10 поширених типів кібератак

Фішинг

Це підвид соціальної інженерії. Метод базується на спонуканні жертви перейти за посиланням на підроблений сайт, та скомпрометувати свої дані або завантажити шкідливе ПЗ.

Методи захисту

Навчайтеся відрізняти фальшиві сайти від справжніх. Захищайте доступи двофакторною автентифікацією. Використовуйте апаратні ключі безпеки.

DoS і DDoS-атаки

Цей вид атак спрямований на перевантаження ресурсу на сервері. Їх важко відстежити, в атаках беруть участь тисячі, або навіть мільйони скомпроментованих пристроїв. Ціль атак — знизити пропускну спроможність трафіку, тобто перекрити доступ відвідувачам до ваших сайтів.

Методи захисту

Проводьте тестування на DoS і DDoS-атаки за допомогою фахівців з ціллю викрити та захистити слабкі місця системи. Використовуйте надійні хмарні сховища з можливістю оперативно збільшити обсяг дискового простору.

Крадіжка Cookie

Тактика викрадення даних користувача через незахищені дані сеансу, коли зловмисник видає свій пристрій за ваш. Зазвичай атака відбувається в незахищених загальнодоступних Wi-Fi.

Методи захисту

Тактика викрадення даних користувача через незахищені дані сеансу, коли зловмисник видає свій пристрій за ваш. Зазвичай атака відбувається в незахищених загальнодоступних Wi-Fi.

SQL ін’єкції

Найстаріша та найнебезпечніша атака, яка передбачає використання вразливостей форм вводу на сайтах та введення шкідливого коду для проникнення і маніпулювання базою даних. Таким чином зловмисники можуть отримати доступ до комерційної таємниці компанії або знищити дані.

Методи захисту

Проводьте періодичне тестування на уразливості програм чи сайтів, користуючись послугами фахівців з безпеки. Виконуйте всі рекомендації професіоналів.

Атаки Brute Force

Це найпростіший метод зламу, що полягає у підборі паролів або контрольних сум. Для цього використовуються програми, які перебирають розповсюджені паролі, фрази та всі слова підряд зі словників.

Методи захисту

Створюйте складні паролі.
Підключайте двофакторну автентифікацію.
Використовуйте апаратні ключі безпеки.

Троянські програми

Назва натякає на міфічного Троянського коня, коли у подарунок заховали вражі війська. Зловмисники теж ховають шкідливі програми, які шпигують за користувачем, у безоплатне програмне забезпечення та файли.

Методи захисту

Вмикайте антивірус. Перевіряйте всі скачані файли. Використовуйте ліцензійні програми та завантажуйте фото на відповідних сервісах, бо будь-яка красива безоплатна картинка може містити вірус.

ClickJacking

Зловмисники змушують натиснути кнопку, якої користувачі не бачать, бо вона прозора. Таким чином вони можуть отримати конфіденційні дані чи змусити завантажити зловмисне ПО.

Методи захисту

Перевіряйте сайт на вбудований вміст. Використовуйте браузери, які підтримують технологію X-Frame-Options: SAMEORIGIN, наприклад, Google Chrome. Захищайте акаунти двофакторною автентифікацією.

Кейлогери

Це програмне забезпечення (або, рідше, апаратні пристрої), що записує кожну активність користувача: натискання клавіш або роботу мишкою. Воно використовується для крадіжки конфіденційних даних, паролів, PIN-кодів тощо. Завантаження шкідливого ПО можливе через фішингові листи чи троянські програми.

Методи захисту

Тримайте антивірус та брандмауер увімкненим. Уникайте завантаження файлів з незнайомих джерел. Перевіряйте програмне забезпечення та видаляйте підозріле. Увімкніть 2ФА. Користуйтеся менеджерами паролів, щоб не вводити їх вручну. Використовуйте ключі безпеки.

Майже від усіх атак, спрямованих на проникнення та крадіжку паролів, у 100% випадків допомагають апаратні ключі безпеки YubiKey!

DNS Spoofing

Хакери вводять неправдиві дані у кеш сервера, який має вразливості. Далі «отруєний» сервер повертає невірний IP та передає дані на інший комп’ютер. Таким чином зловмисник отримує конфіденційні дані.

Методи захисту

Використовуйте Secure DNS (DNSSEC) — набір розширень, основаних на криптографічних цифрових підписах, що допомагають протистояти атакам і знижують ризик «отруєння» сервера.

Watering Hole

Технологія зараження популярних сервісів з ціллю скомпрометувати дані їхніх відвідувачів. Зазвичай користувачі довіряють таким сервісам більше ніж іншим, тож можуть завантажити з них шкідливе ПЗ.

Методи захисту

Залишайтеся пильним на будь-яких сайтах. Перевіряйте всі файли, які треба завантажувати. Перевіряйте всі підключені додатки. Використовуйте надійні та оновлені антивірусні програми. Захищайте вхід до облікових записів за допомогою MFA та ключів безпеки.

>the_kernel