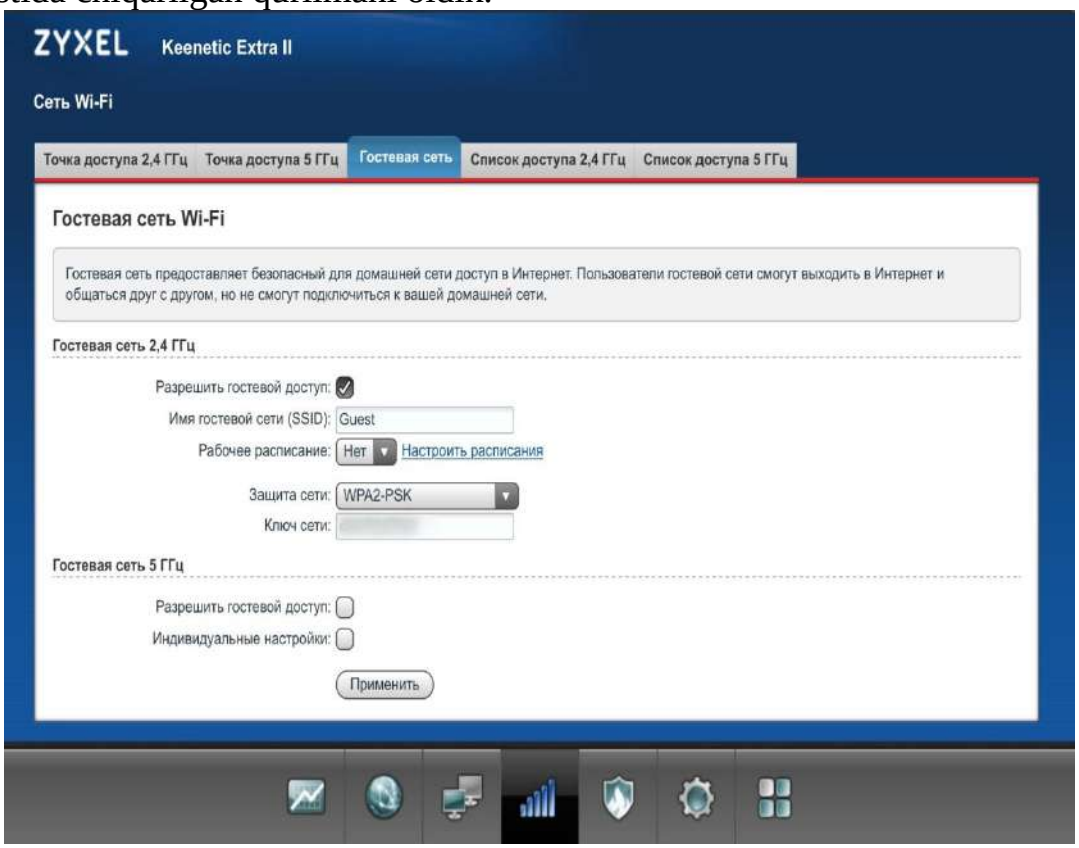
masofadan sozlashimiz, turli xil moslamalarni yoqish va o'chirishimiz mumkin - bu hayotni ancha osonlashtiradi, ammo zamonaviy echimlar egasi uchun jiddiy muammolarni keltirib chiqarishi mumkin.

Afsuski, bunday qurilmalarni ishlab chiquvchilar hali o'z mahsulotlarining xavfsizligi haqida etarlicha g'amxo'rlik qilmayaptilar va ularda topilgan zaifliklar soni yomg'irdan keyin qo'ziqorin kabi ko'paymoqda. Bozorga kirgandan keyin qurilmani qo'llab-quvvatlamaydigan holatlar ko'p uchraydi - masalan, bizning televizorimizda Android 4 asosida ishlaydigan 2016 proshivka mavjud va ishlab chiqaruvchi uni yangilamaydi. Shuningdek, mehmonlar muammolarni qo'shmoqdalar: ularni Wi-Fi-ga kirishni rad etish noqulay, lekin men ham o'zimning qulay tarmog'imga hech kimni kiritishni xohlamayman. Kim biladi, boshqa odamlarning mobil telefonlarida qanday viruslar joylashishi mumkin? Bularning barchasi bizni uy tarmog'ini bir nechta ajratilgan segmentlarga bo'lish zarurligiga olib keladi. Keling, buni qanday qilib, ozgina qon va eng kam moliyaviy xarajatlar bilan aytilganidek, amalga oshirishni tushunishga harakat qilaylik.

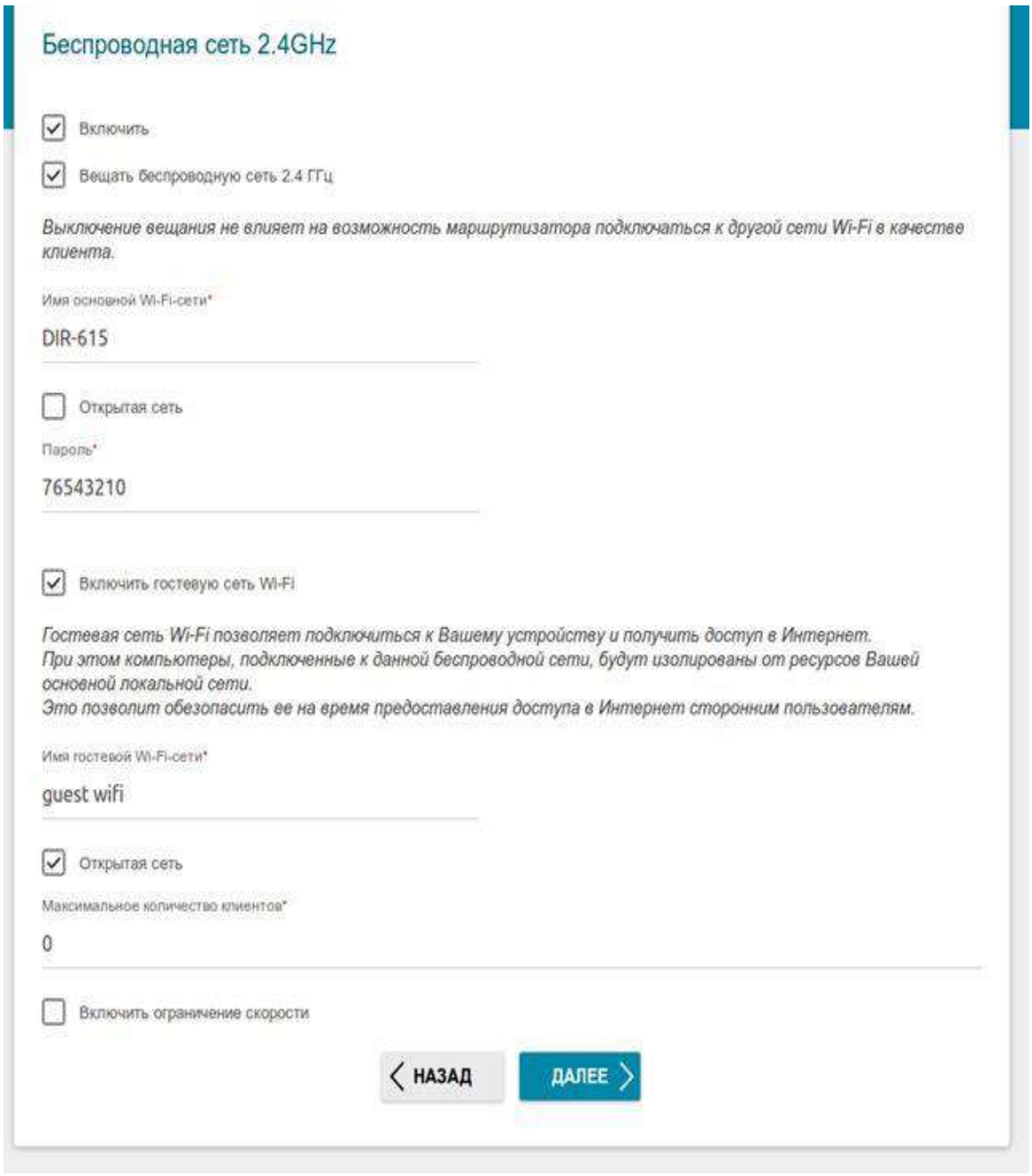
IN korporativ tarmoqlar muammo oddiygina hal qilindi - virtual mahalliy tarmoqlarni (VLAN) qo'llab-quvvatlaydigan boshqariladigan kalitlar, turli xil routerlar, xavfsizlik devorlari va ochkolar simsiz ulanish - bir necha soat ichida kerakli miqdordagi ajratilgan segmentlarni qurishingiz mumkin. Masalan, Traffic Inspector Next Generation (TING) qurilmasi yordamida vazifa bir necha marta bosish bilan hal qilinadi. Mehmonlar tarmog'i segmentining kalitini alohida chekilgan portiga ulash va xavfsizlik devori qoidalarini yaratish kifoya. Uy uchun bu parametr mos kelmaydi, chunki uskunalar narxi yuqori - ko'pincha tarmoq

yo'riqnoma, kalit, simsiz ulanish nuqtasi funktsiyalarini birlashtirgan bitta qurilma tomonidan boshqariladi va yana nimani Xudo biladi.

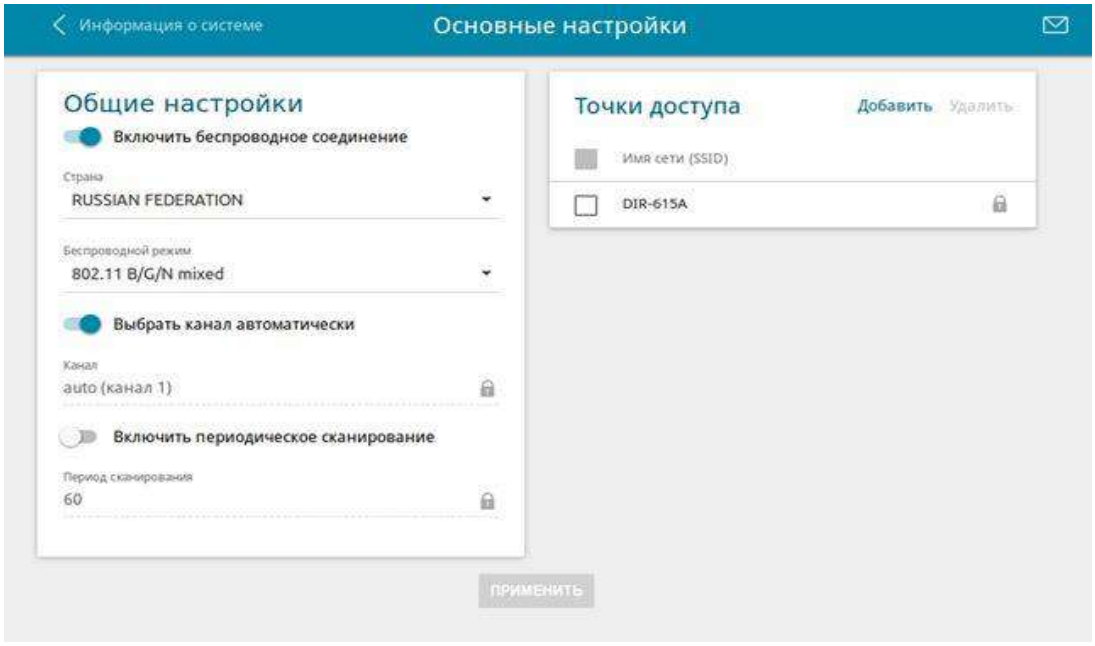
Yaxshiyamki, zamonaviy uy yo'riqchilari (garchi ularni Internet markazlari deb atash to'g'ri bo'lsa ham) juda aqlli bo'lib qolishdi va deyarli barchasida, ehtimol byudjetdan tashqari, izolyatsiya qilingan mehmonni yaratish imkoniyati mavjud wi-Fi tarmog'i... Ushbu izolyatsiyaning ishonchliligi - bu alohida maqola uchun savol, bugungi kunda biz uy jihozlarining dasturiy ta'minotini tekshirmaymiz turli ishlab chiqaruvchilar... Masalan, ZyXEL Keenetic Extra II ni oling. Endi ushbu yo'nalish oddiygina Keenetic deb nomlandi, ammo biz ZyXEL brendi ostida chiqarilgan qurilmani oldik.



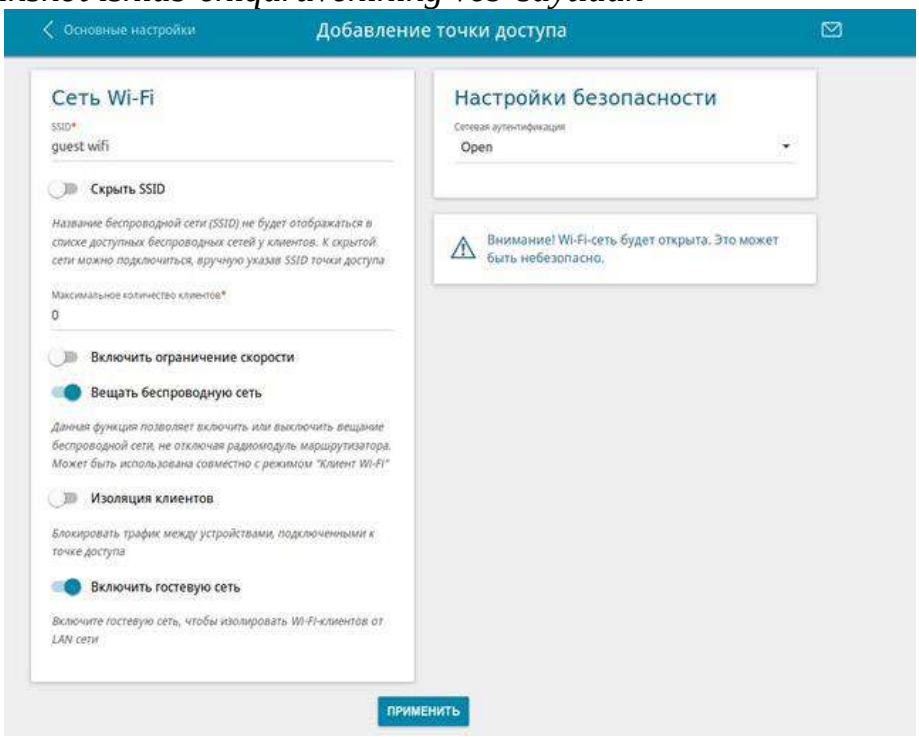
Veb-interfeys orqali sozlash hatto yangi boshlanuvchilar uchun ham qiyinchilik tug'dirmaydi - bir necha marta bosish va bizda o'z SSID, WPA2 xavfsizligi va kirish uchun parol bilan alohida simsiz tarmoq mavjud. Siz mehmonlarni unga kiritishingiz mumkin, shuningdek televizorlar va uzoq vaqt davomida yangilanmagan dasturiy ta'minotli pleerlarni yoki o'zingiz ishonmaydigan boshqa mijozlarni yoqishingiz mumkin. Boshqa ishlab chiqaruvchilarning aksariyat qurilmalarida ushbu funktsiya, xuddi shu tarzda mavjud va yoqilgan. Masalan, dasturiy ta'minotda muammo shu tarzda hal qilinadi d-Link routerlari sozlash sehrgaridan foydalanish.



Qurilma allaqachon sozlangan va ishlayotgan paytda siz mehmonlar tarmog'ini qo'shishingiz mumkin.



Skrinshot ishlab chiqaruvchining veb-saytidan

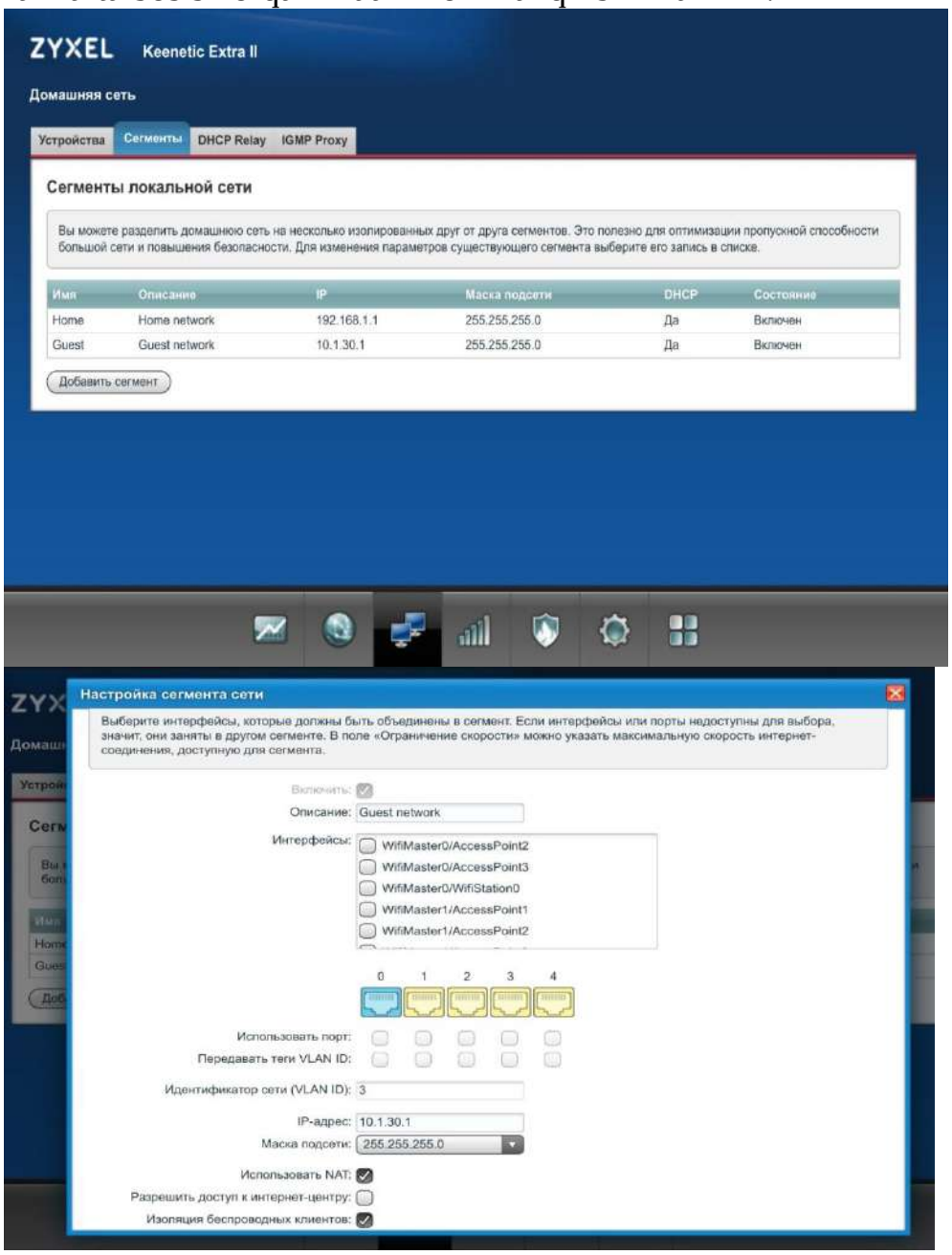


Skrinshot ishlab chiqaruvchining veb-saytidan

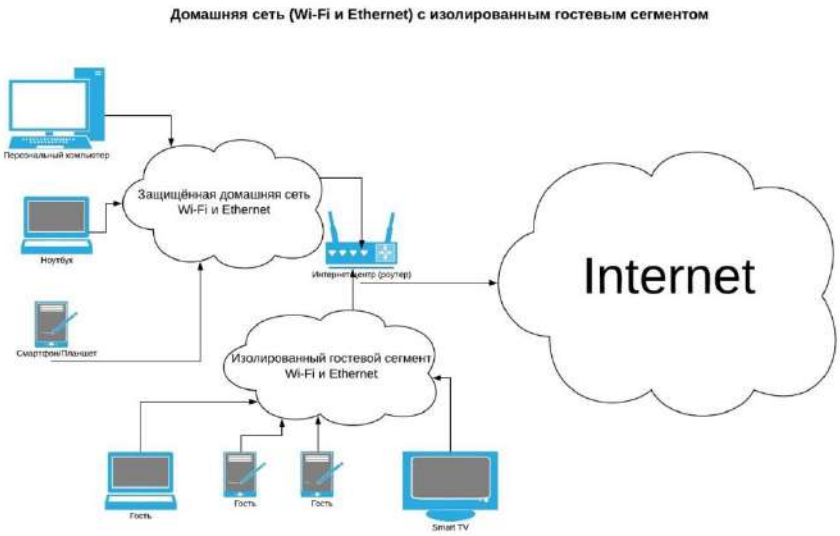
Ethernet tarmoqlarini ajratish

Simsiz tarmoqqa ulanadigan mijozlardan tashqari biz simli interfeysga ega qurilmalarni uchratishimiz mumkin. Mutaxassislarning ta'kidlashicha, izolyatsiya qilingan chekilgan segmentlarni yaratish uchun VLAN-lar - virtual mahalliy tarmoqlar ishlatiladi. Ba'zi uy routerlari ushbu funktsiyani qo'llab-quvvatlaydi, ammo bu juda qiyin bo'ladi. Men shunchaki alohida segmentni yaratishni xohlamayman, biz simli ulanish uchun portlarni bir xil yo'riqchidagi simsiz mehmonlar tarmog'i bilan birlashtirishimiz kerak. Har bir uy jihozlari bunga qodir emas: yuzaki tahlillar shuni ko'rsatadiki, Keenetic Internet-markazlaridan tashqari, MikroTik modellari ham chekilgan portlarni Wi-Fi tarmog'iga ega

bo'lgan bitta mehmon segmentiga qo'shishi mumkin, ammo ularni sozlash jarayoni unchalik aniq emas. Agar narx bo'yicha taqqoslanadigan maishiy yo'riqnoma haqida gapiradigan bo'lsak, faqatgina Keenetic veb-interfeysda bir necha marta bosish orqali muammoni hal qilishi mumkin.



Ko'rib turganingizdek, mavzu muammo bilan osonlikcha kurashdi va bu erda yana bir qiziqarli xususiyatga e'tibor qaratish lozim - siz mehmonlar tarmog'ining simsiz mijozlarini bir-biridan ajratishingiz mumkin. Bu juda foydali: zararli dasturlarni yuqtirgan do'stingizning smartfoni Internetga ulanadi, lekin u mehmonlar tarmog'ida ham boshqa qurilmalarga hujum qila olmaydi. Agar yo'riqnoma shu kabi funktsiyaga ega bo'lsa, uni albatta yoqishingiz kerak, garchi bu mijozlar bilan ishlash imkoniyatlarini cheklaydi - masalan, endi Wi-Fi orqali televizor va media pleer o'rtasida do'stlasha olmaysiz, simli ulanishdan foydalanishingiz kerak bo'ladi. Ayni paytda bizning uy tarmog'imiz yanada xavfsizroq ko'rinadi.



Pastki chiziq nima?

Xavfsizlikka tahdidlar soni yildan-yilga ko'payib bormoqda va aqlli qurilmalar ishlab chiqaruvchilari har doim ham yangilanishlarning o'z vaqtida chiqarilishiga etarlicha e'tibor bermaydilar. Bunday vaziyatda bizda bitta yo'l bor - uy tarmog'i mijozlarini farqlash va ular uchun ajratilgan segmentlarni yaratish. Buning uchun sizga o'n minglab rublga uskunalar sotib olishning hojati yo'q, nisbatan arzon maishiy Internet markazi vazifani uddalashi mumkin. Bu erda men o'quvchilarni byudjet brendlaridan qurilmalar sotib olishdan ogohlantirmoqchiman. Hozir deyarli barcha ishlab chiqaruvchilar ozmi-ko'pmi bir xil apparatga ega, ammo o'rnatilgan dasturiy ta'minotning sifati juda boshqacha. Shuningdek, chiqarilgan modellarni qo'llab-quvvatlash tsiklining davomiyligi. Simli va simsiz tarmoqning izolyatsiya qilingan segmentida birlashishning juda oddiy vazifasi bo'lsa ham, har bir uy yo'riqchisi bunga qodir emas va sizda murakkabroq bo'lishi mumkin. Ba'zan siz faqat xavfsiz xostlarga kirish uchun qo'shimcha segmentlarni yoki DNS filtrlashni sozlashingiz kerak, katta xonalarda siz ulanishingiz kerak wi-Fi mijozlari tashqi kirish nuqtalari orqali mehmonlar tarmog'iga va boshqalar. va h.k. Xavfsizlik masalalaridan tashqari, boshqa muammolar ham mavjud: jamoat tarmoqlarida "Axborot, axborot texnologiyalari va axborotni muhofaza qilish to'g'risida" 97-sonli Federal qonuni talablariga muvofiq mijozlarni ro'yxatdan o'tkazishni ta'minlash kerak. Arzon qurilmalar bunday muammolarni hal qilishga qodir, ammo ularning hammasi ham emas - o'rnatilgan dasturiy ta'minotning funktsionalligi, biz yana takrorlaymiz.

Avast foydalanuvchilarni yangi tahdidlardan himoya qilish to'g'risida gap ketganda doimo oldinga intilishga harakat qiladi. Aqlli televizorda filmlar, sport dasturlari va teledasturlarni tomosha qiladiganlar soni tobora ko'paymoqda. Ular uylaridagi haroratni raqamli termostatlar yordamida boshqaradilar. Ular aqlli soatlar va fitnes bilakuzuklarini taqishadi. Natijada, xavfsizlik talablari kengayib bormoqda shaxsiy kompyuteruy tarmog'idagi barcha qurilmalarni qamrab olish uchun.

Biroq, uy tarmog'i infratuzilmasining asosiy qurilmalari bo'lgan uy routerlari ko'pincha xavfsizlik bilan bog'liq muammolarga duch kelishadi va xakerlarga osonlikcha kirish imkoniyatini beradi. Tripwire tomonidan olib borilgan so'nggi

tadqiqotlar shuni ko'rsatdiki, eng ko'p sotilgan routerlarning 80 foizida zaifliklar mavjud. Bundan tashqari, ma'muriy interfeysga kirish uchun eng keng tarqalgan kombinatsiyalar, xususan, admin / admin yoki admin / parolsiz dunyo bo'ylab yo'riqchilarning 50 foizida foydalaniladi. Foydalanuvchilarning yana 25 foizi yo'riqnoma uchun parol sifatida manzil, tug'ilgan sana, ism yoki familiyadan foydalanadi. Natijada, dunyo bo'ylab yo'riqchilarning 75 foizdan ko'prog'i oddiy parol hujumlariga qarshi himoyasiz bo'lib, bu uy tarmog'iga tahdidlarni tarqatish imkoniyatini ochadi. Bugungi kunda routerlarning xavfsizlik manzarasi har kuni yangi zaifliklar topilgan 1990 yillarni eslatadi.

Uy tarmog'ining xavfsizligi funktsiyasi

Avast Free Antivirus, Avast Pro Antivirus, Avast Internet Security va Avast Premier Antivirus-dagi Home Network Security xususiyati ushbu muammolarni yo'riqnoma va uy tarmog'i sozlamalarini potentsial muammolar uchun skanerlash orqali hal qiladi. Avast Nitro Update-da uy tarmog'idagi xavfsizlikni aniqlash dvigateli ko'p qirrali skanerlash va takomillashtirilgan DNS kirib kelish detektori yordamida to'liq qayta ishlangan. Dvigatel endi yadro drayveri darajasida bajarilgan ARP-skanerlash va portni skanerlashni qo'llab-quvvatlaydi, bu esa skanerlashni oldingi versiyadan bir necha baravar tezroq qiladi.

"Uy tarmog'ining xavfsizligi" saytlararo soxta so'rovlar (CSRF) bilan yo'riqchiga qilingan hujumlarni avtomatik ravishda bloklashi mumkin. CSRF veb-saytlarning zaifliklaridan foydalanadi va kiberjinoyatchilarga veb-saytga ruxsatsiz buyruqlar yuborish imkoniyatini beradi. Buyruq saytga ma'lum bo'lgan foydalanuvchining ko'rsatmasini simulyatsiya qiladi. Shunday qilib, kiberjinoyatchilar foydalanuvchini taqlid qilishi mumkin, masalan, jabrlanuvchiga uning xabarisiz pul o'tkazishi mumkin. CSRF so'rovlari tufayli jinoyatchilar masofadan turib DNS parametrlarini qayta yozish va trafikni firibgar saytlarga yo'naltirish uchun yo'riqnoma sozlamalariga o'zgartirishlar kiritishlari mumkin.

Uy tarmog'i xavfsizligi komponenti potentsial xavfsizlik muammolari uchun uy tarmog'i va yo'riqnoma sozlamalarini skanerlash imkonini beradi. Asbob zaif yoki standartni aniqlaydi wi-Fi parollari, zaif routerlar, Internetga ulanish buzilgan va IPv6 yoqilgan, ammo xavfsiz emas. Foydalanuvchilar faqat ma'lum qurilmalarning ulanganligini tekshirishlari uchun Avast uy tarmog'idagi barcha qurilmalarni ro'yxatlaydi. Komponent aniqlangan zaifliklarni bartaraf etish bo'yicha oddiy tavsiyalar beradi.

Shuningdek, vosita yangi qurilmalar tarmoqqa, tarmoqqa ulangan televizorlarga va boshqa qurilmalarga ulanganda foydalanuvchini xabardor qiladi. Endi foydalanuvchi noma'lum qurilmani darhol aniqlay oladi.

Yangi faol yondashuv foydalanuvchini maksimal darajada har tomonlama himoya qilishni ta'minlaydigan umumiy kontseptsiyani ta'kidlaydi.

Bir necha yil oldin, uy simsiz tarmoq juda sodda edi va qoida tariqasida kirish nuqtasi va Internetga ulanish, onlayn xarid qilish yoki o'yinlar uchun ishlatiladigan juft kompyuterlardan iborat edi. Ammo zamonaviy davrda uy tarmog'i ancha murakkablashdi. Uy tarmog'iga ulangan ko'plab qurilmalar

hozirda nafaqat Internetga kirish yoki ommaviy axborot vositalarini tomosha qilish uchun ishlatiladi. Ushbu maqolada biz sizning uy tarmog'ingizni qanday qilib barcha oila a'zolari uchun xavfsiz qilish haqida gaplashamiz.

Simsiz xavfsizlik

Deyarli har bir uyda simsiz tarmoq (yoki Wi-Fi tarmog'i deb ataladigan) tarmoq mavjud. Ushbu tarmoq noutbuk, planshet yoki o'yin konsoli kabi har qanday qurilmani Internetga ulashga imkon beradi. Simsiz tarmoqlarning aksariyati yo'riqnoma tomonidan boshqariladi, bu sizning Internet-provayderingiz tomonidan Internetga kirishni ta'minlash uchun o'rnatilgan qurilma. Ammo ba'zi hollarda sizning tarmog'ingizni routerga ulangan alohida tizimlar, ya'ni kirish nuqtalari orqali boshqarish mumkin. Sizning qurilmalaringiz Internetga ulangan tizimdan qat'i nazar, ushbu tizimlarning ishlash printsipi bir xil: radio signallarni uzatish. Turli xil qurilmalar Internetga va tarmoqdagi boshqa qurilmalarga ulanishi mumkin. Bu sizning uy tarmog'ingiz xavfsizligi sizning uyingizni himoya qilishning asosiy tarkibiy qismlaridan biri ekanligini anglatadi. Uy tarmog'ingiz xavfsizligini ta'minlash uchun sizga quyidagi ko'rsatmalarga rioya qilishni maslahat beramiz:

- Internet-yo'riqnoma yoki kirish nuqtasi ishlab chiqaruvchisi tomonidan o'rnatilgan administrator parolini o'zgartiring. Ma'mur hisobi tarmoq sozlamalariga o'zgartirish kiritishga imkon beradi. Muammo shundaki, ko'plab routerlar standart, taniqli parollar bilan ta'minlanadi va Internetda ularni topish oson. Shuning uchun siz zavod parolini noyob va kuchli parolga o'zgartirishingiz kerak, uni faqat siz bilasiz.

- Ishlab chiqaruvchining tarmoq nomini o'zgartiring (SSID deb ham ataladi). Bu sizning qurilmalaringiz uy simsiz tarmog'ini qidirishda ko'rgan nomi. Uy tarmog'ingizga tanib olish oson, lekin shaxsiy ma'lumotlar mavjud bo'lmagan noyob nom bering. Tarmoqni "ko'rinmas" deb sozlash - bu samarasiz himoya shakli. Ko'pgina simsiz brauzerlar va har qanday tajribali xakerlar "ko'rinmas" tarmoqlarni osongina aniqlashlari mumkin.

- Tarmoqqa faqat siz ishonadigan odamlar ulanishi va ushbu ulanish shifrlanganligiga ishonch hosil qiling. Bu xavfsizlikni yaxshilashga yordam beradi. Hozirda eng xavfsiz ulanish WPA2 hisoblanadi. Ishlatilganda, tarmoqqa ulanishda parol so'raladi va bu ulanish shifrlashni qo'llaydi. WEP yoki ochiq tarmoq (umuman xavfsizlikni ta'minlamaydigan) kabi eskirgan usuldan foydalanmasligingizga ishonch hosil qiling. Ochiq tarmoq simsiz tarmoqqa autentifikatsiya qilinmasdan ulanish uchun hamma narsaga imkon beradi.

- Tarmoqqa ulanish uchun odamlar kuchli paroldan foydalanganligiga ishonch hosil qiling, bu administrator paroli bilan bir xil emas. Shuni esda tutingki, siz foydalanadigan har bir qurilma uchun faqat bir marta parol kiritishingiz kerak, bu parolni qurilmalar eslab qolishi va saqlashi mumkin.

- Ko'pgina simsiz tarmoqlar "Mehmonlar tarmog'i" deb nomlanadigan narsani qo'llab-quvvatlaydi. Bu mehmonlarga Internetga kirishga imkon beradi, ammo keyinchalik sizning uyingizdagi uy qurilmalariga mehmonlar ulana olmasligi sababli uy tarmog'i ta'minlanadi. Agar siz mehmonlar tarmog'ini qo'shsangiz, WPA2 dan foydalanayotganingizga ishonch hosil qiling va u noyob va kuchli parol bilan himoyalangan.

- Wi-Fi Protected Setup-ni yoki yangi qurilmalarni parol yoki boshqa konfiguratsiya parametrlarini kiritmasdan ulanishga imkon beradigan boshqa sozlamani o'chirib qo'ying.

- Agar sizga barcha parollarni eslab qolish qiyin bo'lsa, ularni saqlash uchun parol menejeridan foydalanishni tavsiya etamiz.

Agar ro'yxatdagi narsalar haqida savollaringiz bo'lsa? Internet-provayderlarga o'ting, yo'riqnoma, kirish nuqtasi ko'rsatmalariga qarang yoki ularning ishlab chiqaruvchilarining veb-saytlariga qarang.

Qurilmalaringiz xavfsizligi

Keyingi qadam - tarmoqqa ulangan barcha qurilmalar ro'yxatini aniqlashtirish va ularning xavfsizligini ta'minlash. Ilgari buni amalga oshirish oson bo'lgan, tarmoqqa kam sonli qurilmalar ulangan edi. Ammo bugungi dunyoda deyarli barcha qurilmalar, shu jumladan televizorlar, o'yin pristavkalari, bolalar kameralari, karnaylar, isitgichlar va hattoki mashinalar ham "doimiy ravishda ulanishi" mumkin. Bog'langan qurilmalarni topishning eng oson usullaridan biri bu Fing kabi tarmoq skaneridan foydalanishdir. Kompyuterga o'rnatilgandan so'ng, ushbu dastur tarmoqqa ulangan barcha qurilmalarni aniqlay oladi. Barcha qurilmalarni topgandan so'ng, ularning xavfsizligi to'g'risida g'amxo'rlik qilishingiz kerak. Eng yaxshi usul xavfsizligini ta'minlash - muntazam ravishda operatsion tizimlarini / proshivkalarini yangilab turing. Iloji bo'lsa, sozlang avtomatik yangilash tizimlar. Agar har bir qurilma uchun parolni ishlatish imkoni bo'lsa, faqat kuchli va kuchli parol... Va nihoyat, ma'lumot olish uchun Internet-provayderingiz veb-saytiga tashrif buyuring bepul yo'llar tarmog'ingizni himoya qilish.

muallif haqida

Cheryl Conley peshqadamlik qilmoqda axborot xavfsizligi Lockheed Martin-da. U 100000 kompaniya xodimlarini o'qitish uchun mulkiy The I Campaign TM metodologiyasidan foydalanadi. Ushbu texnika kompaniya ichidagi fokus-guruhlardan faol foydalanadi va global dasturni muvofiqlashtiradi

Kompyuter tarmoqlarining xavfsizligi tarmoqdan va unda mavjud bo'lgan manbalardan ruxsatsiz foydalanish, noto'g'ri foydalanish, o'zgartirish yoki o'chirishni oldini olish va nazorat qilish bo'yicha qabul qilingan siyosat va amaliyotlar orqali ta'minlanadi. U tomonidan boshqariladigan ma'lumotlarga kirishni avtorizatsiya qilish kiradi tarmoq ma'muri... Foydalanuvchilar o'z vakolatlari doirasida ma'lumotlar va dasturlarga kirishga imkon beradigan identifikator va parolni yoki boshqa autentifikatsiya ma'lumotlarini tanlaydilar yoki tayinlaydilar.

Tarmoq xavfsizligi kundalik ishda, korxonalar, davlat idoralari va jismoniy shaxslar o'rtasida operatsiyalarni amalga oshirishda va aloqalarni amalga oshirishda foydalaniladigan turli xil umumiy va xususiy kompyuter tarmoqlarini qamrab oladi. Tarmoqlar xususiy bo'lishi mumkin (masalan, kompaniya ichida) yoki boshqa (jamoatchilik uchun ochiq bo'lishi mumkin).

Kompyuter tarmog'ining xavfsizligi tashkilotlar, korxonalar va boshqa turdagi muassasalar bilan bog'liq. Bu tarmoqni himoya qiladi, shuningdek himoya va kuzatuv ishlarini bajaradi. Eng keng tarqalgan va oddiy usulda tarmoq manbasini himoya qilish - unga noyob nom va tegishli parolni berishdir.

Xavfsizlikni boshqarish

Tarmoqlar uchun xavfsizlikni boshqarish har xil vaziyatlarda turlicha bo'lishi mumkin. Uy yoki kichik ofis faqat asosiy xavfsizlikni talab qilishi mumkin, yirik korxonalar esa xakerlik va istalmagan xujumlarning oldini olish uchun juda ishonchli texnik xizmat va zamonaviy dasturiy ta'minotni talab qiladi.

Hujum turlari va tarmoq zaifliklari

Zaiflik - bu dizayn, amalga oshirish, ishlash yoki ichki nazoratning zaifligi. Topilgan zaifliklarning aksariyati Umumiy zaifliklar va ta'sirlar (CVE) ma'lumotlar bazasida hujjatlashtirilgan.

Tarmoqlarga turli xil manbalardan hujum qilish mumkin. Ular ikkita toifadan iborat bo'lishi mumkin: "Passiv", tarmoq buzg'unchisi tarmoq orqali o'tayotgan ma'lumotlarni ushlab turganda va "Faol", bu erda tajovuzkor tarmoqning normal ishlashini buzish yoki ma'lumotlarga kirish huquqini olish uchun nazorat qilish buyruqlarini boshlaydi.

Kompyuter tizimini himoya qilish uchun unga qarshi amalga oshiriladigan hujum turlarini tushunish muhimdir. Ushbu tahdidlarni quyidagi toifalarga bo'lish mumkin.

"Orqa eshik"

Kompyuter tizimidagi, kriptosistemadagi yoki algoritmdagi orqa eshik - bu autentifikatsiya yoki xavfsizlikning an'anaviy vositalarini chetlab o'tishning har qanday maxfiy usuli. Ular bir nechta sabablarga ko'ra mavjud bo'lishi mumkin, jumladan original dizayn yoki yomon konfiguratsiya. Ularni ishlab chiquvchi tomonidan qandaydir qonuniy ruxsat olish uchun yoki tajovuzkor boshqa sabablarga ko'ra qo'shishi mumkin. Ularning mavjud bo'lish sabablaridan qat'i nazar, ular zaiflikni yaratadilar.

Xizmat hujumlarini rad etish

Xizmatdan voz kechish (DoS) xujumlari kompyuter yoki qilish uchun mo'ljallangan tarmoq manbai mo'ljallangan foydalanuvchilar uchun kirish mumkin emas. Bunday hujum tashkilotchilari, masalan, qasddan ko'p marta ketma-ket noto'g'ri parolni kiritib, to'siqni keltirib chiqarish orqali, alohida qurbonlar uchun tarmoqqa kirishni to'sib qo'yishi mumkin. hisob qaydnomasi, yoki mashina yoki tarmoq imkoniyatlarini haddan tashqari yuklang va barcha foydalanuvchilarni bir vaqtning o'zida bloklang. Bitta IP-manzildagi tarmoq hujumini yangi xavfsizlik devori qoidasini qo'shish bilan blokirovka qilish mumkin bo'lsa ham, signallarni kelib chiqadigan joyda tarqatilgan xizmatni rad etish (DDoS) ning ko'plab shakllari mumkin. katta raqam manzillar. Bunday holda mudofaa ancha qiyinlashadi. Bunday hujumlar botlar tomonidan boshqariladigan kompyuterlardan kelib chiqishi mumkin, ammo turli xil usullar, shu jumladan aks ettirish va kuchaytirish hujumlari mumkin, bu erda butun tizim o'z-o'zidan bunday signalni uzatadi.

To'g'ridan-to'g'ri kirish hujumlari

Kompyuterga jismoniy kirish huquqini olgan ruxsatsiz foydalanuvchi, ehtimol undan ma'lumotlarni to'g'ridan-to'g'ri nusxalashi mumkin. Bunday tajovuzkorlar operatsion tizimni o'zgartirish, qurtlarni o'rnatish, keyloggerlar, simsiz sichqonchani tinglash yoki ishlatish uchun yashirin qurilmalar. Tizim standart xavfsizlik choralari bilan himoyalangan bo'lsa ham, boshqa operatsion tizimni yoki vositani kompakt-diskdan yoki boshqasidan yuklash orqali ularni chetlab o'tish mumkin. bootable media... aynan shunday hujumlarning oldini olish uchun mo'ljallangan.

Tarmoq xavfsizligi kontseptsiyasi: asosiy fikrlar

Kompyuter tarmoqlarida axborot xavfsizligi foydalanuvchi nomi va parolni kiritish bilan bog'liq autentifikatsiyadan boshlanadi. Buning bir turi bitta omil. Ikki faktorli autentifikatsiya bilan qo'shimcha parametr qo'shimcha ravishda qo'llaniladi (xavfsizlik belgisi yoki "kalit", bankomat kartasi yoki mobil telefon), uch faktorli autentifikatsiya bilan noyob foydalanuvchi elementi (barmoq izi yoki retinani skanerlash) ham ishlatiladi.

Autentifikatsiya qilingandan so'ng, xavfsizlik devori kirish siyosatini qo'llaydi. Ushbu kompyuter tarmog'ining xavfsizligi xizmati ruxsatsiz kirishni oldini olishda samarali hisoblanadi, ammo ushbu komponent tarmoq orqali uzatiladigan kompyuter qurtlari yoki troyan dasturlari kabi xavfli tarkibni skanerlashi mumkin emas. Antivirus dasturi yoki tajovuzni oldini olish tizimi (IPS) bunday zararli dasturlarni aniqlash va blokirovka qilishga yordam beradi.

Ma'lumotlarni skanerlashga asoslangan kirishni aniqlash tizimi ham yuqori darajadagi tahlil uchun tarmoqni kuzatishi mumkin. Cheksiz kompyuter mashg'ulotlarini tarmoq trafigini to'liq tahlil qilish bilan birlashtirib, yangi tizimlar zararli insayderlar yoki foydalanuvchi kompyuteriga yoki akkauntiga zarar etkazgan tashqi zararli hasharotlar shaklida faol tarmoq tajovuzkorlarini aniqlashi mumkin.

Bundan tashqari, ko'proq shaxsiy hayotni ta'minlash uchun ikkita xost o'rtasidagi aloqa shifrlanishi mumkin.

Kompyuter himoyasi

Kompyuter tarmog'ini himoya qilishda qarshi choralar qo'llaniladi - tahdidni, zaiflikni yoki hujumni yo'q qilish yoki oldini olish, zararni minimallashtirish yoki zararni aniqlash va xabar berish bilan kamaytiradigan harakatlar, qurilmalar, protseduralar yoki usullar.

Xavfsiz kodlash

Bu kompyuter tarmoqlari uchun asosiy xavfsizlik choralaridan biridir. Dasturiy ta'minotni ishlab chiqishda xavfsiz kodlash zaifliklarning tasodifiy in'ektsiyasini oldini olishga qaratilgan. Xavfsizlik uchun boshidan boshlab yaratilgan dasturiy ta'minotni yaratish ham mumkin. Bunday tizimlar "dizayndagi xavfsiz" hisoblanadi. Bundan tashqari, rasmiy tekshirish tizim asosidagi algoritmlarning to'g'riligini isbotlashga qaratilgan. Bu, ayniqsa, kriptografik protokollar uchun juda muhimdir.

Ushbu chora, dasturiy ta'minot kompyuter tarmoqlarida axborot xavfsizligini ta'minlash uchun noldan ishlab chiqilganligini anglatadi. Bunday holda, bu asosiy xususiyat deb hisoblanadi.

Ushbu yondashuvning ba'zi usullari quyidagilarni o'z ichiga oladi:

1. Tizimning har bir qismi uning ishlashi uchun zarur bo'lgan ma'lum kuchlarga ega bo'lgan eng kam imtiyoz printsipi. Shunday qilib, tajovuzkor ushbu qismga kirish huquqini qo'lga kiritgan taqdirda ham, u butun tizim bo'yicha cheklangan kuchlarga ega bo'ladi.
2. Kodlarni ko'rib chiqish va birlik sinovlari - bu to'g'riligini rasmiy isbotlash imkoni bo'lmagan hollarda modullarni yanada xavfsizroq qilish uchun yondashuvlar.
3. Tizim va u saqlaydigan ma'lumotlarning yaxlitligini buzish uchun bir nechta quyi tizimlar buzilishi kerak bo'lgan dizayndagi chuqur mudofaa. Bu kompyuter tarmoqlari uchun yanada chuqurroq xavfsizlik texnikasi.

Xavfsizlik arxitekturasi

Ochiq xavfsizlik arxitekturasi AT xavfsizlik arxitekturasini "xavfsizlik nazorati (xavfsizlikka qarshi choralar) joylashuvi va ularning umumiy arxitektura bilan bog'liqligini tavsiflovchi dizayn artefaktlari" deb ta'riflaydi. axborot

texnologiyalari"Ushbu boshqaruv tizimlari maxfiylik, yaxlitlik, mavjudlik, hisobdorlik va ishonch kabi sifat sifatlarini saqlashga xizmat qiladi.

Boshqa mutaxassislar buni kompyuter tarmog'i xavfsizligi va xavfsizligi uchun yagona dizayn deb ta'riflaydilar axborot tizimlaribu ma'lum bir stsenariy yoki atrof-muhit bilan bog'liq bo'lgan ehtiyojlar va mumkin bo'lgan xatarlarni hisobga oladigan va ba'zi vositalarni qachon va qaerda qo'llashni belgilaydigan.

Uning asosiy xususiyatlari:

- turli xil tarkibiy qismlarning aloqasi va ularning bir-biriga bog'liqligi.
- risklarni baholash, ilg'or tajribalar, moliya va huquqiy masalalar asosida nazoratni aniqlash.
- boshqaruv elementlarini standartlashtirish.

Kompyuter tarmog'ining xavfsizligini ta'minlash

Kompyuterning "xavfsizlik" holati uchta jarayonni qo'llash orqali erishiladigan idealdir: tahdidlarning oldini olish, aniqlash va ularga javob berish. Ushbu jarayonlar turli xil siyosat va tizim tarkibiy qismlariga asoslanadi, ular quyidagilarni o'z ichiga oladi:

1. Himoya qila oladigan foydalanuvchi akkauntiga kirishni boshqarish va kriptografiya tizim fayllari va ma'lumotlar.
2. Kompyuter tarmoqlari xavfsizligi jihatidan eng keng tarqalgan profilaktika tizimlari bo'lgan xavfsizlik devorlari. Buning sababi shundaki, ular (agar to'g'ri tuzilgan bo'lsa) ichki tarmoq xizmatlariga kirishni himoya qilishlari va paketli filtrlash orqali hujumlarning ayrim turlarini bloklashlari mumkin. Xavfsizlik devorlari qo'shimcha yoki dasturiy ta'minot bo'lishi mumkin.
3. Tarmoqdagi hujumlarni qanday sodir bo'lishini aniqlash va hujumdan keyin yordam ko'rsatish uchun mo'ljallangan hujumni aniqlash

tizimlari (IDS), auditorlik izlari va kataloglari alohida tizimlar uchun xuddi shunday funktsiyani bajaradi.

"Javob" albatta baholangan xavfsizlik talablari bilan belgilanadi alohida tizim va oddiy xavfsizlikni yangilashdan tortib to tegishli organlarga xabar berish, qarshi hujum va boshqalarga qadar bo'lishi mumkin. Ba'zi maxsus holatlarda buzilgan yoki buzilgan tizimni yo'q qilish yaxshiroqdir, chunki barcha zaif manbalar topilmasligi mumkin.

Xavfsizlik devori nima?

Bugungi kunda kompyuter tarmog'ining xavfsizligi asosan xavfsizlik devorlari yoki tizimdan chiqish protseduralari kabi "profilaktika" choralarini o'z ichiga oladi.

Xavfsizlik devori xost yoki tarmoq va Internet kabi boshqa tarmoq o'rtasida tarmoq ma'lumotlarini filtrlash usuli sifatida aniqlanishi mumkin. Uni real vaqt rejimida filtrlash va blokirovka qilishni ta'minlash uchun tarmoq stekiga ulanadigan (yoki OS yadrosiga o'rnatilgan UNIXga o'xshash tizimlarda) ishlaydigan mashinada ishlaydigan dastur sifatida amalga oshirish mumkin. Boshqa bir dastur - bu "jismoniy xavfsizlik devori" deb nomlangan bo'lib, u tarmoq trafigini alohida filtrlashdan iborat. Bunday vositalar doimiy ravishda Internetga ulangan kompyuterlar orasida keng tarqalgan bo'lib, kompyuter tarmoqlarining axborot xavfsizligini ta'minlashda faol foydalanilmoqda.

Ma'lumotlarning mavjudligi va rivojlangan doimiy tahdidlarni aniqlash uchun mashinalarni o'rganish uchun ba'zi tashkilotlar yirik ma'lumotlar platformalariga murojaat qilishmoqda (masalan, Apache Hadoop).

Biroq, nisbatan kam sonli tashkilotlar samarali aniqlash tizimlariga ega kompyuter tizimlarini qo'llab-quvvatlaydilar va ularning javob berish mexanizmlari ham kamroq. Bu kompyuter tarmog'ining texnologik xavfsizligini ta'minlash muammolarini tug'diradi. Xavfsizlik devorlariga va boshqa avtomatlashtirilgan aniqlash tizimlariga ishonish kiberjinoyatchilikni samarali yo'q qilish uchun asosiy to'siqdir. Biroq, bu hujumlarni to'xtatadigan paketlarni yig'ish moslamalari yordamida asosiy ma'lumotlarni yig'ishdir.

Zaifliklarni boshqarish

Zaifliklarni boshqarish - bu, ayniqsa, dasturiy ta'minot va dasturiy ta'minotdagi zaifliklarni aniqlash, tiklash yoki kamaytirish tsikli. Ushbu jarayon kompyuter tizimlari va tarmoqlarini xavfsizligini ta'minlashning ajralmas qismi hisoblanadi.

Ochiq portlar, xavfli dasturiy ta'minot konfiguratsiyasi va zararli dasturlarga qarshi zaiflik kabi ma'lum bo'lgan "zaif" tomonlarni qidiradigan kompyuter tizimini tahlil qiladigan skaner yordamida zaifliklarni aniqlash mumkin.

Zaif tomonlarni skanerlashdan tashqari, ko'plab tashkilotlar o'z tizimlarida muntazam ravishda penetratsion sinovlarni o'tkazish uchun xavfsizlik autsorsingi bilan shartnoma tuzadilar. Ba'zi tarmoqlarda bu shartnoma shartidir.

Zaif tomonlarni kamaytirish

Kompyuter tizimlarining to'g'riligini rasmiy tasdiqlash mumkin bo'lsa-da, bu hali keng tarqalgan emas. Rasmiy ravishda sinovdan o'tgan operatsion tizimlarga seL4 va SYSGO PikeOS kiradi, ammo ular bozorning juda oz foizini tashkil qiladi.

Tarmoqda axborot xavfsizligini ta'minlaydigan zamonaviy kompyuter tarmoqlari ikki faktorli autentifikatsiya va kriptografik kodlardan faol foydalanmoqda. Bu quyidagi sabablarga ko'ra xavflarni sezilarli darajada kamaytiradi.

Kriptografiyani buzish bugungi kunda deyarli mumkin emas. Uni amalga oshirish uchun ma'lum bir kriptografik bo'lmagan kiritish kerak (noqonuniy ravishda olingan kalit, oddiy matn yoki boshqa qo'shimcha kriptanalitik ma'lumotlar).

Bu tizimga yoki maxfiy ma'lumotlarga ruxsatsiz kirishni yumshatish usuli. Xavfsiz tizimga kirish uchun ikkita element kerak:

- "Siz bilgan narsalar" - parol yoki PIN kod;
- "Sizda bor narsa" - karta, kalit, mobil telefon yoki boshqa jihozlar.

Bu kompyuter tarmoqlari xavfsizligini oshiradi, chunki ruxsatsiz foydalanuvchi kirish uchun bir vaqtning o'zida ikkala elementga ham ehtiyoj sezadi. Xavfsizlik choralariga qanchalik qattiq rioya qilsangiz, shunchalik kam sindirishlar bo'lishi mumkin.

Maxsus brauzerlardan foydalangan holda, tizimingizni xavfsizlik tuzatishlari va yangilanishlari bilan doimiy ravishda yangilab, tajovuzkorlarning imkoniyatlarini kamaytirishingiz mumkin. Ma'lumotlarning yo'qolishi va

zararlanishining ta'siri ehtiyotkorlik bilan ishlab chiqilishi bilan kamaytirilishi mumkin zaxira nusxalari va saqlash.

Uskunani himoya qilish mexanizmlari

Uskuna ham tahdid solishi mumkin. Masalan, xakerlik ishlab chiqarish jarayonida zararli ravishda kiritilgan mikrochiplardagi zaifliklar yordamida amalga oshirilishi mumkin. Kompyuter tarmoqlarida ishlash uchun apparat yoki yordamchi xavfsizlik ham ma'lum himoya usullarini taklif etadi.

Kirish tugmachalari, ishonchli platforma modullari, kirishni aniqlash tizimlari, diskni blokirovka qilish, USB portni o'chirib qo'yish va yordamga kirish kabi qurilmalar va usullardan foydalanish mobil aloqasaqlangan ma'lumotlarga jismoniy kirish zarurati tufayli yanada xavfsiz deb hisoblanishi mumkin. Ularning har biri quyida batafsilroq tavsiflanadi.

Kalitlar

USB kalitlari odatda dasturni litsenziyalashni ochishda ishlatiladi dasturiy ta'minot imkoniyatlari, lekin ularni kompyuteringizga yoki boshqa qurilmangizga ruxsatsiz kirishni oldini olishning bir usuli sifatida ham ko'rish mumkin. Kalit u bilan o'rtasida ishonchli shifrlangan tunnel hosil qiladi dasturiy ta'minot... Bu printsip shundan iboratki, foydalanilgan shifrlash sxemasi (masalan, AdvancedEncryptionStandard (AES)) kompyuter tarmoqlarida yuqori darajadagi axborot xavfsizligini ta'minlaydi, chunki shunchaki o'z dasturiy ta'minotingizni boshqa kompyuterga nusxalash va undan foydalanishdan ko'ra kalitni yorish va takrorlash qiyinroq.

Bunday kalitlarning yana bir ishlatilishi - bu bulutli dasturiy ta'minot yoki virtual xususiy tarmoqlar (VPN) kabi veb-tarkibga kirish uchun foydalanish. Bundan tashqari, USB tugmasi kompyuterni blokirovka qilish yoki qulfdan chiqarish uchun sozlanishi mumkin.

Himoyalangan qurilmalar

Ishonchli platforma menejmenti (TPM) qurilmalari mikroprotsessorlar yoki chipdagi kompyuterlar deb ataladigan kriptografik imkoniyatlarni kirish qurilmalariga birlashtiradi. Server tomonidagi dasturiy ta'minot bilan birgalikda foydalaniladigan TPMlar qo'shimcha qurilmalarni kashf qilish va ularni tasdiqlash, shuningdek, tarmoq va ma'lumotlarga ruxsatsiz kirishni oldini olish uchun mohirona usulni taklif etadi.

Intruziyani aniqlash mashina ochilganda faollashtiriladigan tugmachali tugma yordamida amalga oshiriladi. Qurilma yoki BIOS dastur keyingi safar qurilma yoqilganda foydalanuvchini ogohlantirish uchun dasturlashtirilgan.

Bloklash

Kompyuter tarmoqlari xavfsizligi va axborot tizimlarining xavfsizligiga disklarni blokirovka qilish orqali erishish mumkin. Bu asosan dasturiy ta'minotni shifrlash vositalari qattiq disklarularni ruxsatsiz foydalanuvchilar uchun kirish imkoniga ega bo'lmaslik. Ba'zi ixtisoslashgan vositalar tashqi disklarni shifrlash uchun maxsus ishlab chiqilgan.

USB portlarini o'chirib qo'yish - bu sizning himoyalangan kompyuteringizga ruxsatsiz va zararli kirishni oldini olish uchun yana bir keng tarqalgan xavfsizlik sozlamalari. Xavfsizlik devori ichidagi qurilmadan tarmoqqa ulangan USB-dongllar kompyuter tarmog'i uchun eng keng tarqalgan tahdid deb hisoblanadi.

Qo'llab-quvvatlanadigan mobil qurilmalar uyali aloqa keng tarqalganligi sababli tobora ommalashib bormoqda uyali telefonlar... Bluetooth, so'nggi past chastotali aloqa (LE) va yaqin masofadagi aloqa (NFC) kabi ichki imkoniyatlar davolash vositalarini izlashga olib keldi. Bugungi kunda biometrik tekshirish (barmoq izini o'qish) va QR kodini o'qish uchun mo'ljallangan dastur mobil qurilmalar... Bularning barchasi yangi, xavfsiz usullar ulanishlar mobil telefonlar boshqaruv tizimlariga kirish uchun. Bu ta'minlaydi kompyuter xavfsizligiva shuningdek, himoyalangan ma'lumotlarga kirishni boshqarish uchun ishlatilishi mumkin.

Imkoniyatlar va kirishni boshqarish ro'yxatlari

Kompyuter tarmoqlarida axborot xavfsizligining xususiyatlari imtiyozlarni ajratish va kirish darajasiga asoslangan. Ikkita bunday modellar keng tarqalgan bo'lib foydalanishni boshqarish ro'yxatlari (ACL) va xususiyatlarga asoslangan xavfsizlikdir.

Dasturlarning ishlashini cheklash uchun ACL-lardan foydalanish ko'p holatlarda xavfli ekanligini isbotladi. Masalan, xost kompyuterni aldov yo'li bilan cheklangan faylga kirishga ruxsat berish mumkin. Shuni ham ko'rsatdiki, ACL-ning ob'ektga faqat bitta foydalanuvchiga kirish huquqini berish to'g'risidagi va'dasi amalda hech qachon kafolatlanishi mumkin emas. Shunday qilib, bugungi kunda ACL asosidagi barcha tizimlarda amaliy kamchiliklar mavjud, ammo ishlab chiquvchilar faol ravishda ularni tuzatishga harakat qilmoqdalar.

Imkoniyatlarga asoslangan xavfsizlik asosan tadqiqotlarda qo'llaniladi operatsion tizimlar, tijorat operatsion tizimlari hali ham ACL-lardan foydalanmoqda. Shu bilan birga, qobiliyatlar faqat til darajasida amalga

oshirilishi mumkin, bu asosan dasturga xos uslubga olib keladi, bu asosan standart ob'ektga yo'naltirilgan dizaynni takomillashtiradi.

Ma'lumotlaringiz xavfsizligiga asosiy tahdid Butunjahon Internet tarmog'idan kelib chiqadi. Qanday ta'minlash kerak ishonchli himoya uy tarmog'i?

Ko'pincha, foydalanuvchilar Internetga ulangan uy kompyuterini himoya qilish uchun odatiy antivirus etarli deb noto'g'ri o'ylashadi. Routerlarning qutilaridagi yozuvlar ham chalg'ituvchi bo'lib, ushbu qurilmalar apparat darajasida xakerlar hujumlaridan himoya qila oladigan kuchli xavfsizlik devoriga ega. Ushbu so'zlar qisman haqiqatdir. Avvalo, ikkala vosita ham to'g'ri sozlashni talab qiladi. Biroq, ko'plab antivirus paketlarida oddiygina xavfsizlik devori xususiyati yo'q.

Shu bilan birga, vakolatli himoya Internetga ulanishdan boshlanadi. Zamonaviy uy tarmoqlarida, qoida tariqasida, Wi-Fi routerlari kabel orqali Ethetnet ulanishidan foydalaniladi. Mahalliy tarmoq orqali Internetga kirish imkoniyati mavjud ish stoli kompyuterlar va noutbuklar, smartfonlar va planshetlar. Bundan tashqari, bitta to'plamda ikkala kompyuterning o'zi va atrof-muhitmasalan, printerlar va brauzerlar, ularning aksariyati tarmoq orqali ulanadi.

Hujumchi sizning kirish nuqtangizni buzish bilan nafaqat sizning Internet-ulanishingizdan foydalanishi va uy kompyuterlaringizni boshqarishi, balki IP-manzilingizdan foydalangan holda World Wide Web-da noqonuniy tarkibni joylashtirishi, shuningdek, tarmoqqa ulangan uskunalarda saqlangan ma'lumotlarni o'g'irlashi mumkin. Bugun biz tarmoqlarni himoya qilish, ularning ish faoliyatini ta'minlash va buzishni oldini olishning asosiy qoidalari haqida gaplashamiz.

Uskuna

Ko'pgina zamonaviy tarmoq uskunalari xavfsizlik sozlamalarini talab qiladi. Eng avvalo u keladi turli xil filtrlar, xavfsizlik devorlari va rejalashtirilgan kirish ro'yxatlari haqida. Tayyor bo'lmagan foydalanuvchi shuningdek himoya parametrlarini o'rnatishi mumkin, ammo siz ba'zi bir nuanslarni bilishingiz kerak.

Yo'l transporti shifrlash usulidan foydalanamiz Kirish nuqtasini o'rnatayotganda, eng ishonchli transport vositalarini himoya qilish mexanizmlarini yoqish, murakkab, ma'nosiz parolni yaratish va AES shifrlash bilan WPA2-dan foydalanish haqida g'amxo'rlik qiling. WEP eskirgan va bir necha daqiqada yorilib ketishi mumkin.

Hisob-kitoblarni muntazam ravishda o'zgartiramiz Kuchli kirish parollarini o'rnating va ularni muntazam ravishda o'zgartiring (masalan, har olti oyda bir). Eng oson yo'li - foydalanuvchi standart foydalanuvchi nomi va parolini "admin" / "admin" qoldirgan qurilmani buzishdir.

SSIDni yashirish SSID (Service Set Identifier) \u200b\u200b- simsiz tarmoqning ommaviy nomi, foydalanuvchi qurilmalari buni ko'rishlari uchun havo orqali tarqatiladi. SSID-ni yashirish opsiyasidan foydalanib, yangi boshlangan tajovuzkorlardan himoya qilinadi, ammo keyin yangi qurilmalarni ulash uchun kirish nuqtasi parametrlarini qo'lda kiritishingiz kerak bo'ladi.

Maslahat Kirish nuqtasini birinchi marta o'rnatishda SSID-ni o'zgartiring, chunki bu nom yo'riqchining modelini aks ettiradi, bu zaif tomonlarni qidirishda tajovuzkorga maslahat bo'lishi mumkin.

O'RNATILGAN FIREWALL TASHKILOTI Ko'p hollarda marshrutizatorlar xavfsizlik devorlarining oddiy versiyalari bilan jihozlangan. Ularning yordami bilan tarmoqdagi xavfsiz ishlash uchun ko'plab qoidalarni yaxshilab sozlashning iloji bo'lmaydi, lekin siz asosiy zaifliklarni qoplashingiz yoki masalan, ishni taqiqlashingiz mumkin pochta mijozlari.

MAC ADDRESS tomonidan kirish huquqini cheklash MAC-manzillar ro'yxatidan (Media Access Control) foydalanib, jismoniy manzillari bunday ro'yxatga kiritilmagan qurilmalar uchun mahalliy tarmoqqa kirishni rad etishingiz mumkin. Buning uchun siz tarmoq tomonidan tasdiqlangan uskunalar ro'yxatini qo'lda yaratishingiz kerak bo'ladi. Har bir qurilma jihozlangan tarmoq interfeysi, zavod tomonidan tayinlangan noyob MAC-manzil mavjud. Uni uskunadagi yorliqqa yoki belgilarga qarab yoki maxsus buyruqlar va tarmoq skanerlaridan foydalanib tanib olish mumkin. Agar sizda veb-interfeys yoki displey mavjud bo'lsa (masalan, yo'riqnoma va tarmoq printerlari), sozlamalar menyusida MAC manzilini topishingiz mumkin.

Kompyuterning tarmoq kartasining MAC manzilini uning xususiyatlaridan topish mumkin. Buning uchun “Boshqaruv paneli | Tarmoqlar va Internet | Tarmoq va almashish markazi "-ni tanlang, so'ng oynaning chap qismida" Adapter sozlamalarini o'zgartirish "havolasiga o'ting, foydalanilayotgan tarmoq kartasini o'ng tugmasini bosing va" Holat "-ni tanlang. Ochilgan oynada "Tafsilotlar" tugmachasini bosishingiz va tarmoq kartangizning MAC manzilini ko'rsatib, olti juft raqam ko'rsatiladigan "Fizik manzil" qatoriga qarashingiz kerak.

Yana ko'p narsalar mavjud tezkor yo'l... Uni ishlatish uchun "Win + R" tugmalar birikmasini bosing, paydo bo'lgan qatorda CMD-ni kiriting va "OK" tugmasini bosing. Ochilgan oynada buyruqni kiriting:

Enter tugmasini bosing. Ko'rsatilgan ma'lumotlarda "Fizik manzil" satrlarini toping - bu qiymat MAC-manzil.

Dasturiy ta'minot

Tarmoqni jismoniy himoya qilib, "mudofaa" ning dasturiy ta'minotiga g'amxo'rlik qilish kerak. Bunda sizga murakkab antivirus paketlari, xavfsizlik devorlari va zaiflik skanerlari yordam beradi.

FOYDALARGA KIRISHNI O'RNATISH Tizimdagi papkalarni yoki faqat muhim ma'lumotlarni foydalanuvchilar uchun qulay bo'lgan kataloglarga joylashtirmang ichki tarmoq... Bundan tashqari, tizim diskida tarmoqqa kiradigan papkalarni yaratmaslikka harakat qiling. Bunday kataloglarning barchasi, agar alohida ehtiyoj bo'lmasa, "Faqat o'qish" atributini cheklash yaxshiroqdir. Aks holda, hujjat niqobidagi virus umumiy papkada joylashishi mumkin.

TARMOQ EKRANINI O'RNATING Dasturiy ta'minot xavfsizlik devorlarini sozlash oson va o'z-o'zini o'rganish rejimiga ega. Uni ishlatishda

dastur foydalanuvchidan qaysi ulanishlarni ma'qullashini va qaysi birini rad etishni zarur deb bilishini so'raydi.

Kasperskiy Iinternet Security kabi mashhur savdo mahsulotlariga o'rnatilgan shaxsiy xavfsizlik devorlaridan foydalanishni tavsiya etamiz, Norton internet Xavfsizlik, NOD Internet Security, shuningdek Comodo Firewall kabi bepul echimlar. Xodimlar bilan ta'minlangan windows xavfsizlik devoriafsuski, u faqat asosiy port sozlamalarini ta'minlaydigan ishonchli xavfsizlik bilan maqtana olmaydi.

Zaiflik testi

Kompyuteringiz va tarmoq salomatligi uchun eng katta xavf "teshiklari" va noto'g'ri tuzilgan himoya vositalarini o'z ichiga olgan dasturlar tomonidan yuzaga keladi.

XSpider Tarmoqni zaif tomonlarini skanerlash uchun ishlatish uchun qulay dastur. Bu sizga dolzarb muammolarning aksariyatini tezda aniqlashga imkon beradi, shuningdek ularning tavsifi va ba'zi hollarda echimlarini taqdim etadi. Afsuski, bir muncha vaqt oldin kommunal xizmat pullik bo'ldi va bu, ehtimol, uning yagona kamchilikidir.

NmapTijorat bo'lmagan ochiq manbali tarmoq skaneri manba kodi... Dastur dastlab UNIX foydalanuvchilari uchun ishlab chiqilgan, ammo keyinchalik ommalashganligi sababli Windows-ga ko'chirildi. Yordamchi dastur mo'ljallangan tajribali foydalanuvchilar... Nmap oddiy va qulay interfeysammo, u ishlab chiqaradigan ma'lumotlarni asosiy bilimsiz tushunish qiyin bo'ladi.

KIS 2013 Ushbu to'plam nafaqat keng qamrovli himoya, balki diagnostika vositalarini ham taqdim etadi. Siz uni skanerlash uchun ishlatishingiz mumkin o'rnatilgan dasturlar muhim zaifliklar uchun. Ushbu protsedura natijasida dastur kommunal xizmatlar ro'yxatini taqdim etadi, bu bo'shliqlarni yopish kerak va har bir zaiflik haqida batafsil ma'lumot va uni qanday tuzatish mumkin.

Tarmoqni o'rnatish bo'yicha maslahatlar

Siz tarmoqni nafaqat uni joylashtirish va sozlash bosqichida, balki u allaqachon mavjud bo'lganda ham xavfsizroq qilishingiz mumkin. Xavfsizlikni ta'minlashda ulangan qurilmalar sonini, joylashishini hisobga olish kerak tarmoq kabeli, Wi-Fi signalining tarqalishi va unga to'sqinlik qiladigan turlar.

Kirishning bir nuqtasini joylashtirish Wi-Fi tarmog'iga qancha hududni kiritish kerakligini taxmin qiling. Agar sizning kvartirangizning faqat maydonini qoplashingiz kerak bo'lsa, unda simsiz kirish nuqtasini derazalar yoniga qo'ymasligingiz kerak. Bu nazoratchilar - bepul simsiz Internetga ulanish punktlarini qidirayotgan va noqonuniy usullardan foydalangan holda zaif himoyalangan kanalni ushlab qolish va buzish xavfini kamaytiradi. Shuni esda tutish kerakki, har bir beton devor signal kuchini yarimga kamaytiradi. Shuni ham yodda tutingki, shkaf oynasi - bu Wi-Fi signali uchun deyarli o'tib bo'lmaydigan ekran bo'lib, u ba'zi hollarda radio to'lqinlarining kvartirada ma'lum yo'nalishlarda tarqalishini oldini olish uchun ishlatilishi mumkin. Bundan tashqari, ba'zi Wi-Fi routerlari apparat signal kuchini sozlash imkonini beradi. Ushbu parametr yordamida siz kirish nuqtasi bo'lgan xonadagi foydalanuvchilarga sun'iy ravishda

kirishni taqdim etishingiz mumkin. Ushbu usulning nochorligi sizning kvartirangizning chekka joylarida signal etishmasligi mumkin.

QABUL QILISH Asosan kabel yordamida tashkil etilgan tarmoq aloqa eng yuqori tezligi va ishonchliligini ta'minlaydi va shu bilan birga unga Wi-Fi ulanishi bilan tashqi tomondan bog'lanish imkoniyati chiqarib tashlanadi. Wi-Fi ulanishi bilan sodir bo'lishi mumkinligi sababli, unga yonboshlab turish ehtimoli. Ruxsatsiz ulanishni oldini olish uchun kabel tarmog'ini yotqizayotganda simlarni mexanik shikastlanishdan himoya qilish to'g'risida g'amxo'rlik qiling, maxsus simi kanallaridan foydalaning va shnur juda ko'p osilib turadigan yoki aksincha haddan tashqari taranglashadigan joylarga yo'l qo'ymang. Kabelni kuchli shovqin manbalari yaqinida yoki yomon muhitda (haddan tashqari harorat va namlik) o'tkazmang. Shu bilan bir qatorda, siz ekranlangan kabeldan foydalanishingiz mumkin qo'shimcha himoya.

Elementdan himoya qilish Simli va simsiz tarmoqlar momaqaldiroqlarga ta'sir qiladi va ba'zi hollarda chaqmoq chaqishi nafaqat tarmoq uskunalariga, balki tarmoq kartasishuningdek, ko'plab kompyuter komponentlari. Ushbu xavfni kamaytirish uchun avval elektr rozetkalarini va kompyuter qismlarini erga ulang. Shovqin va kuchlanishdan himoya qilish davrlarini o'z ichiga olgan Pilot tipidagi qurilmadan foydalaning.

Bundan tashqari, uzluksiz quvvat manbai (UPS) eng yaxshi echim bo'lishi mumkin. Zamonaviy versiyalar ikkala kuchlanish stabilizatorlarini va avtonom elektr ta'minotini, shuningdek ular orqali tarmoq kabelini ulash uchun maxsus ulagichlarni o'z ichiga oladi. Agar to'satdan Internet-provayderning uskunasiga chaqmoq tushsa, bunday UPS sizning kompyuteringizning tarmoq kartasida zararli quvvat oqimiga yo'l qo'ymaydi. Shuni esda tutish kerakki, har qanday holatda, rozetkalarni yoki jihozni o'zi erga ulash juda muhimdir.

VPN tunnel qurish vositalaridan foydalanish

VPN tunnellari (Virtual Private Network) tarmoq orqali uzatiladigan ma'lumotlarni himoya qilishning juda ishonchli usuli hisoblanadi. Tunnel texnologiyasi shifrlangan kanalni yaratadi, bu orqali ma'lumotlar bir nechta qurilmalar o'rtasida uzatiladi. Uy tarmog'ida axborotni himoya qilishni kuchaytirish uchun VPN-ni tashkil qilish mumkin, ammo bu juda zahmatli va talab qiladi maxsus bilim... VPN-dan foydalanishning eng keng tarqalgan usuli bu uy kompyuteringizga tashqi tomondan, masalan, ish kompyuteringizdan ulanishdir. Shunday qilib, sizning mashinalaringiz o'rtasida uzatiladigan ma'lumotlar trafikni shifrlash bilan yaxshi himoyalangan bo'ladi. Ushbu maqsadlar uchun juda ishonchli foydalanish yaxshiroqdir bepul dastur Hamachi. Bunday holda, sizga faqat tayyor bo'lmagan foydalanuvchi vakolatiga kiradigan VPN tashkilotining asosiy bilimlari kerak bo'ladi.