УДК 004.415.056.5

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД ВНУТРІШНІХ ЗАГРОЗ

Дмитрук В.Р., Толюпа С.В.
Київський національний університет імені Тараса Шевченка, м. Київ
E-mail: vladislava.dmitruk@gmail.com

Protection of information resources against internal threats

Analysis of security mechanisms regarding insider attacks in modern information systems is conducted. The main tasks and functions of Information Protection and Control (IPC) technology are examined. Information security system from insider threats includes technical security mechanisms and software, psychological and organizational measures and work with staff. In order to ensure and develop comprehensive security system creating of the appropriate unit to adress internal threats, developing enterprise security policies and implementing continuous security monitoring are proposed.

Процеси глобалізації та інформатизації відіграють важливу роль у діяльності кожного підприємства. Створення електронних архівів та масивів даних стає, з одного боку, необхідно умовою підвищення ефективності роботи кожного підприємства, а з іншого – джерелом нових небезпек. Так, згідно за статистикою, станом на 2015 рік співвідношення інцидентів інформаційної безпеки, що виникло через внутрішні загрози, до інцидентів, пов’язаних з зовнішніми джерелами загроз, тримається на рівні 65% до 35% відповідно.

Інсайдер - робітник компанії, який має доступ до конфіденційної інформації, розміщеної у комп'ютерній мережі установи. Внутрішні порушники поділяються на наступні категорії: лояльні інсайдери (недбалі та маніпульовані); скривджені та нелояльні інсайдери; мотивовані ззовні (мотивовані фінансово та впроваджені); інші порушники (ті, що мають на меті вплинути на вартість акцій підприємства) [1].

Протидія інсайдерству має здійснюватися безперервно, адже кожен співробітник, який має доступ до інформації є потенційним порушником. При цьому необхідно дотримуватись балансу між закритістю інформації та її доступністю для працівників компанії, інакше вони не зможуть виконувати свої прямі обов’язки. Основні напрямки захисту від інсайдерів [2]: захист документів; захист каналів витоку; моніторинг дій користувачів.

Information Protection and Control (IPC) – технологія захисту конфіденційної інформації від внутрішніх загроз. Рішення класу IPC призначені для захисту інформації від внутрішніх загроз, запобігання різних видів витоків інформації, корпоративного шпигунства і бізнес-розвідки. У цій системі комбінується два основні підходи до захисту: шифрування носіїв даних у всіх вузлах мережі та здійснення контролю за технічними каналами витоку інформації із залученням технологій DLP.

До додаткових завдань цієї системи належать:

- запобігання передачі зовні не тільки конфіденційної, а й іншої небажаної інформації;

- запобігання передачі небажаної інформації не тільки зсередини назовні, але і зовні всередину інформаційної системи організації;

- запобігання використання працівниками Інтернет-ресурсів та ресурсів мережі в особистих цілях;

- захист від спаму та вірусів;

- оптимізація завантаження каналів, зменшення нецільового трафіку;

- облік робочого часу і присутності робітників на робочому місці;

- архівування інформації на випадок випадкового видалення або псування оригіналу;

- захист від випадкового або навмисного порушення внутрішніх нормативів;

- забезпечення відповідності стандартів в області інформаційної безпеки і чинного законодавства.

IPC – системи використовують DLP-системи для здійснення контролю за потоками інформації, що циркулюють ззовні та у мережі. Основним завданням DLP-систем, є запобігання передачі конфіденційної інформації за межі інформаційної системи. Така передача (витік) може бути навмисною або ненавмисною. Як показує практика, більша частина витоків відбувається не через зловмисні наміри, а через помилки, неуважність, безтурботність, недбалість працівників. Інша частина пов'язана зі злим умислом операторів і користувачів ІС. Зрозуміло, що інсайдери, як правило, намагаються подолати засоби DLP-систем. Результат цієї боротьби залежить від багатьох факторів. Гарантувати успіх тут неможливо.

Технології IPC використовують різні підключаються криптографічні модулі, в тому числі найбільш ефективні алгоритми DES, Triple DES, RC5, RC6, AES, XTS-AES.

Технологія DLP в IPC підтримує контроль наступних технічних каналів витоку конфіденційної інформації: периферійні пристрої (USB, LPT, COM, WiFi, Bluetooth і інше); локальні і мережеві принтери; корпоративна електронна пошта; веб-пошта; соціальні мережі та блоги; файлообмінні мережі, форуми та інші інтернет-ресурси; засоби миттєвого обміну повідомленнями тощо.

Технології DLP в IPC підтримують контроль в тому числі наступних протоколів обміну даними: FTP, FTP-over-HTTP, FTPS, HTTP, HTTPS (SSL), NNTP, POP3, SMTP.

Крім основного перед DLP-системою можуть стояти і вторинні (побічні) завдання. Вони такі:

- архівування повідомлень, які пересилаються на випадок можливих у майбутньому розслідувань інцидентів;

- запобігання передачі зовні не тільки конфіденційною, але і іншої небажаної інформації (образливих виразів, спаму, еротики, зайвих обсягів даних тощо);

- запобігання передачі небажаної інформації не тільки зсередини назовні, але і зовні всередину інформаційної системи;

- запобігання використанню працівниками державних інформаційних ресурсів в особистих цілях;

- оптимізація завантаження каналів, економія трафіку;

- контроль присутності працівників на робочому місці;

- відстеження благонадійність співробітників, їх політичних поглядів, переконань, збір компромату.

Для того, щоб зафіксувати передачу конфіденційної інформації, використовуютсья такі технології:

1) сигнатури – пошук у потоці даних певної послідовності символів;

2) «цифрові відбитки» (Digital Fingerprints або DG). DLP/IPC-системі передається якийсь стандартний документ-шаблон, з нього створюється «цифровий відбиток» і записується в базу даних DF. Після цього в правилах контентної фільтрації настроюється процентна відповідність шаблону з бази;

3) «мітки». - призначення спеціальних «міток» файлам, що містять конфіденційну інформацію;

4) пошук за регулярними виразами;

5) лінгвістичні методи;

6) ручне детектування («Карантин»).

Однак, жоден з наведених методів детектування конфіденційної інформації не може вважатися цілком надійним. Необхідно комбінувати різні продукти та методи, зважаючи на їхні сильні та слабкі сторони. Загалом система захисту інформації від внутрішніх загроз повинна включати в себе як технічний захист каналів витоку, так і програмні засоби, психологічні та організаційні заходи, і роботу з персоналом.

Спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам CERT-UA розробив рекомендації щодо захисту інформаційних ресурсів від внутрішніх загроз. Так, необхідно будувати систему захисту, орієнтуючись на попередній досвід компанії щодо внутрішніх інцидентів ІБ. Перш за все, необхідно забезпечити надійний захист критично важливих ресурсів, для цього необхідно використовувати різноманітні технології та системи захисту (DLP, SIEM, IDS тощо). Для створення системи інформаційного захисту можуть використовуватись такі продукти, як McAfeeDataLossPreventio Host, Reconnex, PortAuthority 5.0, StarForceContentEnterprise. Однак жоден з них не може забезпечити повний захист від діяльності інсайдерів. На думку спеціалістів даної організації, головним індикатором захищеності від внутрішніх загроз є взаємовідносини з партнерами та між співробітниками [3].

Отже, необхідно комплексно забезпечувати та розвивати систему захисту. Для того, щоб забезпечити комплексність ІБ, потрібно сформувати відповідний підрозділ з протидії внутрішнім загрозам, розробити політику безпеки підприємства та впровадити постійний контроль за станом безпеки підприємства. Систему захисту необхідно постійно покращувати та вдосконалювати.

Література

1. Ульянов В.В. Динамика безопасности: от внешних угроз – к внутренним / В.В.Ульянов // Защита информации. INSIDE.– 2008. - № 4. – С. 34 – 38.
2. Probst, C.W. Insider Threats in Cyber Security/ C.W. Probst– 2010. – 245р.
3. CUA-15-04R. Рекомендації CERT-UA з протидії загрозі інсайдера [Електронний ресурс] / І. Соколов - №1 – 2015 - Режим доступу: http://cert.gov.ua/pdf/CUA-15-04R.pdf