УДК 004.056.53

Роман Русланович Орлов,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

Юрій Миколайович Онищенко,
кандидат наук з державного управління, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ

Web-сервери: безпека використання та застосування

На сьогодні уразливості в Web-застосуваннях, як і раніше, залишається одним з найбільш поширених недоліків забезпечення захисту інформації. Загроз занадто багато, і потрібно щось закласти в основу ієрархії захисту. Інтернет вже давно не просто мережа html-сторінок. Це складні додатки, скрипти, транспортна мережа, телеконференції, електронна пошта і багато іншого. Звичайно, корпоративний firewall вже не вирішує всіх проблем безпеки. Адже рівний і узагальнений підхід до забезпечення безпеки даних кожного співробітника компанії неминуче призводить до наявності проломів в захисті. Через це страждають потреби того чи іншого працівника, коли виявляються закритими критичні для виконання роботи ресурси. Більш того, багато систем безпеки відокремлюють від загального доступу тільки життєво важливі дані (наприклад, бухгалтерський облік), в той час як інші відомості, які вважаються менш важливими, доступні всім. Звичайно, це не означає, що співробітники сусіднього підрозділу вивчають дані своїх колег. Але така відкритість робить дані всіх працівників вразливими до атаки через одну-єдину лазівку в мережі. Тому замість псування даних на 1-2 комп'ютерах страждають усі.

Вірус Code Red вивів з ладу саме ті сервери, які були захищені від елементарних атак з Мережі і не стежили за своєю зростаючою уразливістю (через відсутність подібних прецедентів). Мала місце вразливість, але у зв'язку з тим, що раніше подібні атаки не проводилися, ніхто про неї не думав. У підсумку така безпечність коштувала мільйонів доларів. Узагальнимо основні причини уразливості веб-серверів.

Більшість зростаючих підприємств регулярно змінює конфігурацію

своїх мереж, додаючи нові робочі станції (іноді і сервери), забуваючи при цьому тестувати ЛВС на безпеку. Зрозуміло, заборонити підключати нових користувачів неможливо, але варто задуматися про розширення мережі заздалегідь. Позначити її сегменти, які здатні до розширення, і проводити попереднє тестування на безпеку. Більшість веб-майстрів мають кореневий або адміністраторський доступ до сервера. Розумніше прописати кожному користувачеві свою політику доступу, що обмежує його права прямими обов'язками. Наприклад, співробітник працює тільки з одним каталогом сервера, але має доступ на всі інші. Тим самим він ставить під загрозу не тільки свій сектор робіт, але і всі дані сервера. Звичайно, статус веб-майстра має не кожен користувач, хоча обмежити доступ з міркувань безпеки слід і самим високим за професійною ієрархією професіоналам.

Програмне забезпечення веб-серверів (суміш піратських, ліцензійних, shareware- і freeware-програм) робить систему вразливою. Найбезпечніший підхід – сумісне програмне забезпечення від одного виробника.

Безпека веб-серверів зводиться до управління ризиками. Але не кожна компанія має потребу у вищому ступені захисту своєї інформації. Питання рівня безпеки – це питання використання ресурсів мережі. Якщо веб-сервер існує, наприклад, тільки для потреб маркетингу, то особливо складну систему захисту встановлювати не варто. Проте системи забезпечення електронної комерції, електронних платежів вимагають потужних заходів безпеки. Тому прийнято розділяти рівні захисту веб-серверів.

Безпека – це люди, процеси, програми, безперервний пошук уразливих місць системи, налагоджена структура ліквідації загрози і контроль над виконуваними програмами. На теперішній час нормальне функціонування Web-сервера, підключеного до мережі Internet, практично неможливе, якщо не приділяти належну увагу питанням забезпечення його безпеки. Ця проблема може бути вирішена шляхом використання комплексного підходу до захисту ресурсів сервера від можливих атак. Для цього до складу комплексу засобів захисту сервера повинні входити системи антивірусного захисту, контролю цілісності, виявлення вторгнень, розмежування доступу, криптографічного захисту, а також підсистема управління. При цьому кожна з систем повинна бути оснащена елементами власної безпеки.

Одержано 27.10.2019