ІНТЕРНЕТ ТА ІНФОРМАЦІЙНА БЕЗПЕКА

Паршукова Л. М.
старший викладач кафедри інформатики та ІКТ
Уманський державний педагогічний університет
імені Павла Тичини

Спілкування з використанням новітніх засобів комунікації увібрав в себе Інтернет. Всесвітня інформаційна мережа розвивається великими темпами, кількість учасників постійно зростає. За деякими даними, у мережі зареєстровано близько 1,5 мільярди сторінок. Деякі «живуть» до півроку, а деякі працюють на своїх власників в повну силу і приносять великий прибуток. Інформація в мережі охоплює всі сторони життєдіяльності людини і суспільства. Користувачі довіряють цій формі себе і свою діяльність. Проте досвід роботи в галузі комп'ютерних технологій повен прикладів несумлінного використання ресурсів Інтернет.

Фахівці кажуть, що головна причина проникнення в комп'ютерні мережі - безтурботність і непідготовленість користувачів. Це характерно не лише для пересічних користувачів, але і для фахівців в області комп'ютерної безпеки. Разом з тим, причина не тільки в халатності, але й у порівняно невеликому досвіді фахівців з безпеки у сфері інформаційних технологій. Пов'язано це зі стрімким розвитком ринку мережевих технологій і самої мережі Інтернет.

За даними лабораторії Касперського, близько 90% від загального числа проникнень на комп'ютер шкідливих програм використовується за допомогою Інтернет, через електронну пошту і перегляд Web-сторінок. Особливе місце серед таких програм займає цілий клас - Інтернет-черв'як. Саме поширюються, не залежно від механізму роботи виконують свої основні завдання щодо зміни налаштувань комп'ютера-жертви, крадуть адресну книгу або цінну інформацію, вводять в оману самого користувача, створюють розсилку з комп'ютера за адресами, взятим із записної книжки, роблять комп'ютер чиїмось ресурсом або забирають частину ресурсів для своїх цілей або в гіршому випадку самоліквідуються, знищуючи всі файли на всіх дисках.

Всі ці та інші з ними пов'язані проблеми можна вирішити за

допомогою наявності в організації опрацьованого документа, що відображає політику інформаційної безпеки компанії. У такому документі мають бути чітко прописані такі положення:

Як ведеться робота з інформацією підприємства;

Хто має доступ;

Система копіювання і зберігання даних;

Режим роботи на ПК;

Наявність охоронних та реєстраційних документів на обладнання та програмне забезпечення;

Виконання вимог до приміщення, де розташовується ПК і робоче місце користувача;

Наявність інструкцій і технічної документації;

Наявність робочих журналів та порядок їх ведення.

Крім того, необхідно постійно відслідковувати розвиток технічних та інформаційних систем, що публікуються у періодичній пресі або стежити за подіями, обговорюваних на подібних семінарах.

На переконання експертів «Лабораторії Касперського», завдання забезпечення інформаційної безпеки повинна вирішуватися системно. Це означає, що різні засоби захисту (апаратні, програмні, фізичні, організаційні і т.д.) повинні застосовуватися одночасно і під централізованим управлінням. При цьому компоненти системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

На сьогоднішній день існує великий арсенал методів забезпечення інформаційної безпеки [6; 275]:

Засоби ідентифікації і аутентифікації користувачів (так званий комплекс ЗА);

Засоби шифрування інформації, що зберігається на комп’ютерах і переданої мережами;

- Міжмережеві екрани;
- Віртуальні приватні мережі;
- Кошти тематичній фільтрації;
- Інструменти перевірки цілісності вмісту дисків;
- Засоби антивірусного захисту;
- Системи виявлення вразливостей мереж і аналізатори мережевих атак.

Кожне з перерахованих коштів може бути використано як

самостійно, так і в інтеграції з іншими. Це робить можливим створення систем інформаційного захисту для мереж будь-якої складності і конфігурації, що не залежать від використовуваних платформ.«

Системи шифрування дозволяють мінімізувати втрати у разі несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії, а також перехоплення інформації при її пересилання по електронній пошті або передачу з мережних протоколах. Завдання даного засоби захисту - забезпечення конфіденційності. Основні вимоги, що пред'являються до систем шифрування - високий рівень криптостійкості і легальність використання на території України (або інших держав).

Міжмережевий екран являє собою систему або комбінацію систем, що утворить між двома або більше мережами захисний бар'єр, що оберігає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних.

Основний принцип дії міжмережевих екранів - перевірка кожного пакету даних на відповідність вхідного і вихідного IP-адреси базі дозволених адрес. Таким чином, міжмережеві екрани значно розширюють можливості сегментування інформаційних мереж та контролю за циркулювання даних.

Говорячи про криптографії і міжмережевих екранах, слід згадати про захищених віртуальних приватних мережах (Virtual Private Network - VPN). Їх використання дозволяє вирішити проблеми конфіденційності і цілісності даних при їх передачі по відкритим комунікаційних каналів. Використання VPN можна звести до вирішення трьох основних завдань:

1. захист інформаційних потоків між різними офісами компанії (шифрування інформації здійснюється тільки на виході в зовнішню мережу);

2. захищений доступ віддалених користувачів мережі до інформаційних ресурсів компанії, як правило, здійснюваний через інтернет;

3. захист інформаційних потоків між окремими додатками всередині корпоративних мереж (цей аспект також дуже важливий, оскільки більшість атак здійснюється з внутрішніх мереж).

Ефективний засіб захисту від втрати конфіденційної інформації - фільтрація вмісту вхідної та вихідної електронної пошти.

Перевірка самих поштових повідомлень і вкладень в них на основі правил, встановлених в організації, дозволяє також убезпечити компанії від відповідальності за судовими позовами і захистити їх співробітників від спаму. Засоби тематичній фільтрації дозволяють перевіряти файли всіх поширених форматів, у тому числі стислі і графічні. При цьому пропускна здатність мережі практично не змінюється.

Всі зміни на робочій станції або на сервері можуть бути відслідковані адміністратором мережі або іншим авторизованим користувачем завдяки технології перевірки цілісності вмісту жорсткого диска (integrity checking). Це дозволяє виявляти будь-які дії з файлами (зміна, видалення або ж просто відкриття) та ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами. Контроль здійснюється на основі аналізу контрольних сум файлів (CRC-сум).

Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Крім того, розроблені технології моделювання поведінки, що дозволяють виявляти новостворювані вірусні програми. Виявлені об’єкти можуть піддаватися лікуванню, ізолюватися (поміщатися в карантин) та видалені. Захист від вірусів може бути встановлена на робочі станції, файлові і поштові сервери, міжмережеві екрани, що працюють під практично будь-який з поширених операційних систем (Windows, Unix-і Linux-системи, Novell) на процесорах різних типів.

Фільтри спаму значно зменшують непродуктивні трудозатрати, пов’язані з розбором спаму, знижують трафік і завантаження серверів, покращують психологічний фон в колективі і зменшують ризик залучення співробітників компанії на шахрайські операції. Крім того, фільтри спаму зменшують ризик зараження новими вірусами, оскільки повідомлення, що містять віруси (навіть ще не увійшли до бази антивірусних програм) часто мають ознаки спаму і фільтруються. Щоправда, позитивний ефект від фільтрації спаму може бути перекреслений, якщо фільтр поряд зі сміттєвими видаляє або маркує як спам і корисні повідомлення, ділові або особисті.

Для протидії природним загрозам інформаційної безпеки в компанії має бути розроблений і реалізований набір процедур щодо

запобігання надзвичайних ситуацій (наприклад, щодо забезпечення фізичного захисту даних від пожежі) та мінімізації збитку в тому випадку, якщо така ситуація все-таки виникне. Один з основних методів захисту від втрати даних - резервне копіювання з чітким дотриманням встановлених процедур (регулярність, типи носіїв, методи зберігання копій і т.д.) [5; 382].

Список використаних джерел

1. Галатенко, В.А. Основи інформаційної безпеки. Інтернет-університет інформаційних технологій - ІНТУІТ.ру, 2008;
2. Галатенко, В.А. Стандарти інформаційної безпеки. Інтернет-університет інформаційних технологій - ІНТУІТ.ру, 2005;
3. Лопатин, В.М. Інформаційна безпека Росії: Людина, суспільство, держава. Серія: Безпека людини і суспільства. М.: 2000. - 428 с;
4. Шаньгін, В.Ф. Захист комп'ютерної інформації. Ефективні методи і засоби. - М.: ДМК Пресс, 2008. - 544 с.
5. Щербаков, О.Ю. Сучасна комп'ютерна безпека. Теоретичні основи. Практичні аспекти. - М.: Книжковий світ, 2009. - 352 с.