СП «Інфоком»
вул. Володимирська, 8
Київ, 01001, Україна
тел.: +380 (44) 230 52 00
infocom@infocom.ua
infocom.ua

infoScan

Незалежний аудит захищеності інформаційної інфраструктури

infocom.ua

2024

infoScan

web-сторінка послуги

НЕЗАЛЕЖНИЙ АУДИТ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

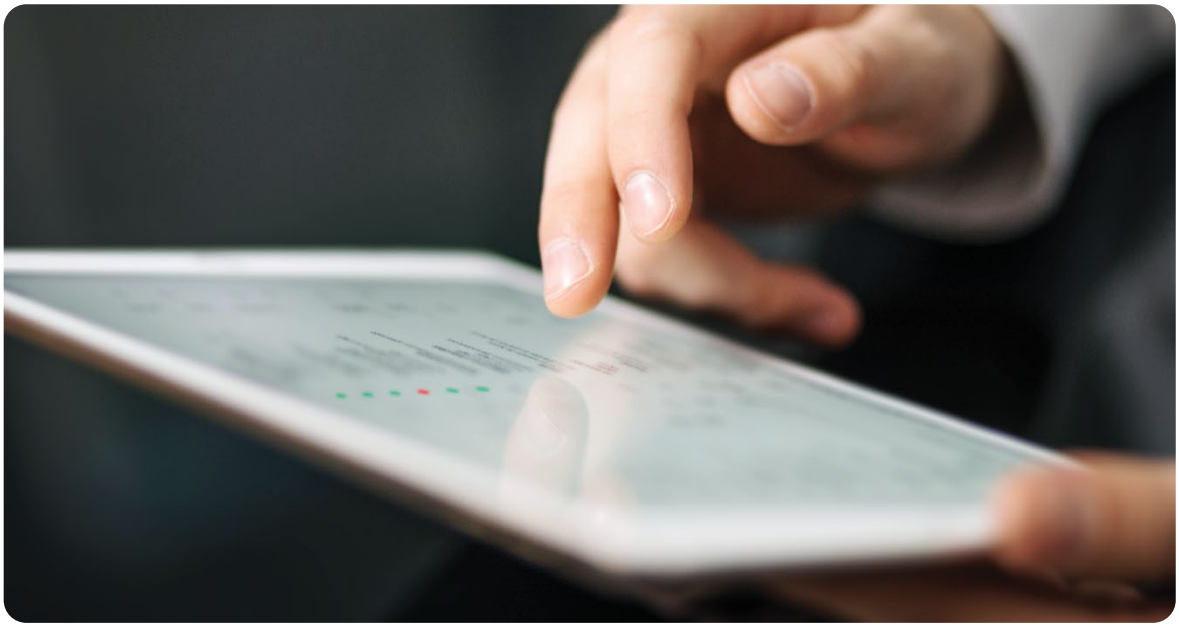
Аудит захищеності інформаційної інфраструктури - комплекс заходів спрямований на пошук будь-яких вразливостей та потенційних загроз, які можуть призвести до несанкціонованого проникнення сторонніх осіб у вашу мережу. Періодичне проведення аудиту є важливим для забезпечення ефективності заходів безпеки та виявлення нових загроз, які можуть виникнути внаслідок змін у вашій інформаційній інфраструктурі та застосованих технологіях.

Наявність вразливостей у вашій мережі дає можливість зловмисникам реалізовувати загрози і таким чином отримувати доступ до конфіденційних даних, завдавати шкоди поточним робочім процесам або зупиняти їх повністю. Своєчасне виявлення таких вразливостей та їх відповідне усунення є критично важливими для забезпечення безпеки інформаційної інфраструктури.

Інформаційна інфраструктура може бути вразлива з багатьох причин. Серед основних видів вразливостей, які можуть існувати в інформаційних системах слід виділити наступні:

- Вразливості програмного забезпечення: помилки в програмному забезпеченні або застаріле програмне забезпечення, яке може бути використано зловмисниками
- Вразливості мережі: слабкі місця в мережі, обумовлені неправильною конфігурацією мережного обладнання, недостатнім рівнем захисту від зовнішніх атак або недостатня захищеність пристроїв, які підключені до мережі
- Вразливості управління доступом: використання слабких паролів, втрата або крадіжка пристроїв, проблеми управління правами доступу тощо
- Вразливості фізичної інфраструктури: недостатній рівень захисту приміщень, де зберігаються сервери та інші пристрої, які містять конфіденційну інформацію.

Якщо вразливості пов'язані з фізичною інфраструктурою та управлінням доступом великою мірою є питаннями адміністративними та організаційними, які можуть бути, здебільшого, вирішені компаніями чи організаціями власними силами, то вразливості програмного забезпечення та мережеві вразливості є суто технічними та потребують аналізу спеціалістів з кібербезпеки.



infocom
TRUSTED SECURITY

Перші чотири етапи аудиту захищеності інформаційної інфраструктури включають збір інформації та аналіз наявних ризиків. Така робота передбачає тісну співпрацю між представниками Infocom та компанією чи організацією яка проходить аудит. Під час цих етапів визначаються потенційні загрози, проводиться оцінка ймовірності та наслідків їх реалізації, а також визначення пріоритетів захисних заходів. Також до уваги беруться такі фактори як потенційне джерело загроз (із середини периметру або ззовні), можливі методу впливу (мережні, апаратні або соціальні) та об'єкти загрози (корпоративні дані, робочі процеси тощо).

Етапи аудиту інформаційної безпеки

Після визначення усього спектру можливих загроз спеціалістами Infocom проводиться перевірка мережевої інфраструктури (конфігурація обладнання, схема підключення, тощо) та здійснюється «сканування» з використанням спеціалізованого програмного забезпечення. Отримані таким чином дані дозволяють виявляти всі слабкі місця в інформаційній системі, такі як відкриті порти, застарілі версії програмного забезпечення, слабко захищені мережеві протоколи, неправильно налаштоване або підключене обладнання. Після проведення аудиту, представниками Infocom формується звіт, в якому відображаються всі виявлені вразливості та детальні рекомендації щодо їх усунення, а також пропозиції щодо покращення загального рівня безпеки інформаційної інфраструктури. За бажанням компанії чи організації, Infocom може провести додатковий повторний аудит для перевірки рівня імплементації раніше наданих рекомендацій та пропозицій.

Послуга infoScan це:

- Виявлення та усунення наявних вразливостей у вашій інформаційній інфраструктурі
- Зменшення ризиків порушення діяльності компанії через проактивне виявлення загроз
- Поліпшення рівня кіберзахисту без додаткових значних вкладень
- Детальний звіт з рекомендаціями щодо покращення вашої безпеки
- Підтримка та консультації від фахівців

infocom
TRUSTED SECURITY