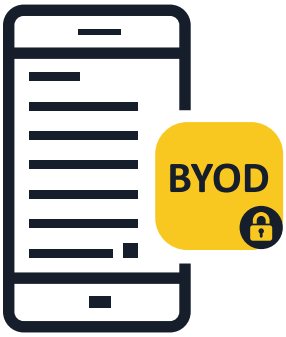
ШКІДЛИВЕ ПЗ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

ПОРАДИ Й РЕКОМЕНДАЦІЇ ДЛЯ ПІДПРИЄМСТВ

1 Інформуйте свій персонал щодо ризиків мобільних пристроїв

- Експлуатація мобільних пристроїв розмиває межу між корпоративним та особистим використанням. Підприємства можуть серйозно постраждати від атаки, первісно спрямованої на особистий мобільний пристрій. Мобільний пристрій — це комп'ютер, тому захищати його потрібно як комп'ютер.



2 Впровадження корпоративної політики для використання власних пристроїв (BYOD)

- Працівники, які використовують свої мобільні пристрої для доступу до інформації та систем підприємства (навіть якщо це тільки електронна пошта, календар чи бази даних контактів), повинні дотримуватися політики компанії. Ретельно обирайте технічні рішення для керування мобільними пристроями та їх захисту, а також для заохочування вашого персоналу до обачності.

3 Зробіть політику безпеки щодо мобільних пристроїв частиною вашої загальної системи безпеки

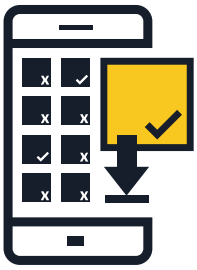
- Якщо пристрій не відповідає політиці безпеки, він не повинен отримувати дозвіл на підключення до корпоративної мережі і доступ до корпоративних даних. Компанії мають впроваджувати власні рішення для управління мобільними пристроями (Mobile Device Management, MDM) або управляння корпоративними мобільними рішеннями (Enterprise Mobility Management, EMM).
- На додачу, критично важливо встановити рішення для захисту від мобільних загроз. Це забезпечить підвищену видимість та розуміння рівня загроз для застосунків, мережі та операційної системи.

4 Остерігайтесь використовувати для доступу до корпоративних даних загальнодоступні мережі Wi-Fi

- Загалом, загальнодоступні мережі Wi-Fi не є безпечними. Якщо працівник здійснює доступ до корпоративних даних за допомогою безкоштовного підключення Wi-Fi в аеропорту або кав’ярні, ці дані можуть бути доступними і для зловмисників. Компаніям рекомендується в цьому напрямку розробляти політику “раціонального використання”.

5 Регулярно оновлюйте операційні системи та застосунки

- Порадьте своїм працівникам завантажувати оновлення програмного забезпечення для операційної системи їх мобільних пристроїв, щойно такі буде запропоновано. Вивчайте політику операторів мобільного зв'язку й виробників мобільних телефонів щодо оновлень, - особливо це є актуальним для платформи Android. Найсвіжіші оновлення гарантують не тільки вищу безпеку вашого пристрою, але й вищу продуктивність.



6 Встановлюйте застосунки тільки з перевірених джерел

- На тих мобільних пристроях, що підключаються до корпоративної мережі, компанії повинні дозволяти встановлення застосунків тільки з офіційних джерел. Як варіант, розгляньте можливість створення корпоративного магазину застосунків, де кінцеві користувачі матимуть доступ до застосунків, погоджених компанією, зможуть їх завантажувати та встановлювати. Зверніться до свого постачальника рішень безпеки за порадою щодо налаштування або створіть власне рішення.

7 Запобігання повному зняттю обмежень (“джейлбрейку”)

- “Джейлбрейк” — це процес зняття обмежень безпеки, визначених розробником операційної системи, з отриманням повного доступу до операційної системи та функцій. “Джейлбрейк” вашого пристрою може значно послабити його безпеку, розкриваючи прогалини в безпеці, які, можливо, й не були дотепер очевидними. В корпоративному середовищі не слід дозволяти використання пристроїв з розблокованим обліковим записом суперкористувача.

8 Розгляньте варіанти хмарних сховищ даних

- Користувачі мобільних пристроїв часто хочуть отримувати доступ до важливих документів не тільки через свої робочі ПК, а й зі своїх власних телефонів чи планшетів за межами офісу. Компаніям слід оцінити можливість створення безпечного хмарного сховища та служб синхронізації файлів для безпечного задоволення таких потреб.

9 Заохочуйте свій персонал до встановлення застосунків мобільної безпеки

- Будь-які операційні системи вразливі до зараження. Якщо є така можливість, забезпечте, щоб вони використовували рішення для мобільної безпеки, яке виявляє та блокує шкідливе ПЗ, шпигунські програми та шкідливі застосунки, а також містить інші функції конфіденційності та захисту від викрадення.

EUROPOL EC3 European Cybercrime Centre

EMA

#MobileMalware