TARMOQDA HIMOYANI TA'MINLASH ZAMONAVIY CHORALARI VA TAVSIYALARI

Sultonmuratova Mashhura Quvonchbek qizi
TATU Urganch filiali talabasi
E-mail: sultonmuratovamashhura@gmail.com

Annotatsiya. Bu maqolada tarmoqda himoyani ta'minlash zamonaviy choralari va tavsiyalari, shuningdek, ularning qo'llanilishi, ularning muhimligini va amaliyotga tatbiq etilishi mumkin bo'lgan foydalarini o'rganish mumkin. Tarmoq xavfsizligi sohasidagi asosiy standartlarni va tavsiyalarni identifikatsiya qilish, standartlarning amaliyotga tatbiq etish haqida ma'lumotlar berilgan.

Аннотация. В этой статье рассматриваются современные меры и рекомендации по сетевой безопасности, а также их применение, важность и практическая польза. Дана информация об определении основных стандартов и рекомендаций в области сетевой безопасности, а также о внедрении стандартов.

Annotation. This article explores modern network security measures and recommendations, as well as their application, importance, and practical benefits. Information is given on the identification of the main standards and recommendations in the field of network security, and the implementation of the standards.

Kalit so'zlar: IDS prinsipi, kriptografiya, non-profit tashkilot, xavfsizlik, OWASP.

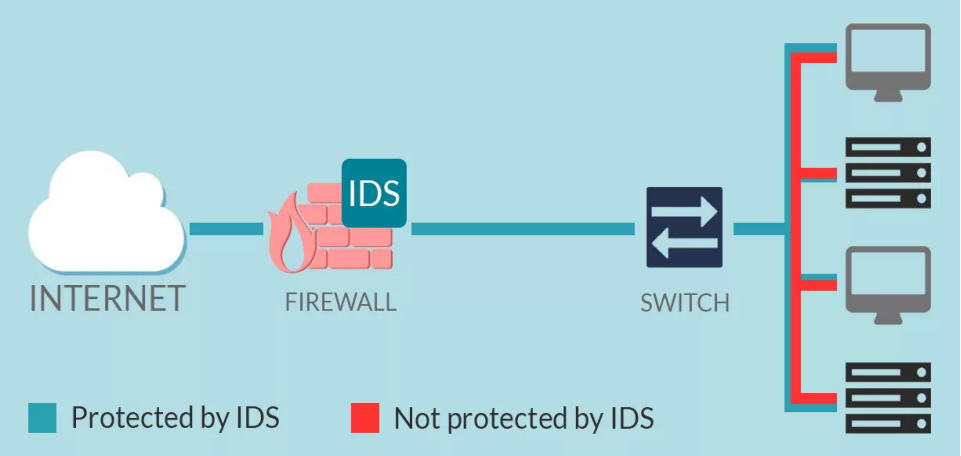
Ключевые слова: Принцип IDS, криптография, некоммерческая организация, безопасность, OWASP.

Key words: IDS principle, cryptography, non-profit organization, security, OWASP.

Kirish. Telekommunikatsiya texnologiyalari sohasida standart atamasi, texnologiyalar, protokollar va kommunikatsiya tizimlari uchun o'zaro muvofiqlikni ta'minlash maqsadida belgilangan standartlarni qo'llashni va amalga oshirishni ifodalaydi. Standart atamalari, telekomunikatsiya sohasidagi bir qator muhim tashkilotlar va qo'llanmalar tomonidan belgilanadi.

IDS (Intrusion Detection System) – buzg'unchilikni aniqlash tizimi degan ma'noni anglatadi. IDS prinsipi trafik tahlili asosida tahdidlarni aniqlashdan iborat, ammo keyingi harakatlar administratorga bog'liq. IDS tizimlari o'rnatish joyi va ishlash prinsipiga ko'ra turlarga bo'linadi. Ushbu sohada eng keng tarqalgan ikkita IDS turi mavjud:

1. Network Intrusion Detection System (NIDS);
2. Host-based Intrusion Detection System (HIDS).



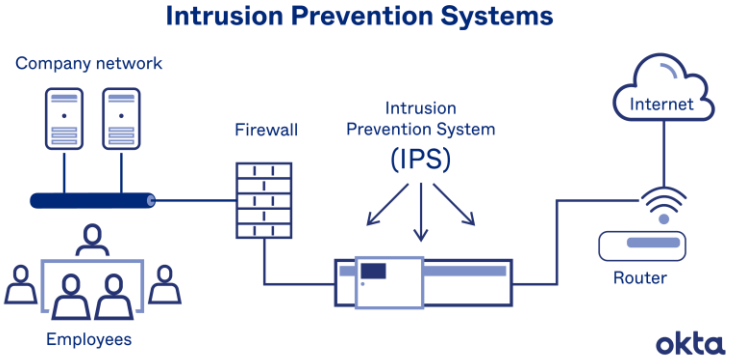
1-rasm. IDS ishlash prinsipi

IPS (Intrusion Prevention System) - bu kirishni oldini olish tizimi. An'anaviy himoya vositalariga nisbatan antivirus, spam-filtrlar, xavfsizlik devorlari - IDS / IPS tarmoq himoyasini ancha yuqori darajada ta'minlaydi.

IPS tarmoqdagi xavfli faoliyat shakllarini aniqlash va oldini olish uchun bir nechta usullardan foydalanadi. Ular orasida imzolarini (signature-based) va imzolaridan tashqari metodlarni (anomaly-based) hisobga oladi.

1. Imzolar: IPS avvaldan bilinadigan xavfli faoliyat imzolarini (misol uchun, virus, trojanlar, port skanerlar) taqiqlaydi. Ular har bir xavfli faoliyat shakliga mos keladigan imzolar katalogida saqlanadi. Tarmoqdagi trafikni monitoring qilish orqali IPS imzolarni trafikda qidirib topadi va qo'llanuvchilarni xavfli faoliyatga qarshi himoya qiladi.

2. Anomaliya asosida: IPS normal tarmoq holatini model qiladi va tarmoqdagi anomaliyalarni aniqlash uchun qo'llanadi va tarmoqdagi obyektlarning tavsiya etilgan holatlarini (masalan, portlar, protokollar, kirish/chiqishlar) o'rganadi va tarmoqdagi har qanday anomaliyalarni aniqlab chiqaradi. Masalan, agar bir qurilmadan katta miqdorda ma'lumotlar yuborilsa yoki bir portdan tavsiya etilgan miqdordan ko'p so'rovlar kelgan bo'lsa, bu anomaliyalar sifatida tan olinadi.



2-rasm. IPS ishlash prinsipi

Himoyani ta’minlashning zamonaviy choralari quyidagilarni o‘z ichiga oladi:

- Kriptografiya: bu texnologiya bir qator himoya xizmatlarini ta’minlaydi, jumladan, ma’lumotlarni jo‘natish va saqlash vaqtida shifrlash;
- Ruxsatni nazorat qilish: maqsad, asosiy kompyuter yoki tarmoqdagi ma’lumotlarni kirishga ruxsat etilgan foydalanuvchilar tomonidan foydalanishni, tomosha qilishni yoki o‘zgartirishni chegaralashdan iborat;
- Tizimning butunligi: maqsad tizim va undagi ma’lumotlar asosiy vakil bo‘lmagan tomon yoki ruxsat etilmagan shaklda o‘zgartirilmasligi yoki buzilmasligini ta’minlashdan iborat;
- Audit, ro‘yxatdan o‘tkazish va monitoring: tizim administratorlariga yovuz niyatli ta’sirlar vaqtida va undan keyin tarmoq jurnalini yig‘ish va tahlil qilishga yordam beradi. Ma’lumotlar tarmoqda qo‘llanilgan himoya strategiyasi samarasini baholashda qo‘llaniladi.
- Boshqaruv: tizim admisintratorlariga ularning asosiy kompyuteri va tarmog‘idagi xavfsizlik parametrlarini tahlil qilish va sozlashda yordam beradi. Administrativ nazorat tarmoq faoliyati aniqligini tekshirish uchun va sozlash elementlarini ulash uchun ishlatilishi mumkin.

Tarmoq xavfsizligini ta’minlashda, zamonaviy, eng yaxshi standartlar va kerakli amaliyotlar mavjud. Quyidagi standartlar tarmoq xavfsizligi sohasidagi eng yuqori darajali amaliyotlarni belgilashda yordam beradi:

1. ISO 27001: “Information Security Management Systems (ISMS) – Requirements” nomi bilan ma’lum bo‘lgan xalqaro standartdir. Bu standart tashkilotlar uchun ma’lumotlar xavfsizligi boshqarish tizimini qurish va boshqarishga yo‘naltirilgan talablarni belgilaydi, shuningdek, tashkilotlarga ma’lumotlar xavfsizligini tahlil qilish, risklarini boshqarish, obyektlarini boshqarish, xavfsizlikning amalga oshirilishini kuzatish va tahlil qilish, xavfsizlik tashkilotining ma’lumotlar xavfsizligi faoliyatini boshqarish va uning natijalarini baholashga yordam beradi.

3-rasm. ISO 27001 standartining boshqarish tizimi

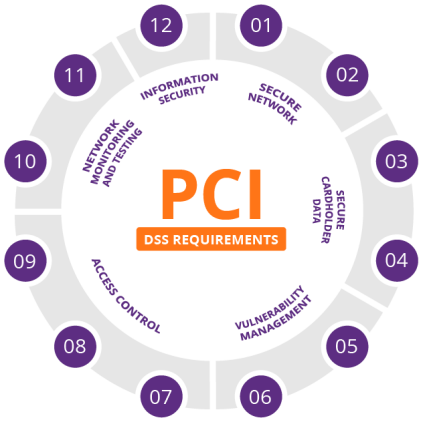
2. CIS Controls: “Center for Internet Security Controls” (Internet Xavfsizligi Markazining Boshqaruv Kontrollari) – ma’lumotlar xavfsizligi sohasida faol tashkilotlar uchun amaliyotlar, usullar va maslahatlar to‘plamini o‘z ichiga oladi. Bu standart ma’lumotlar xavfsizligi sohasidagi eng asosiy qo‘llanmalarni o‘z ichiga olgan 18 ta asosiy kontrollarni belgilaydi.

4-rasm. CIS Controls standarti kontrollari

3. GDPR (General Data Protection Regulation): Yevropada shaxsiy ma’lumotlarni himoya qilish va ulardan foydalanishni boshqarishga doir umumiy qoidalar to‘plami hisoblanadi. Bu standart tashkilotlarga shaxsiy ma’lumotlarni to‘plash, saqlash va ulardan foydalanish jarayonlarini boshqarishda kerakli bo‘lgan talablarni va amaliy usullarni taqdim etadi.

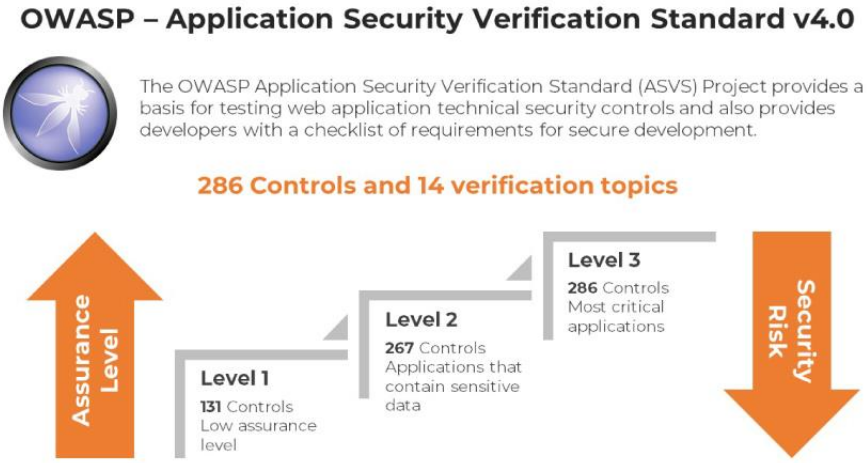
5-rasm. GDPR standartining boshqaruv tizimi

4. PCI DSS (Payment Card Industry Data Security Standard): To‘lov kartalari ma’lumotlarini himoya qilishga oid xalqaro standart hisoblanadi. Bu standart to‘lov kartalari bilan bog’liq ma’lumotlarni qabul qilish, saqlash, ulardan foydalanish va ulardan foydalanishni cheklash jarayonlarini boshqarishga oid talablarni belgilaydi.



6-rasm. PCI DSS standartining boshqaruv tizimi

5. OWASP – “Open Web Application Security Project” (Ochiq Veb Ariza Xavfsizligi Proyekti): Bu non-profit tashkilot, ochiq manbali dasturlar va veb ilovalarning xavfsizligi bilan bog’liq masalalarni tahlil qilish, ma’lumotlar va resurslarni taqdim etish, maslahatlar berish va xavfsizlik bo‘yicha standartlarni ishlab chiqish bilan shug’ullanadi.



7-rasm. OWASP standartining boshqaruv tizimi

Standartlar odatda xalqaro tashkilotlar, sohalarni tashkil qilgan institutlar, sohalarni reglamentatsiya qilgan davlat va sohalaridagi xavfsizlik sohasidagi mutaxassislar tomonidan yaratiladi va yangilanadi.

Tarmoq xavfsizligini ta’minlash uchun quyidagi tavsiyalarga amal qilinadi:

1. Xavfsizlik sozlamalarini tekshirish: Tarmoq qurilishlaridagi xavfsizlik sozlamalarini tekshirib, tavsiya etilgan xavfsizlik sozlamalarini o‘rnatishni ta’minlash (parollar, tarmoq segmentlari orqali kirishni cheklash, atrofni nazorat qilish va boshqa xavfsizlik sozlamalari bilan bog’liq);

2. Xavfsizlik protokollari va algoritmlaridan foydalanish: Tarmoqda xavfsizlikni ta’minlash uchun yuqori darajada xavfsizlik protokollari va algoritmlaridan foydalanish (misol uchun, WPA2 yoki WPA3 kabi xavfsizlik protokollari va TLS (Transport Layer Security) kabi xavfsizlik protokollari tarmoqdagi ma’lumot almashishni shifrlashga yordam beradi);

3. Yangilanishlarni o‘rnatish: Tarmoq tizimlaridagi xavfsizlik bo‘shliqlarini yopish uchun tizimdagi ba’zi tizimlar va dasturlarni yangilash;

4. Xavfsizlikni monitor qilish: Tarmoqni xavfsizlikni nazorat qilish uchun xavfsizlikni monitor qilish vositalaridan foydalanish (bu vositalar tarmoqdagi faolliklarni kuzatib borish, nizolarni aniqlash, zararli faoliyat va xavfsizlik hujjatlari bilan bog’liq xabarlarini aniqlashga yordam beradi);

5. Foydalanuvchilar uchun xavfsizlik ta’limoti: Foydalanuvchilarga xavfsizlik sohasida ta’lim berish (foydalanuvchilarga parolni to‘g’ri saqlash, xavfsizlik sozlamalarini tushunish, e-mail yoki internet bilan bog’liq qo‘llanuvchiga tegishli xabarlar haqida ma’lumot berish);

6. Ma’lumotlarni nusxalash va tiklash: Tarmoqdagi ma’lumotlarni nusxalash va tiklash (ma’lumotlarning yo‘qolishiga qarshi xavfsizlikni ta’minlaydi);

7. Xavfsizlikni nazorat qilish: Tarmoqda xavfsizlikni nazorat qilish uchun to‘g’ridan-to‘g’ri tarmoqni nazorat qilib borish (xavfsizlikni nazorat qilish strategiyalari va xavfsizlikning yuqori darajadagi sozlamalarini o‘rnatish kerak);

8. Xavfsizlikni sinash va imtihon qilish: Tarmoq xavfsizligini sinash va imtihon qilish uzoq vaqt mobaynida tarmoqni xavfsizlik bo‘shliqlari va tizimlarini aniqlashga yordam beradi.

Oldingi va joriy tarmoq xavfsizligi standartlari tarmoq xavfsizligi, ma’lumotlar himoyasi va xavfsizlikni ta’minlash uchun keng qo‘llaniladigan talablarni belgilaydi. Ushbu standartlar tarmoq infrastrukturasi, tizimlar, ilovalar va ma’lumotlar xavfsizligi bilan bog’liq muhim masalalarni qamrab olib, xavfsizlik tizimlarini va tahlillarini tashkil etishda yordam beradi.

Xulosa. Tarmoq xavfsizligi bugungi kunda muhim bo‘limlardan biri hisoblanib, standartlar va tavsiyalar orqali ta’minlanishi ma’lum bo‘ldi. Bu standartlar va tavsiyalar tarmoq xavfsizligini ta’minlash, zararli faoliyatlar va tuzatishlardan himoya qilishga yordam berish uchun kerakli qadam va maslahatlarni taqdim etadi. Aynan tarmoq xavfsizligi standartlarining oldingi va joriylarini bir-birlaridan farqlarini o‘rganib, hozirgi standart tarmoqlar ancha yaxshilanganini birgalikda ko‘rdik va ularning qo‘llanilishi tizimda xavfsizlikni oshirishda muhim ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR

1. Koblits. N. Kurs teorii chisel i kriptografii - M., Nauchnoe izdatelstvo TVP, 2001 g., 260 ctr. (perevod s angliyskogo).

2. Gerasimenko V.A. Zaщita informatsii v avtomatizirovannыx sistemax obrabotki dannыx kn. 1.-M.: Energoatomizdat. -1994.-400s.

3. Miller V. Ispolzovaniya ellipticheskix krivыx v kriptografii .: -1986.-417-426s.

4. O‘z DSt 1109:2006 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Atamalar va ta’riflar».
5. Stamp Mark. Information security: principles and practice. USA, 2011.

Internet resurslari

6. http://www.google.com
7. http://www.it-ebooks.info
8. www.poe.com