УДК 004.056.
© Л. Мороз[15], Б.Цаль[2], 2013

ВИРІШЕННЯ ПРОБЛЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Досліджено програмний продукт «Контур інформаційної безпеки SearchInform», який дає змогу ефективно контролювати інформаційні потоки підприємства на всіх рівнях - від комп'ютера окремого користувача до серверів локальної мережі.

A software product "SearchInform Information Security Perimeter" which allows to control the data streams of enterprise on all levels from every single user's workstation to corporate servers was under research.

1. ВСТУП

На сьогодні захищена інформація - це один з найважливіших факторів успіху діяльності будь-якої організації. Середня вартість одного випадку витоку інформації у світі становить близько 5,3 млн. доларів. Існує безліч каналів передачі даних: електронна пошта, соціальні мережі (Facebook, Однокласники, ВКонтакте та ін.), форуми, блоги, служби миттєвого обміну повідомленнями (ICQ, MSN, Google Talk, Mail.ru Агент, Windows Live, X-Lite і пр.), зовнішні носії інформації, мобільні пристрої, принтери, FTP-сервери, Skype [1-3].Якщо канали передачі інформації в організації не контролюються, або контролюється всього 1-2 канали, то важлива інформація може бути вільно передана конкурентам.

Сучасна система інформаційної безпеки повинна дозволяти співробітнику використовувати всі канали для передачі інформації, а фахівцям з інформаційної безпеки - аналізувати інформаційні потоки, що йдуть по цих каналах. При цьому реалізація комплексної політики інформаційної безпеки неможлива при наявності хоча б одного неконтрольованого службою безпеки каналу потенційних витоків.

Програмний продукт «Контур інформаційної безпеки SearchInform» - це зручний засіб контролю інформаційних потоків [1]. Він дозволяє ефективно захищати бізнес від збитків, пов'язаних з витоками інформації.

[15] Національний університет «Львівська політехніка»
[2]

2. МЕТА РОБОТИ

Метою даної роботи є аналіз програмного продукту «Контур інформаційної безпеки SearchInform», дослідження принципів роботи продукту та оцінка ефективності.

3. ОГЛЯД ДОСЛІДЖЕНЬ

«Контур інформаційної безпеки SearchInform» – це один з лідерів на ринках інформаційної безпеки. Продукт використовується в багатьох великих організаціях, що працюють у різних галузях - від банківської справи до машинобудування.

Програмне рішення дозволяє ефективно контролювати інформаційні потоки підприємства на всіх рівнях: від комп'ютера окремого користувача до серверів локальної мережі. Контролюються також всі дані, що йдуть в Інтернет. Контур має модульну структуру, тобто користувач може за своїм вибором встановити тільки частину компонентів.

Інтеграція з доменною системою Windows дає можливість достовірно ідентифікувати користувача, що відправив повідомлення електронною поштою, Skype, ICQ, MSN, JABBER або залишив його на форумі або блозі, навіть якщо співробітник скористався для цього поштовою скринькою на безкоштовному сервері, підписався чужим ім'ям (нікнеймом) або увійшов у мережу з чужого комп'ютера.

SearchInform дозволяє повноцінно контролювати ноутбуки по всіх каналах, навіть коли вони знаходяться за межами корпоративної мережі.

Агент EndpointSniffer ретельно приховує свою присутність на лептопі, виявити його непросто навіть кваліфікованому фахівцю. Він збирає відправлені дані, які будуть передані для аналізу відділу інформаційної безпеки відразу ж, як тільки лептоп виявить з'єднання з мережею.

У 2013 році вийшло додаткове рішення - MicrophoneSniffer, що дозволяє при включеному ноутбуці записувати розмови навколо.

«Контур інформаційної безпеки SearchInform» на сьогодні підтримує перехоплення пошти, IM, Skype і HTTP-трафіку з iPhone та iPad.

Елементи «Контура інформаційної безпеки SearchInform» :

Контроль робочого часу співробітників .

Поряд із захистом конфіденційної інформації компанії та боротьбою з інсайдерством, важливим завданням сьогодні є виявлення неефективних співробітників.

ProgramSniffer – новий модуль, що входить до складу «Контуру інформаційної безпеки SearchInform» надає співробітникові служби безпеки звіти про:

– час, коли співробітник приходить та йде з роботи;
– час реальної роботи за комп'ютером;
– статистику та час використання додатків.

2. Розпізнавання дій інсайдерів.

Часто недобросовісні співробітники, намагаючись обдурити службу безпеки, передають інформацію в графічному вигляді або, наприклад, у зашифрованому архіві.

Для повноцінного контролю необхідно:

- розпізнати текст в графічних файлах і здійснювати пошук по ньому;

- виявити передачу зашифрованих архівів по всіх каналах можливого витоку інформації;

-виявити пересилку файлів із зміненим типом.

3. Робота з колективом:

DLP-система відстежує настрої в колективі шляхом моніторингу повідомлень співробітників в інтернет-месенджерах (Skype, ISQ) і соцмережах у робочий час.

Оптимізація роботи:

За допомогою DLP-системи можна контролювати реакцію колективу на нововведення та відповідно до неї ефективно коригувати внутрішню політику підприємства.

Кожен з компонентів контура інформаційної безпеки підприємства узгоджується з єдиною системою розмежування прав доступу. Система володіє рядом гнучких налаштувань і дозволяє вибудувати ієрархію доступу до конфіденційної інформації будь-яким чином.

Всі компоненти системи мають клієнт-серверну структуру. Серверна - це одна з платформ для перехоплення даних - SearchInform NetworkSniffer або SearchInform EndpointSniffer, і клієнтські програми, призначені для роботи з базою перехоплених даних та проведення службових розслідувань.

SearchInform NetworkSniffer - платформа для перехоплення даних на рівні віддзеркаленого трафіку, тобто NetworkSniffer обробляє трафік, не впливаючи на роботу корпоративної мережі. Перехоплюються дані, що пересилаються користувачами по мережевих протоколах та каналах (SMTP, POP3, IMAP, HTTP, HTTPs, MAPI, ICQ, JABBER, MSN) на рівні локальної мережі.

SearchInform EndpointSniffer - платформа для перехоплення трафіку за допомогою агентів**.** Додатково дозволяє контролювати співробітників, що перебувають за межами корпоративної мережі, які можуть

вільно передати конфіденційні дані з ноутбука третім особам. SearchInform EndpointSniffer збирає відправлені дані і передає їх для аналізу відділу інформаційної безпеки.

Переваги роботи агентів IMSniffer і MailSniffer на платформі SearchInform EndpointSniffer у тому , що вони володіють підвищеною стійкістю до різних збоїв (навіть якщо сервери стануть недоступними, перехоплення буде здійснюватися), здатні перехоплювати і ті дані, які передаються по захищених протоколах. SearchInform EndpointSniffer-агенти контролюють:

Перехоплення інтернет-трафіку

SearchInform NetworkSniffer дозволяє здійснювати перехоплення інформації, яка передається через інтернет. Підтримуються всі поширені протоколи, які можуть використовуватися інсайдерами. Пропонується підтримка проксі-серверів - як програмних (Kerio, Squid і т.д.), так і апаратних (BlueCoat, IronPort і т.д.) - через стандартний протокол ICAP.

Електронну пошту

Один з найбільш небезпечних каналів витоків, оскільки підтримується пересилання великих обсягів даних. Підтримуються протоколи SMTP, POP3, MAPI, IMAP.

HTTP

Можливість витоку інформації через соціальні мережі, блоги, форуми, а також через Web-додатки для відправки електронної пошти та SMS, Web-чати.

FTP

Цей протокол - найважливіший засіб передачі великих обсягів даних, і може використовуватися недобросовісними співробітниками для передачі цілих баз даних, деталізованих креслень, пакетів відсканованих документів та ін.

Skype

«Контур інформаційної безпеки SearchInform» є першим з рішень в області інформаційної безпеки, який забезпечив перехоплення не тільки голосових і текстових повідомлень, а й файлів, переданих через Skype.

Служби миттєвого обміну повідомленнями (IM)

Підтримуються протоколи ICQ, MSN, Mail.ru Агент, JABBER, які активно використовуються офісними працівниками.

«Контур інформаційної безпеки SearchInform» включає ще такі програми:

1. PrintSniffer

Це програма, яка контролює вміст документів, відправлених на друк. Всі дані перехоплюються, вміст файлів індексується і зберігається в базі заданий проміжок часу.

2. DeviceSniffer – програма, що виконує аудит зовнішніх носіїв, підключених до комп'ютера (флешки, компакт-диски, зовнішні вінчестери).

3. MonitorSniffer – призначений для перехоплення інформації, яка відображається на моніторах користувачів і збереження отриманих знімків екрану в базі даних. Підтримується контроль екрану одного або декількох користувачів у режимі реального часу, можна відстежувати стан екранів користувачів термінальних серверів, що працюють за RDP-з'єднанню (протоколу віддаленого робочого столу).

4. FileSniffer – контролює роботу користувачів на загальних мережевих ресурсах, які містять великі обсяги конфіденційних даних, не призначених для розповсюдження за межами компанії.

SearchInform FileSniffer дозволяє контролювати всі операції з файлами на загальнодоступних мережевих ресурсах, захищаючи інформацію, що знаходиться на них.

Програмний продукт «Контур інформаційної безпеки SearchInform» здійснює індексацію робочих станцій, що дозволяє у реальному часі відслідковувати появу, копіювання, переміщення та видалення конфіденційної інформації на робочих станціях користувачів.

4. ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА «КОНТУРУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ SEARCHINFORM» ІЗ АНАЛОГАМИ DLP-СИСТЕМ

Програмний комплекс DeviceLock 7 Endpoint DLP призначений для захисту від інсайдерських витоків даних з комп'ютерів і серверів корпоративних інформаційних систем . Базовий компонент комплексу - DeviceLock 7 , контролюює доступ користувачів до периферійних пристроїв і локальних портів комп'ютерів , доповнюється двома функціональними компонентами - NetworkLock ™ і ContentLock ™ . NetworkLock дозволяє контролювати комунікації користувачів через популярні мережеві додатки , включаючи електронну пошту за допомогою протоколів SMTP і SMTP- SSL , web - пошту Gmail ™ , Yahoo! Mail ™ , Windows Live ® Mail , Mail.Ru , AOL Mail , Yandex.Mail , WEB.DE , GMX.de , месенджери ICQ ® , MSN ® Messenger , Jabber ® , IRC , Yahoo! Messenger ™ , Mail.ru Agent , соціальні мережі Google+ , Twitter ™ , Facebook ® , LiveJournal ™ , LinkedIn ® , MySpace ™ , Одноклассники ™ , ВКонтакте ™ , XING.com , Studivz.de , Meinvz.de ,

Schuelervz.net , передачу файлів по протоколах FTP і FTP- SSL , а також Telnet - сесії. ContentLock забезпечує фільтрацію контенту даних при їх копіюванні на знімні носії і при передачі по мережевих каналах комунікацій .

Розробник - компанія ЗАТ « Смарт Лайн Інк», Росія. Штаб - квартира і підрозділ розробки Смарт Лайн знаходяться в Москві. Компанія має закордонні офіси продажів у США , Великобританії , Німеччини та Італії.

Websense , Inc є розробником в області комплексних рішень з безпеки , таких як: веб-дані і електронна пошта, і забезпечує захист важливої інформації (Essential Information Protection). Штаб – квартира знаходиться в Сан -Дієго , Каліфорнія . Websense поширює свої рішення через глобальну мережу за допомогою партнерської лінії. Рішення Websense щодо забезпечення безпеки допомагає організаціям блокувати шкідливий код , запобігати втратам конфіденційної інформації та забезпечити доцільне використання інтернету.

Компанія McAfee пропонує ряд рішень для безпечної роботи в Інтернеті. Ці рішення ґрунтуються на передових технологіях забезпечення безпеки , включаючи захист від вірусів і шкідливих програм. McAfee – компанія – розробник антивірусного програмного забезпечення. Штаб-квартира знаходиться у Санта-Кларі, штат Каліфорнія, США.

McAfee займається розробкою різних утиліт і додатків для забезпечення антивірусної безпеки і захисту комп'ютерних систем для підприємств і домашніх користувачів.

Нижче подана порівняльна таблиця архітектур систем DeviceLock, WebSense DSS, McAfee та Контуру інформаційної безпеки SearchInform.

Таблиця 1

Порівняння архітектури систем

Ключ порівняння	Контур інформаційної безпеки SearchInform	DeviceLock	WebSense DSS	McAfee
Кількість необхідних серверів і ліцензій стороннього ПЗ (SQL, Oracle, Windows Server)	Один сервер, Windows Server 2003 і вище, MS SQL 2005 і вище.	Два або більше сервери	Один сервер	Один сервер
База перехопленої інформації	Так	Так	Ні	Ні
Інтеграція з поштовими серверами	Так	Ні	Так	Так
Інтеграція з проксі-серверами	Так	Ні	Так	Ні
Робота в кількох доменах	Так	Ні	Ні	Так
Наявність ролей в системі	Так. Розмежування на рівні доступу до системи і доступу до даних	Немає інформації	Частково	Так
Розмежування прав на доступ до перехопленої інформації	Так	Немає інформації	Ні	Так
Маскування служб агента перехоплення	Так, повна	Агента видно в диспетчері завдань	Ні	Ні

Таблиця 2

Порівняння каналів, які контролюють системи

Ключ порівняння	Контур інформаційної безпеки SearchInform	DeviceLock	WebSense DSS	McAfee
Контроль корпоративної електронної пошти	POP3, SMTP, IMAP, MAPI, NNTP, Web-mail (HTTP)	Підтверджено лише SMTP	Тільки дзеркальний вихідний трафік по SMTP, IMAP, MAPI,	Є
Контроль особистої електронної пошти	Так	Так, лише вихідних повідомлень	При порушенні політики	При порушенні політики
Контроль чатів соц. мереж	Так	Ні	Тільки вихідні повідомлення	Ні
Контроль Skype	Все, включаючи звук	Так, крім звуку	Так, крім звуку	Тільки чат
Контроль HTTP (S)	Так	Так	Так	Так
Контроль FTP (S)	Так	Так	Так	Так
Контроль знімних носіїв, можливість тіньового копіювання	Так	Так	Частково	Частково
Перехоплення друку	Так	Частково	Так	Так
Контроль мобільних пристроїв	Так	Ні	Ні	Ні
Контроль ноутбуків поза мережею компанії	Так. Повний контроль з записом на прихований розділ диска	Ні	Тільки при налаштуванні згідно політики	Обмежено
Знімки екрану	Так. Гнучка настройка	Ні	Ні	За заданим інтервалом
Перегляд робочого столу в режимі реального часу	Так	Ні	Ні	Ні

Контроль вмісту робочих станцій і файл серверів	Так	Частково	Ні	Тільки теговані документи
Можливість запису розмов через мікрофон ноутбука	Так	Ні	Ні	Ні
Запис набраного на клавіатурі тексту	Так	Ні	Ні	Ні
Контроль та аналіз використання програм співробітниками	Так	Ні	Ні	Ні

Таблиця 3

Порівняння аналітичних можливостей

Ключ порівняння	Контур інформаційної безпеки SearchInform	DeviceLock	WebSense DSS	McAfee
Розпізнавання графічних файлів (OCR)	Так	Так	Так	Ні
Підтримувані морфології	Українська, російська, англійська	Не заявлено	Англійська	Англійська
Пошук по абзацах тексту	Так	Так, лише точний пошук	Так, лише точний пошук	Так, лише точний пошук
Пошук за атрибутами	Так	Частково	Так	Так
Складні вирази	Так	Так	Ні	Так
Наявність готових політик	Так	Так	Ні	Ні

5. ВИСНОВКИ

Отже, для вирішення проблем інформаційної безпеки на підприємстві необхідно використовувати якісні та ефективні програмні продукти, які в комплексі забезпечать надійний захист. Перевагами дослідженого продукту «Контур інформаційної безпеки SearchInform» є:

1. Простота та швидкість впровадження.

2. Можливість контролювати всі канали передачі інформації, включаючи Skype, соціальні мережі, принтери, а також роботу користувачів на файл-серверах.

3. Функція «пошук схожих», яка дає змогу власними силами швидко і гнучко налаштувати систему оповіщення, не запрошуючи сторонніх фахівців. При цьому для ефективного захисту конфіденційних даних необхідні мінімальні трудовитрати на аналіз інформаційних потоків.

4. Повна інтеграція з доменною структурою Windows дозволяє достовірно ідентифікувати користувача.

5. Розширені пошукові можливості дають змогу ефективно захищати конфіденційні дані при мінімальних трудовитратах на аналіз інформаційних потоків.

1. В. М. Чаплига. Особливості впровадження контуру інформаційної безпеки SearchInform [Електронний ресурс]/ В. М. Чаплига, О. А. Нємкова// - т. 2, Вип. 4. - С. 82-86, 2012. 2. А. В. Єригін. Аналіз ефективності систем запобігання витоку конфіденційної інформації з локальних мереж – Сибірська державна автомобільно-дорожня академія , С. 40-47,2011. 3. М.Д. Воронцова. / М.Д. Воронцова, Ж.А. Мингалєва,// Безпека інформації, як складова економічної безпеки підприємства – Пермський державний університет, С. 9-13, 2010.