УДК 004.62+004.77 **А. В. Платоненко**

СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ДЕРЖАВНИХ ТА ПРИВАТНИХ УСТАНОВ УКРАЇНИ

Розглянуто сучасні загрози інформаційної безпеки для державних та приватних установ України. Представлено статистичні дані про збитки від міжнародних компаній, шляхи та методи, які реалізують зловмисники для несанкціонованого отримання даних. Розглянуто програмно-апаратне забезпечення, яке дозволяє керувати можливими загрозами інформаційної безпеки та захистити корпоративну мережу від зловмисних дій, які можуть понести за собою значні збитки.

Ключові слова: інформаційна безпека, загрози інформаціної безпеки, збитки від кіберзлочинів, захист мереж від несанкціонованого доступу.

Вступ

Інформаційна безпека не несе за собою можливості заробітку, оскільки потребує певних витрат, але завдяки цим витратам можливо захистити установи від значних майбутніх збитків. Загрози інформаційної безпеки несуть за собою великі ризики, які можуть обернутись на величезні збитки не тільки для організацій, що не впровадили систему захисту інформації, а і для цілої країни.

В наш час загрози інформаційної безпеки можуть з’являтись дуже часто, адже кожного дня зловмисники знаходять нові вразливості, завдяки яким можуть нанести шкоду як для державних установ, так і для приватних організацій.

Мобільними пристроями щоденно користується мільйони людей, але коли за безпекою своїх особистих даних мало хто слідкує, то у корпоративних мережах важливим фактором є збереження інформації, що в ній передається. Нажаль шахраї знову й знову знаходять нові можливості для звершення несанкціонованого доступу до інформації (в компанії «Palo Alto Networks» щоденно звітують про знаходження більше 25 тисяч нових зловмисних програм для мобільних пристроїв).

Основна частина

Таким чином постає питання захисту мобільних пристроїв, які можуть використовуватись за межами офісу компанії та створювати нові загрози витоку інформації. Завдяки спеціальним технічним рішенням, які стають частиною корпоративної мережі та програмному забезпеченню на пристроях користувачів з’являється змога запобігти небажаним втратам важливої інформації.

На рис. 1 зображена структурна схема захищеної корпоративної мереж із використанням мобільних пристроїв. Інформація з мережі Інтернет та корпоративної мережі передається через мережевий екран, до якого підключений прилад управління мобільними пристроями, який в свою чергу керує мобільними підключеннями до мережі та має доступ до хмарного сервісу, за допомогою якого можна отримати захист від вірусів «нульового дня».

Завдяки такому приладу управління можна отримати: статистику загроз, засоби захисту від зловмисного коду в програмах для мобільних пристроїв, створення та управління правилами безпеки для мобільних пристроїв у мережі.

Для ефективного захисту мобільних пристроїв замало тільки встановленого на них програмного забезпечення. Важливими є правила роботи в мережі, перелік дозволених програм та формату файлів, що в них можна використовувати, адже дуже велика кількість зловмисних програм приховується за розповсюдженими форматами документів (зокрема *.pdf). Саме тому краще віддавати перевагу хмарним сервісам, які оцінюють поведінку файлів та допомагають швидше визначити загрозу, ніж після оновлення бази сигнатур антивірусу.

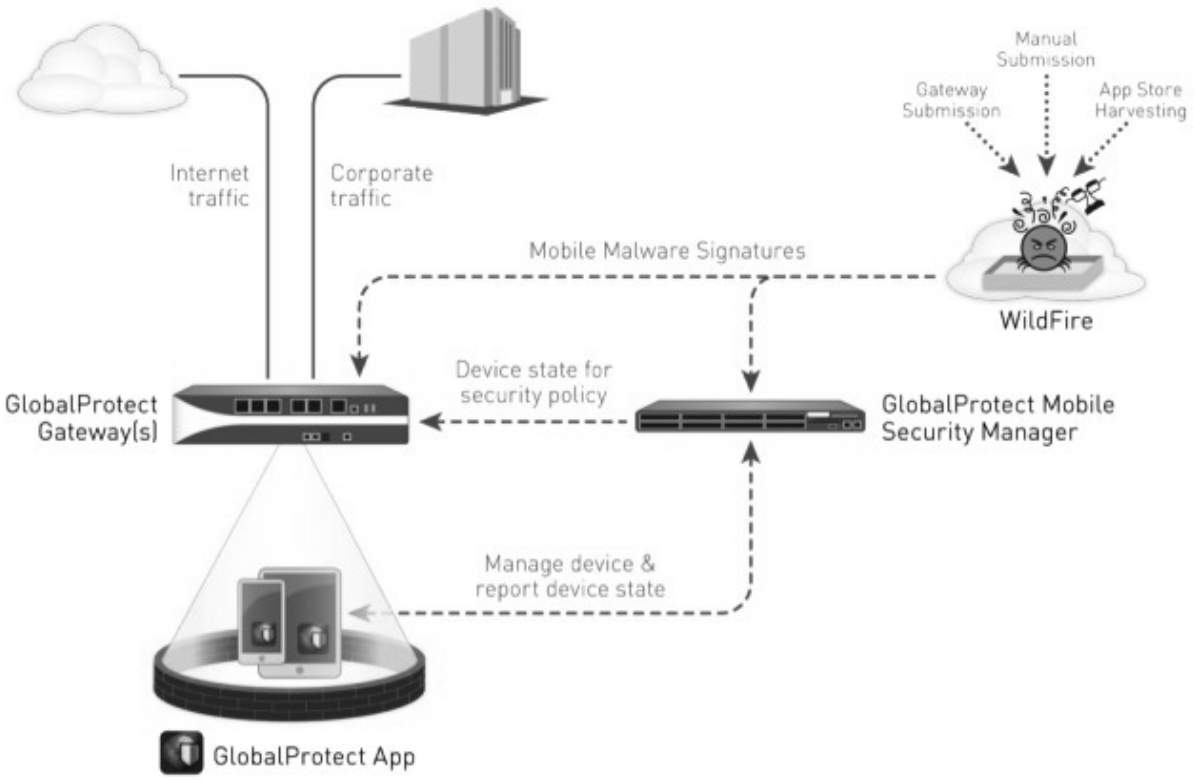

Рис. 1. Структурна схема захищеної корпоративної мережі з використанням мобільних пристроїв

Окрім цього, ніколи не потрібно забувати про людей, які користуються мобільними пристроями, адже саме вони через неуважність можуть випадково встановити зловмисну програму, що заблокує їх пристрій та буде вимагати кошти за розшифрування інформації, або ще гірше, розповсюдиться на весь список контактів. Наприклад відома атака в кінці 2014 року «Привіт! Тобі фото…», що заразила мільйони мобільних телефонів українців, залишаючи їх без грошей на рахунку та змоги навіть отримати повідомлення чи прийняти дзвінок, на декілька місяців стала проблемою для мобільних операторів і вповноважених фахівців спецслужб.

Нажаль, Україна зайняла 5 місце у світовому рейтингу з ризику зіткнення з веб-загрозами. За третій квартал 2015 року третина (33,7%) користувачів антивірусних продуктів зіткнулась із загрозами, які розповсюджується через мережу Інтернет. Проблемою є відсутність оновлення програмного забезпечення та використання піратських програм. Біля 17% заражень було здійснено на користувачів застарілої WindowsXP. Також небезпечними є шифрувальні програми, що вимагають гроші після шифрування файлів, доступ до яких не можливий без спеціального ключа.

Великою проблемою є соціальна інженерія. Зловмисники завдяки соціальним мережам, фішинговим та зловмисним сайтам розповсюджують свої програми. Таким чином може постраждати не тільки користувач особисто, а і компанія, працівником якої він є. Нажаль ця проблема стала дуже розповсюдженою ще і завдяки використанню USB-накопичувачів, на яких встановлено зловмисне програмне забезпечення. Зловмисники залишають їх у місцях, де працівники проводять вільний час. Після підключення знайдених носіїв інформації до комп'ютерів, злочинці вже можуть віддалено отримати доступ і нанести шкоду для організації.

За статистичною інформацією компанії «Microsoft»:

- 243 дні атакуючий знаходиться в мережі компанії, до того як його буде виявлено;
- 76% вдалих атак на мережу здійснюється через зламані облікові записи користувачів;
- 500 млрд. $ становить матеріальний збиток від кіберзлочинництва в світі;
- 3,5 млн. $ становить середній збиток від злому для компанії.

Лише за 8 місяців 2015 року правоохоронними органами України вже було зафіксовано понад 20 тис. незаконних операцій з платіжними картками фізичних осіб, які спричинили збитки на суму близько 500 млн. грн. Це лише ті факти, які вдалося зафіксувати і встановити.В окремих випадках заяви від банків до МВС не надходять. Банківські працівники намагаються своїми силами встановити зловмисників. Для отримання інформації про банківські рахунки злочинці йдуть на дуже дорогі і витратні заходи. Вони наймають фахівців, розробляють спеціальні програми для викрадення баз даних з комерційних структур, які накопичують таку інформацію. Саме тому за останні два роки вдвічі більше фахівців різних компаній першочергову увагу приділяють питанню інформаційної безпеки.

Розповсюдженою проблемою залишаються безпроводові мережі, якими щоденно користуються мільйони людей. Частою помилкою користувачів є довіра до відкритих мереж, тобто мереж які не використовують пароль для підключення до неї, а отже й не дають змогу шифрування інформації, що передається. Для захисту інформації, яка передається безпроводовими мережами можна виділити такий перелік рекомендацій:

- зміна параметрів доступу адміністратора до налаштувань;
- обмеження доступу з фільтрації MAC-адрес (англ. Media Access Control);
- режим прихованого ідентифікатора SSID (англ. Service Set IDentifier);
- використання стандарту WPA2, 801.11i (WI - FI Protected Access2);
- відключення стандарту WPS (англ. Wi-Fi Protected Setup);
- створення віртуальних персональних мереж (VPN).

Нажаль, зловмисники завдяки спеціалізованому програмному забезпеченню, досить легко зможуть підмінити MAC-адресу, визначити прихований ідентифікатор, а також підібрати PIN-код підключення до точки безпроводного доступу, але підібрати пароль стандарту WPA2, який може досягати до 64 символів, буде досить тяжко, якщо він не сформований зі звичних слів, що є у базі словників з паролями, які часто використовуються. Ще більш надійним є варіант використання спеціалізованих серверів авторизації, які періодично генерують нові паролі, а також віртуальних персональних мереж, які додатково будуть шифрувати інформацію, що передається через загальну мережу.

Один із варіантів атаки на безпроводову мережу реалізували співробітники компанії iTrust, дослідницького центру по кібербезпеці при Сінгапурському університеті технологій і дизайну (SUTD).Вони придумали досить оригінальний спосіб перехоплення сигналів безпроводового принтера за допомогою закріпленого смартфону на безпілотному літаючому засобі. На рис. 2 зображена структурна схема даної атаки.

Спочатку система розроблялася для підприємств як недорогий спосіб перевірки безпеки Wi-Fi мереж, але в процесі роботи над проектом дослідники виявили, що їх розробка може також використовуватися в зловмисних цілях.Потенційними жертвами системи є безпроводові принтери, які зазвичай являються найслабшою ланкою в безпровідній мережі компанії. Як правило, вони поставляються з відкритим Wi-Fi з'єднанням і багато компаній просто забувають змінити налаштування при підключенні пристрою до мережі.Це відкрите з'єднання потенційно може бути використане сторонніми в якості точки доступу для підключення до мережі та крадіжки важливої інформації.

Розроблена дослідниками система сканує незахищені безпроводові принтери і попереджає користувача у разі виявлення вразливого пристрою. Також можливо виконувати аналогічну операцію, але не зупинятись на виявленні пристрою, а проникнути у безпроводову мережу.Для цього створюється підробна точка доступу, яка видає себе за безпроводовий принтер. У разі успішного втілення зловісного плану в реальність можна вільно перехоплювати усі документи, що відправляються співробітниками компанії на друк, і за декілька секунд перенаправити їх в хмарне середовище, використовуючи підключення мобільного телефону.

В даному випадку існують певні особливості та труднощі, наприклад безпілотний літаючий засіб із смартфоном повинен знаходитися в радіусі 25 метрів від мережі. Тобто, використовуючи подібний метод існує великий ризик викриття. Але даний вид атаки є досить цікавим та заслуговує на увагу, враховуючи стрімкий розвиток використання безпілотних літаючих засобів по всьому світу.

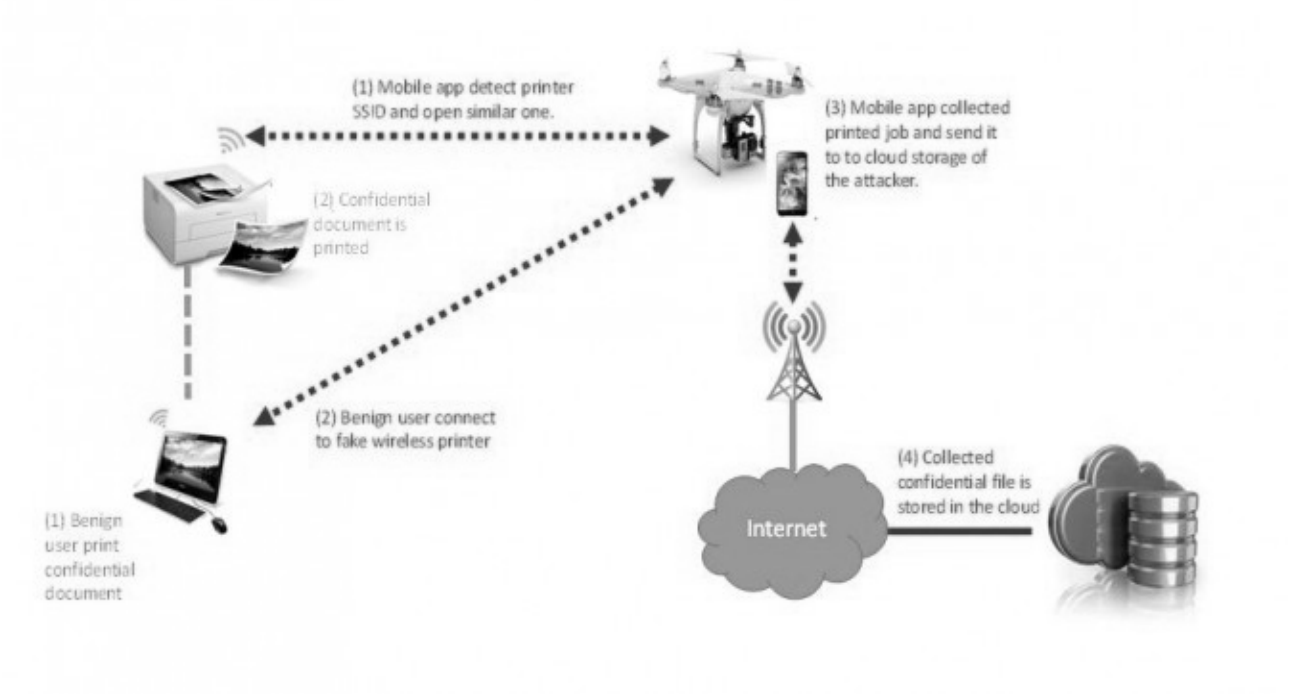

Рис. 2. Структурна схема злому безпроводових принтерів з використанням мобільного телефону, що закріплений на безпілотному літаючому засобі

Висновки

Оскільки велика кількість компаній дозволяє використовувати мобільні пристрої для віддаленої роботи, а завдяки соціальним мережам спілкуються зі своїми клієнтами, то необхідно забезпечити певний рівень захисту користувачів від можливих загроз. Якщо раніше просто блокувались певні сайти, щоб працівники не відволікались від роботи, то зараз їх використання є необхідністю.Таким чином, одним із варіантів вирішення даної проблеми є NGFW (NextGenerationFirewall – мережеві екрани нового покоління, структурна схема показана на рис. 3), завдяки яким можливо обмежити трафік по категоріям та відслідковувати поведінку користувачів, надати доступ необхідним пристроям до певних сайтів, файлів, програм та оцінити можливі ризики від них. Використовуючи таке програмно-апаратне забезпеченнє є можливість захистити корпоративну мережу від зловмисних дій, які могли б понести за собою значні збитки.

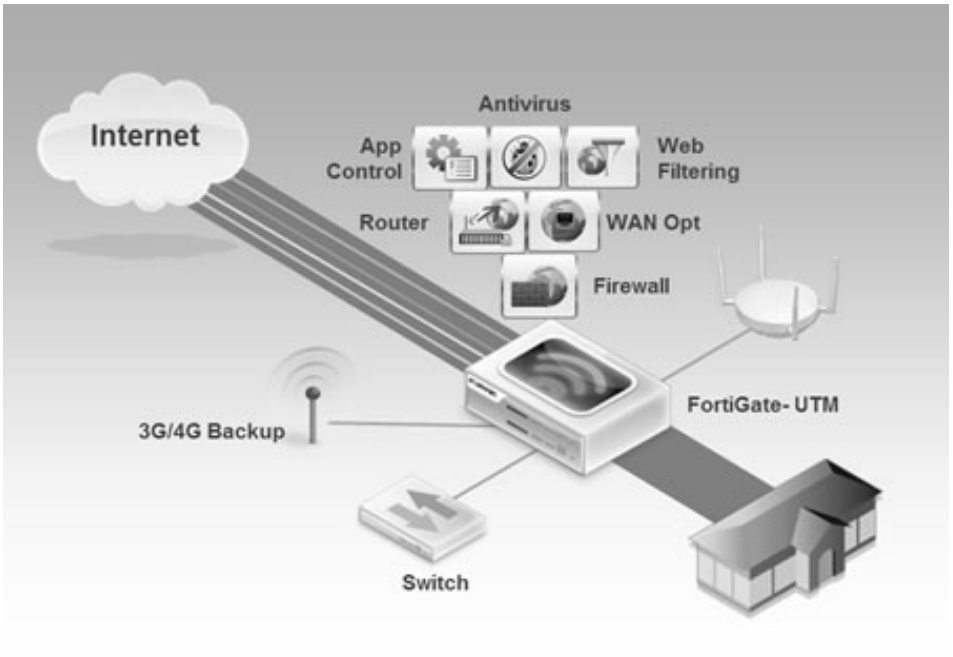

Рис. 3. Структурна схема NGFW (NextGenerationFirewall)

Проведення тестів на проникнення, оновлення програмного та апаратного забезпечення є важливим питанням. Але необхідно проводити періодичне навчання працівників компанії та фахівців з інформаційної безпеки, адже не дивлячись на розвиток технологій, саме людина лишається найвразливішою ланкою в інформаційній безпеці.

Література

1. Міжнародний стандарт ISO/IEC 27001:2013 - Information security management.
2. Матеріали конференції «FORTINET SECURITY DAY 2015». Україна, Київ, 15.04.2015.
3. Матеріали конференції «DATACENTERS & SECURITY DAY 2015». Україна, Київ, 21.10.2015.
4. Вебінар на тему: «Огляд засобів інформаційної безпеки для мобільних пристроїв» компанії «PaloAltoNetworks» (25.03.2015).
5. За 8 місяців МВС викрито понад 20 тис. незаконних операцій з платіжними картками на суму близько 500 млн.грн. [Електронний ресурс] – Режим доступу: http://www.mvs.gov.ua/mvs/control/main/uk/publish/article/1628496 (30.10.2014).
6. 33,7% украинских пользователей сталкиваются с угрозами через интернет. [Електронний ресурс] – Режим доступу: http://itc.ua/news/tret-ukrainskih-polzovateley-stalkivayutsya-s-ugrozami-rasprostranyaemyimi-cherez-internet/ (30.10.2014).
7. Hacking wireless printers with phones on drones. [Електронний ресурс] – Режим доступу: http://www.wired.com/2015/10/drones-robot-vacuums-can-spy-office-printer/ (30.10.2014).

Надійшла 20.11.2015 р. Рецензент: д.т.н., проф. Розорінов Г. М.