Засоби захисту мереж

Безпека мережі (Network security) — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів.

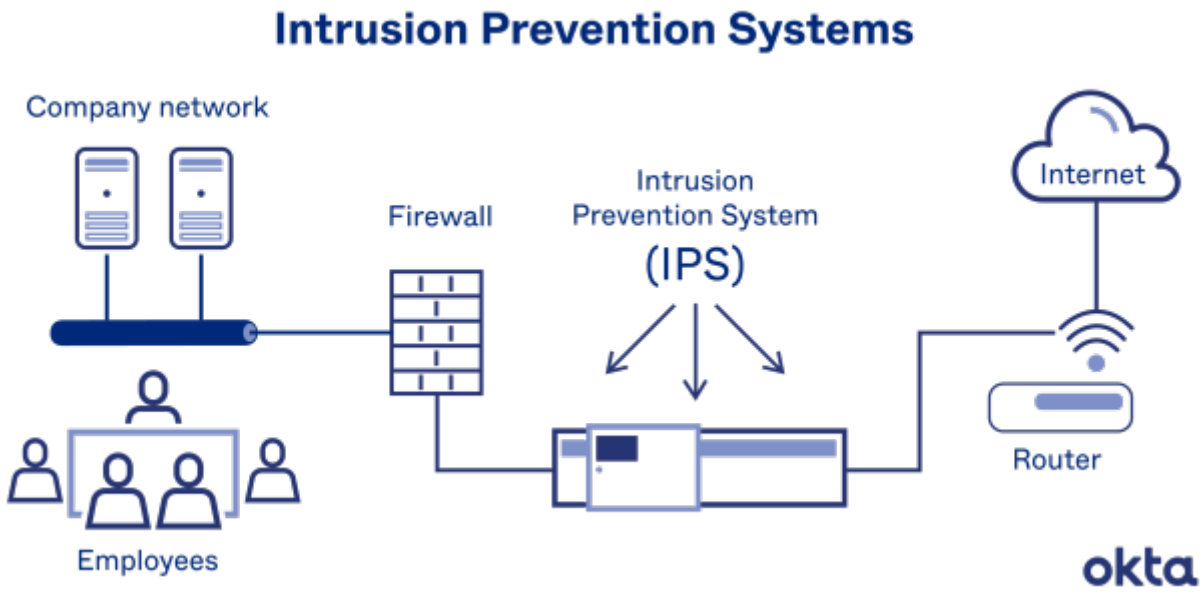
Безпека мережі є одним із важливих аспектів кібербезпеки, організації та уряди повинні використовувати потужні інструменти та методи кібербезпеки для пом’якшення сучасних загроз. У цій статті ми напишемо про деякі інструменти, які допоможуть захистити різні мережі.

Засоби захисту мережі – це програмне та апаратне забезпечення, яке використовується для захисту комп’ютерних мереж від несанкціонованого доступу, використання, розкриття, порушення цілісності, руйнування або перешкоджання роботі.

Концепції мережевої безпеки

Мережева безпека починається з аутентифікації, що зазвичай включає в себе ім'я користувача і пароль. Коли для цього потрібно тільки одна деталь аутентифікації (ім'я користувача), то це називають однофакторною аутентифікацією. При двофакторній аутентифікації, користувач ще повинен використати маркер безпеки або 'ключ', кредитну картку або мобільний телефон, при трьохфакторній аутентифікації, користувач повинен застосувати відбитки пальців або пройти сканування сітківки ока.

Після перевірки дійсності, брандмауер (firewall) забезпечує доступ до послуг користувачам мережі. Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень (Instrusion Prevention System (IPS)).



Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб

зберегти конфіденційність.

Як працює система безпеки

Система безпеки мережі не ґрунтується на одному методі, а використовує комплекс засобів захисту. Навіть якщо частина обладнання виходить з ладу, решта продовжує захищати дані Вашої компанії від можливих атак.

Встановлення рівнів безпеки мережі надає Вам можливість доступу до цінної ділової інформації з будь-якого місця, де є доступ до мережі Інтернет, а також захищає її від загроз. Система безпеки мережі:

- Захищає від внутрішніх та зовнішніх мережних атак. Небезпека, що загрожує підприємству, може мати як внутрішнє, так і зовнішнє походження. Ефективна система безпеки стежить за активністю в мережі, сигналізує про аномалії та реагує відповідним чином.
- Забезпечує конфіденційність обміну інформацією з будь-якого місця та в будь-який час. Працівники можуть увійти до мережі, працюючи вдома або в дорозі, та бути впевненими у захисті передачі інформації.
- Контролює доступ до інформації, ідентифікуючи користувачів та їхні системи. Ви маєте можливість встановлювати власні правила доступу до даних. Доступ може надаватися залежно від ідентифікаційної інформації користувача, робочих функцій, а також за іншими важливими критеріями.
- Забезпечує надійність системи. Технології безпеки дозволяють системі запобігти як вже відомим атакам, так і новим небезпечним вторгненням. Працівники, замовники та ділові партнери можуть бути впевненими у надійному захисті їхньої інформації.

Категорії інструментів мережевої безпеки

Брандмауер (firewall) — це пристрій безпеки мережі (може бути програмним або апаратним), який діє як ворота між мережею та іншими мережами. Він відстежує та фільтрує вхідний і вихідний трафік та виявляє різні атаки, наприклад сканування вразливостей.

Зворотний брандмауер — це тип брандмауера, який розміщується поза мережею або пристроєм і також діє як ворота між джерелом і одержувачем, його основна мета — відстежувати та очищати вихідний трафік, запобігаючи витоку важливої інформації.

IPS (система запобігання вторгненням) — це тип інструменту безпеки мережі, який постійно відстежує трафік і може вживати заходів у разі виявлення зловмисного трафіку (повідомлення, видалення тощо). Інформація про безпеку та керування подіями (SIEM)

SIEM (Security information and event management) — у комп'ютерній безпеці є програмними продуктами, які об'єднують управління інформаційною безпекою SIM (англ. Security information management) та управління подіями безпеки SEM (англ. Security event management). Технологія SIEM забезпечує аналіз в реальному часі подій (тривог) безпеки,

отриманих від мережевих пристроїв і додатків. SIEM представлено додатками, приладами або послугами, і використовується також для журналювання даних і генерації звітів в цілях сумісності з іншими бізнес-даними.

Віртуальна приватна мережа (VPN) — це спосіб встановити безпечне з’єднання між мережевими пристроями, оскільки трафік усередині VPN зашифровано та захищено від Інтернету.

EDR (Endpoint Detection and Response) - це система, яка використовується для виявлення та реагування на кібератаки на кінцевих точках. EDR відстежує пристрої на наявність ознак атак, таких як підозріла активність, несанкціоновані зміни файлів та несанкціонований доступ до даних.

> **Захист кінцевих точок** - це сукупність заходів, спрямованих на захист пристроїв, таких як комп'ютери, смартфони та планшети, від кіберзагроз. Це важлива частина кібербезпеки, адже кінцеві точки часто є першою лінією оборони від атак.

Захист у мережах Wi-Fi

Вайфай (від англ. Wireless Fidelity, Wi-Fi, WiFi) — торгова марка Wi-Fi Alliance та загальновживана назва для стандарту IEEE 802.11 передавання цифрових потоків даних по радіоканалах.

Назва покоління	Стандарт IEEE	Рік	Максимальна швидкість з'єднання (Мбіт/с)	Смуги радіочастот (ГГц)
Wi-Fi 7	802.11be	(2024)	≤ 46120	2.4 / 5 / 6
Wi-Fi 6E	802.11ax	2020	≤ 9608	6
Wi-Fi 6	802.11ax	2019	≤ 9608	2.4 / 5
Wi-Fi 5	802.11ac	2014	≤ 6933	5
Wi-Fi 4	802.11n	2008	≤ 600	2.4 / 5
(Wi-Fi 3)*	802.11g	2003	≤ 54	2.4
(Wi-Fi 2)*	802.11a	1999	≤ 54	5
(Wi-Fi 1)*	802.11b	1999	≤ 11	2.4
(Wi-Fi 0)*	802.11	1997	≤ 2	2.4
* Назви Wi-Fi 0, 1, 2, 3 є широковживаними, однак неофіційн				

Ключові аспекти захисту мережі Wi-Fi

Пароль

- **Використовуйте сильний пароль:** ваш пароль Wi-Fi має бути довгим (мінімум 12 символів) і містити суміш літер, цифр та символів. Уникайте використання особистої інформації, такої як імена, дати народження або адреси.
- **Не діліться своїм паролем:** тримайте свій пароль Wi-Fi в секреті та не діліться ним ні з

ким, навіть із сусідами чи друзями.
- **Змініть пароль за замовчуванням:** Багато маршрутизаторів мають паролі за замовчуванням, які легко вгадати. Обов'язково змініть пароль за замовчуванням на власний, сильний пароль.

Шифрування

- **Використовуйте протокол шифрування WPA2 або WPA3:** ці протоколи шифрують трафік у вашій мережі Wi-Fi, що ускладнює перехоплення даних зловмисниками. Старі протоколи, такі як WEP, є вразливими та їх слід уникати.
- **Вимкніть WPS (Wi-Fi Protected Setup):** WPS - це зручний спосіб підключення пристроїв до мережі Wi-Fi, але він має вразливість, яку можуть використовувати зловмисники. Якщо можливо, вимкніть WPS на своєму маршрутизаторі.

Гостьова мережа

Налаштуйте гостьову мережу: Якщо потрібно дозволити гостям отримати доступ до вашого Інтернету, налаштуйте гостьову мережу із окремим паролем. Таким чином, ваші особисті пристрої та дані будуть захищені від гостей.

Також можна увімкніть MAC-фільтрацію: MAC-фільтрація дозволяє вам надати доступ до вашої мережі Wi-Fi лише для пристроїв з певними MAC-адресами.

Джерела

- Безпека мережі
- All What you Need to Know about Network Security Tools
- SIEM
- Wi-Fi