УДК 34:004

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ РАСКРЫТИЯ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕСАНКЦИОНИРОВАННЫМ ИЗМЕНЕНИЕМ ИНФОРМАЦИИ, ХРАНЯЩЕЙСЯ НА СЕРВЕРЕ ОРГАНИЗАЦИИ

А.А. Мурлин

ФГБОУ ВПО «Тамбовский государственный технический университет», г. Тамбов

Рецензент д-р юрид. наук, профессор М.А. Желудков

Ключевые слова и фразы: внешняя сеть и внутренняя сети; информация в незашифрованном виде; канал связи; ключ шифрования; криптосервер; личные данные; сервер регистрации; сервер резервных копий; учет вторжений.

Аннотация: Дано техническое решение, дающее возможность организации максимально содействовать следствию, способствующею минимальному привлечению при этом сотрудников организации. Это решение сокращает время передачи данных в правоохранительные органы, что положительно сказывается на результатах расследования. Изложена идея решения регистрации данных о несанкционированных вторжениях на сервере организации.

В настоящее время широко используются информационные технологии для хранения и передачи личных данных на предприятиях. Эта информация хранится на серверах, открытых для доступа через сеть Интернет, так как зачастую требуется наличие возможности обмена этими данными между различными организациями [2]. Примером такой организации может служить «Многофункциональный центр предоставления услуг населению».

В связи с необходимостью передачи этой информации через открытую сеть [3], возникла необходимость в защите данных, передаваемых по существующим каналам связи, а также в защите информации, хранящейся на сервере от вторжения посторонних лиц, преступным путем пытающихся получить или повредить имеющуюся информацию.

Мурлин Александр Александрович – аспирант кафедры «Уголовное право и прикладная информатика в юриспруденции», e-mail: akella68aleks@yandex.ru, ТамбГТУ, г. Тамбов.

Основные технические сложности состоят в следующем [2]:

1) на большинстве серверов не ведется учет вторжений. То есть не записывается путь, по которому пользователь вошел на сервер, время пребывания и какая информация была изменена или скопирована. Причина этого состоит в том, что при большом количестве запросов к серверу, техника не справляется с нагрузкой и не успевает обрабатывать данные, а средства Windows собирают и предоставляют информацию в недоступном даже для системного администратора виде;

2) большинство серверов хранит информацию в незашифрованном виде;

3) основная часть информации передается по незащищенным каналам связи или когда канал связи защищен криптосервером, используется слишком простой ключ шифрования, который не меняется или меняется слишком редко.

Пользуясь вышеописанными недостатками системы, злоумышленник может практически безнаказанно получить доступ к личной информации, хранящейся на сервере и изменить или использовать ее в корыстных целях.

Только правоохранительные органы могут позволить себе отслеживать подобные вторжения, при этом задействуя средства учета компаний, предоставляющих услуги связи, что в наше время – активного развития этой области – может негативно сказаться на качестве услуг, предоставляемых этими компаниями [5].

Предположим, на сервер, где хранятся личные данные, было совершено проникновение с целью повредить информацию, которая там хранится. События разворачиваются следующим образом [7, 8]:

1) системный администратор, который обслуживает этот сервер, обнаруживает повреждение информации и докладывает об этом руководству;

2) руководство организации обращается в полицию с заявлением, в котором указаны примерные сроки вторжения, имеющаяся на сервере информация о доступе к нему и данные о той информации, которая была изменена;

3) полиция обрабатывает мотивы для изменения информации и возможности сотрудников (или бывших сотрудников) организации на доступ к серверу;

4) если проверка сотрудников ничего не дала, полиция отправляет запрос провайдеру на получение информации о том, с каких адресов проходили запросы к внутренней сети этой организации (обработка этих данных занимает длительное время);

5) после обнаружения тех каналов, по которым могло произойти вторжение, ведется работа с каждым из них, что может занять значительное время, которого будет достаточно для того, чтобы злоумышленник «замел все следы».

Возможности решения данной задачи на базе организации, которой принадлежит сервер:

1) записывать полный путь к компьютеру, с которого было организовано проникновение (по примеру функции tracert в Windows [1]);

2) регистрировать данные о том, какая информация и когда была изменена;

3) хранить эти данные на другом сервере, не имеющем выход во внешнюю сеть.

На рисунке изображена схема процесса взаимодействия организации с правоохранительными органами при неправомерном использовании информации.

Основной сервер – содержит целевую информацию, к которой осуществляется доступ.

Сервер резервных копий – содержит копию информации, которая моет быть изменена в процессе работы основного сервера.

Сервер регистрации – регистрирует следующие данные:

– когда была изменена информация на основном сервере;

– какая информация была изменена;

– с какого IP-адреса осуществлялся доступ к данной информации.

Рассмотрим представленную схему на примере.

В организации существует отдел, который занимается обслуживанием основного сервера. Если информация, хранящаяся на основном сервере, была изменена без подтверждения необходимости произведенных изменений, системные администраторы, отвечающие за безопасность сервера, готовят данные о том, какая информация была изменена, когда и с какого

Схема взаимодействия организации с правоохранительными органами при неправомерном использовании информации

IP-адреса. Эти сведения включают в себя информацию с сервера регистрации и сервера резервных копий.

Пунктирная линия на схеме означает, что существует возможность передачи данных с основного сервера, если в ней возникнет необходимость (то есть у следствия появляются причины проверить информацию о вторжении), но на практике быстрее и проще и для полиции, в целях расследования преступления «по горячим следам», и для организации не прерывать свою работу на долгое время.

Исходя из вышеизложенного, эффективнее будет изымать только данные с сервера резервных копий и сервера регистрации, не затрагивая основной сервер.

Таким образом, в данной статье изложено техническое решение, дающее возможность организации максимально содействовать следствию, практически не привлекая при этом сотрудников организации. Это решение сокращает время передачи данных в правоохранительные органы, что положительно сказывается на результатах расследования. К тому же регистрация данных о несанкционированных вторжениях на сервере регистрации позволит ответственным лицам организации своевременно получать информацию о таких действиях и существенно сократит время между фактическим совершением противоправного деяния и обращением организации в правоохранительные органы с заявлением об обнаружении результатов данного деяния.

Список литературы

1. Аллен, Р. Active Directory. Сборник рецептов. Windows Server 2003 и Windows 2000 / Р. Аллен. – СПб. : Питер, 2006. – 432 с.

2. Волкова, В. Теория систем : учеб. пособие для вузов / В. Волкова, А. Денисов. – М. : Высшая школа, 2006. – 511 с.

3. Гниденко, И. Информационные технологии в бизнесе : учеб. пособие / И. Гниденко, С. Соколовская. – М. : Вектор, 2005. – 160 с.

4. Кастельс, М. Информационная эпоха: экономика, общество и культура / М. Кастельс. – М. : Изд-во ГУ–ВШЭ, 2000. – 607 с.

5. Кулемина, Ю. Информационные системы в экономике / Ю. Кулемина. – М. : Окей-книга, 2009. – 112 с.

6. Лазарев, И. Новая информационная экономика и сетевые механизмы ее развития / И. Лазарев, К. Лазарев, Г. Хижа. – М. : Дашков и Ко, 2005. – 244 с.

7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (с изменениями от 28.07.2012) [Электронный ресурс] // ГАРАНТ. – Режим доступа : http://base.garant.ru/12125178/. – Загл. с экрана.

8. О полиции : федер. закон от 07.02.2011 г. № 3-ФЗ (с изменениями от 25.06.2012) [Электронный ресурс] // ГАРАНТ. – Режим доступа : http://base.garant.ru/12182530/. – Загл. с экрана.

9. Ясенев, В. Информационные системы и технологии в экономике / В. Ясенев. – М. : Юнити-Дана, 2008. – 560 с.

Improving Crime Detection in Unauthorized Data Modification on Company Server

A.A. Murlin

Tambov State Technical University, Tambov

Key words and phrases: account intrusions; backup server; communication channel; cryptographic server; encryption key; external network and internal network; information in an unencrypted form; personal data; registration server.

Abstract: The paper describes the technical solution, allowing an organization to contribute to crime detection with minimal involvement of the staff. The solution shortens the time of data transfer to law enforcement bodies, having a positive effect on the investigation. The idea of data registration of unauthorized intrusion in company server has been described.
