Безпека бездротових мереж

Безпека мережі

Безпе́ка мере́жі — заходи, які захищають інформаційну мережу від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу.

Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів.

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 забезпечує доступ до послуг користувачам мережі. Для виявлення і пригнічування дії шкідливих програм використовується антивірусне програмне забезпечення або системи запобігання вторгнень (IPS).

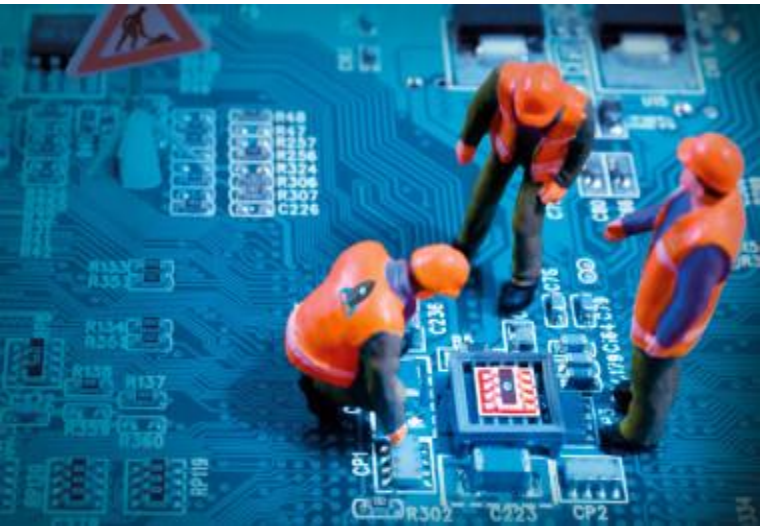
Зв'язок між двома комп'ютерами з використанням мережі може бути зашифрований, щоб зберегти конфіденційність.

РОБОТА СИСТЕМИ БЕЗПЕКИ

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.

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.

ЗАХИСТ В WI-FI МЕРЕЖАХ

Існує два основних варіанти пристрою бездротової мережі:

-**Ad-hoc** - передача безпосередньо між пристроями;
-**Hot-spot** - передача здійснюється через точку доступу;

В **Hot-spot** мережах присутня точка доступу, за допомогою якої відбувається не тільки взаємодія всередині мережі, але і доступ до зовнішніх мереж. **Hot-spot** представляє найбільший інтерес з точки зору захисту інформації, бо зламавши точку доступу, зловмисник може отримати інформацію не тільки зі станцій, розміщених в даній бездротовій мережі.

МЕТОДИ АУТЕНТИФІКАЦІЇ

Аутентифікація - видача певних прав доступу абоненту на основі наявного в нього ідентифікатора

-**IEEE 802.11** передбачає два методи аутентифікації:

-Відкрита аутентифікація;
-Аутентифікація із загальним ключем (англ. **Shared Key Authentication**)

WPA також використовує два способи аутентифікації:

Аутентифікація за допомогою передвстановленого ключа **WPA-PSK;**
Аутентифікація за допомогою **RADIUS**-сервера

РЕЖИМ ПРИХОВАНОГО SSID

Для свого виявлення точка доступу періодично розсилає кадри-маячки (англ. **beacon frames**). Кожен такий кадр містить службову інформацію для підключення і, зокрема, присутній **SSID** (ідентифікатор бездротової мережі). У разі прихованого **SSID** це поле порожнє, тобто неможливо виявлення вашої бездротової мережі і не можна до неї підключитися, не знаючи значення **SSID**. Але всі станції в мережі, підключені до точки доступу, знають **SSID** і при підключенні, коли розсилають **Probe Request** запити, вказують ідентифікатори мереж, наявні в їх профілях підключень. Прослуховуючи робочий трафік, з легкістю можна отримати значення **SSID**, необхідне для підключення до бажаної точки доступу.Режим прихованого **SSID**Микола Скрипський. Комп'ютерні мережі. **ceo@mgm.cv.ua**

СПЕЦИФІЧНІ МЕХАНІЗМИ БЕЗПЕКИ

Реалізувати сервіси безпеки можна, впровадивши на певному рівні моделі OSI такі механізми:

шифрування

цифровий підпис

керування доступом

контроль цілісності даних

автентифікаційний обмін

заповнення трафіку

керування маршрутом

нотаризація

ПЗ для безпеки в КМ

Secure Shell, SSH (англ. **Secure SHell** — «безпечна оболонка») — мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і тунелювання **TCP**-з'єднань (наприклад, для передачі файлів)

ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ ЩОДО ЗАХИСТУ МЕРЕЖІ

Використовуйте антивірусне ПЗ

Намагайтеся використовувати ПЗ тільки з джерел яким ви дійсно довіряєте

Використовуйте відкрите програмне забезпечення

Не використовуйте додатки, які визначають Ваше місце положення

Не переходіть на веб-ресурси, що здаються Вам підозрілими

Намагайтеся охороняти свою приватність

Дякую за увагу!