УДК 004.031.6
В. Сташук, І. Павлов, Л. Матійчук, кан. екон. наук; доц.
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ОЦІНКА ІСНУЮЧИХ СИСТЕМ ВИЯВЛЕННЯ АТАК

UDC 004.031.6
V. Stashuk, I. Pavlov, L. Matiychuk, Ph.D.; Assoc. Prof.

EVALUATION OF EXISTING ATTACK DETECTION SYSTEMS

На сьогоднішній день дуже інтенсивно розвиваються технології захисту корпоративних мереж, які включають в себе:

- МЕ (Firewall) – це програма або спеціалізована апаратна реалізація, що, ґрунтуючись на деяких правилах, дозволяє або забороняє передачу інформації, що проходить через неї, з метою обмеження деякої підмережі від зовнішнього доступу чи навпаки, для заборони виходу назовні. Міжмережеві екрани реалізують механізми контролю доступу із зовнішньої мережі до внутрішньої шляхом фільтрації всього вхідного і вихідного трафіку, пропускаючи тільки авторизовані дані. Всі міжмережеві екрани функціонують на основі інформації, яка отримується з різних рівнів еталонної моделі ISO/OSI, і чим вищий рівень OSI, на основі якого побудований МЕ, тим вищий рівень захисту, що ним забезпечується. Існують три основних типи міжмережевих екранів – пакетний фільтр (packet filtering), шлюз на сеансовому рівні (circuit-level gateway) і шлюз на прикладному рівні (application-level gateway). Існує дуже мало міжмережевих екранів, які можуть бути одночасно віднесені до одного з названих типів. Як правило, Firewall суміщає в собі функції двох або трьох типів.
- Найбільш очевидний недолік МЕ – неможливість захисту від користувачів, які знають ідентифікатор і пароль для доступу в сегмент корпоративної мережі, який захищається. МЕ може обмежити доступ до ресурсів, але він не може заборонити авторизованому користувачу скопіювати цінну інформацію або змінити які-небудь параметри. А по статистиці не менше ніж 70% всіх загроз безпеці надходить зі сторони співробітників організації.
- Віртуальна приватна мережа (VPN – Virtual Private Network). Технологія VPN призначена для побудови єдиного прозорого користувацького середовища поверх будь-якої транспортної мережі. Таке рішення дозволяє організувати: безпечний віддалений доступ персоналу до мережі підприємства чи організації з будь-якого робочого місця, підключеного до мережі Інтернет; достовірний підрахунок вживаних абонентом ресурсів в широкомовних транспортних мережах (наприклад, в мережах Ethernet); безпечну передачу конфіденційної інформації по мережі Інтернет без побудови додаткових фізичних каналів зв'язку. При побудові таких мереж можливо використовувати як комутовані канали зв'язку (dial-up), так і некомутовані (виділені лінії). При цьому для забезпечення конфіденційності інформації, що передається, не потребується організація додаткової виділеної лінії, а можливе використання вже існуючої, що значно знижує вартість побудови мереж VPN. Безпека інформації, що передається по мережі забезпечується шляхом шифрування з використанням будь-якого з наявних криптоалгоритмів.
- Сканер безпеки. Класичним сканером, який поставляється з усіма *nix подібними операційними системами є nmap. Програма призначена для сканування мереж з будь-якою кількістю об'єктів, визначаючи стан об'єктів мережі, що сканується а також портів і відповідних служб. Для цього nmap використовує багато різних методів сканування таких як UDP, TCP connect(), TCP SYN (напіввідкрите), FTP proxy (прорив через ftp), Reverse-ident, ICMP (ping), FIN, ACK, Xmas tree, SYN і NULL сканування.
- Одним з найновіших сканерів безпеки є Nessus. Nessus являє собою безплатний сучасний сканер безпеки локальних і віддалених систем. Початок Nessus Project було покладено в 1998 році, перший реліз вийшов в квітні. На той період найпоширенішим сканером безпеки був SATAN. Задачею Nessus являється визначення запущених служб і вразливостей, включаючи

найпопулярніші повідомленні про «дірки» wu-ftpd, наявність демонів DDOS, проблеми ipfw FreeBS і ін. Основний принцип полягає в тому, що вся інформації потребує перевірки, тобто інформація багерів основних служб не вважається основоположною.

- Систему виявлення вторгнень (IDS). Для запобігання комп'ютерним атакам, необхідно розробляти та налаштовувати системи захисту інформації та системи виявлення атак. Системи виявлення комп'ютерних атак – це один із найважливіших елементів систем інформаційної безпеки мереж. Враховуючи зростання в останні роки число проблем зв'язаних з комп'ютерною безпекою постійно зростає, як і пов'язаних з ними число хакерських атак (рис. 1). Системи виявлення вторгнень включають в себе: виявлення спроб несанкціонованого доступу та захист від атак типу „відмова в обслуговуванні" (DOS-атак).

Виявлення атак потребує виконання однієї із двох умов: розуміння очікуваної поведінки підконтрольного об'єкта системи або знання всіх можливих атак і їх модифікацій.

При створенні систем виявлення атак використовуються два основні підходи:

– виявлення аномальної поведінки, використовуючи апарат математичної статистики, який досить добре себе зарекомендував. Даний підхід використовується, як правило, при виявленні DoS-атак, які використовують посилку великої кількості трафіку за короткий інтервал часу [25];

– виявлення зловживань, використовуючи сигнатури, що описують послідовність байт і дій, які характеризують несанкціоновану діяльність. Цей підхід знайомий по антивірусних системах, які побудовані саме за цим принципом.

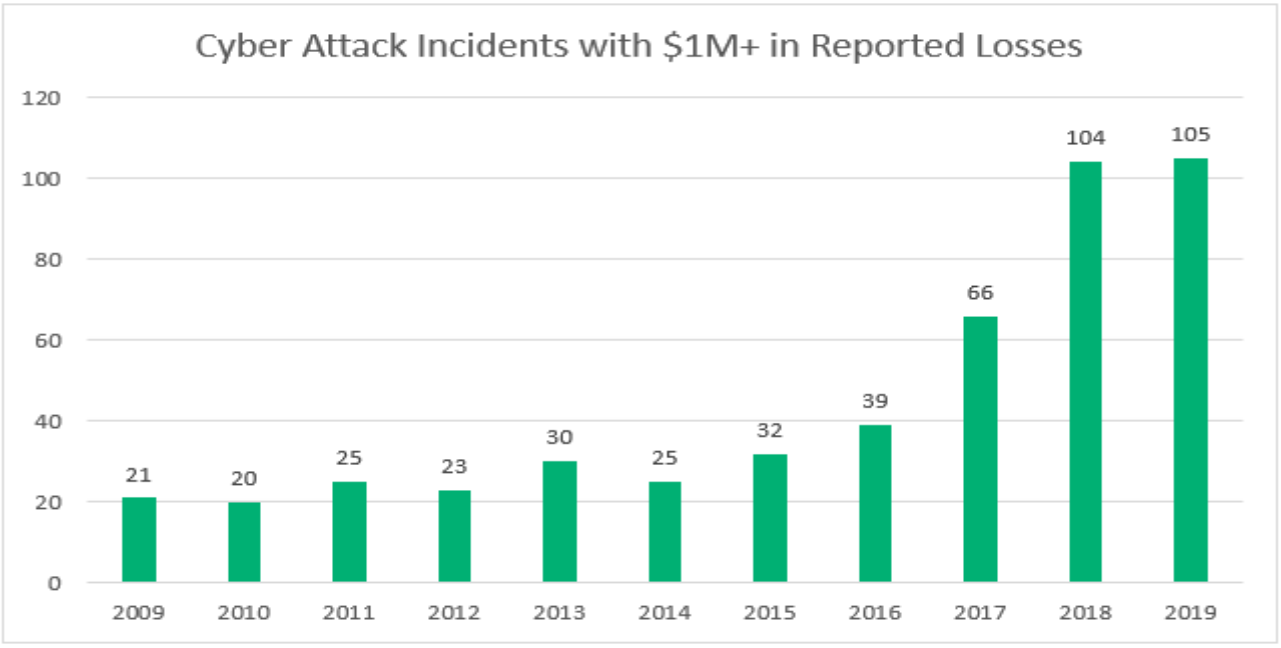

Рисунок 1. Кількість атак в мережі Інтернет