Концепция системы контроля безопасности функционирования POS-сетей в реальном времени

Д. В. Козлов, Н. П. Садовникова

Волгоградский государственный технический университет

mrdiko4@gmail.com, npsn1@yandex.ru

Аннотация

В статье проводится анализ текущей ситуации в сфере обнаружения и предотвращения киберугроз. Описываются существующие решения администрирования и предотвращения мошенничества в POS-сетях. Предлагается концепция мониторинга безопасности функционирования POS-сети в реальном времени. В статье также описаны основные функциональные требования сервиса мониторинга и его интеграция с системой администрирования POS-сетей.

Ключевые слова: анализ угроз, проактивный мониторинг, информационная система, POS-сети.

1. Введение

На сегодняшний день мошенничество — это многомиллиардный бизнес в долларовом эквиваленте, и он растет с каждым годом. Глобальный обзор экономической преступности PwC в 2016 году зафиксировал то, что киберпреступность поднялась на 2-е место наиболее известных экономических преступлений, затрагивающих 32% организаций. Большинство компаний все еще недостаточно подготовлены для борьбы с подобного рода угрозами и даже не понимают риски: только 37% организаций в мире имеют план реагирования на киберугрозы. В России, эта цифра еще ниже и составляет всего 26% и только 43% руководителей обеспокоены кибербезопасностью. При этом, 25% компаний считают, что киберпреступность затронет их в ближайшие два года [1].

Исследование, проведенное Национальной федерацией розничной торговли, показало, что около миллиона малых предприятий в год сообщают о том, что они стали жертвами мошенничества [2].

Согласно исследованиям Trustwave, 90% утечек данных выпадают на предприятия мелкорозничной торговли. В отчете по безопасности Trustwave за

2012 год указывается, что в тройку лидеров попали розничная торговля (45%), общепит (24%) и гостиничный бизнес (9%) [3].

Когда клиент покупает кредитную или дебетовую карту, или кассир вводит номер счета, данные поступают в торговую точку (POS). На данном этапе данные очень уязвимы, потому что чаще всего они находятся в текстовом формате (т.е. не зашифрованы). Если данные перехвачены кибер-вором, их можно тиражировать на поддельные карты и использовать для мошеннических целей.

Многие руководитель предприятий считают, что у них есть «безопасная гавань» от ответственности, если они успешно проходят проверку PCI (Payment Card Industry - индустрия платежных карт) [4]. Это просто неверно. Соблюдение PCI не гарантирует безопасность данных пользователей платежных систем, а только обеспечивает необходимый минимум защиты для получения доступа к банковской системе при осуществлении торговых операций.

Злоумышленники используют различные типы вредоносных программ для кражи данных держателей карт, в том числе регистраторы ключей, анализаторы пакетов и скреперов памяти [5].

Данные карты обычно зашифровываются только в тот момент, когда POS-система отправляет их в банк-эквайринг. До этого момента ответственность за сохранность данных лежит на владельце торговой точки. Кибер-воры знают это, и используют эту уязвимость для захвата незашифрованных данных еще на этапе их обработки в локальных сетях торговых точек. Если злоумышленники могут получить доступ к POS-системе, они могут установить вредоносное программное обеспечение (вредоносное ПО), которое копирует информацию об учетных записях клиентов. Это в конечном счете повлечет утечку данных и финансовые потери, как для клиентов, так и для бизнеса [6].

Для управления POS-сетями, сегодня успешно внедряются системы администрирования POS-устройств. Такие системы позволяют:

- Вести учет имеющихся POS-устройств и их конфигурации.
- Удаленно обновлять ПО на POS-устройствах.
- Удаленно конфигурировать параметры работы POS-устройств.
- Удаленно доставлять ключи безопасности по защищенным каналам. При этом, отдельно выделяется задача доставки первого ключа в устройство (мастер ключа, под которым, в дальнейшем, передаются все остальные ключи).

Наиболее распространенными из подобных систем являются: First Data [7], Networks POS [8], TransLink.iQ [9], а также решения компании INETCO для мониторинга POS [10]. Большинство из подобных систем ограничиваются только возможностью удаленного обновления и конфигурирования POS-устройств. В некоторые системах, таких как TransLink.iQ и система мониторинга INETCO, реализованы функции мониторинга POS-сетей в реальном времени. Однако, весь мониторинг в этих системах сводится к мониторингу аппаратных ресурсов, нагрузки на сеть передачи данных, а также отображению интегральных оценок по осуществленным транзакциям (количество и скорость обработки).

Сегодня, на рынке не существует систем, способных осуществлять сбор и отображение информации в реальном времени о критических параметрах

безопасности функционирования POS-устройств. Перечень всех необходимых параметров можно найти в стандарте PA-DSS Payment Application Data Security Standard - стандарт безопасности данных платежных приложений). Соблюдения требований этого стандарта позволяет минимизировать риски компрометации данных. Следовательно, актуальной является задача реализации сервиса мониторинга POS-сетей, позволяющего осуществлять контроль за выполнением требований PA-DSS в реальном времени.

2. Требования к системе контроля функционирования POS-сетей в реальном времени

Стандарт безопасности данных в индустрии платежных карт PCI DSS был принят в 2004 году для обеспечения единых требований безопасности при передаче, хранении и обработки данных в электронной коммерции.

С января 2014 года все торговые организации должны руководствоваться рекомендациями PCI DSS 3.0, которая имеет 12 требований, состоящих из более чем 400 элементов и подэлементов контроля безопасности [11]. Стандарт безопасности PCI DSS представляет собой совокупность требований по обеспечению безопасности данных о держателях платёжных карт, которые передаются, хранятся и обрабатываются в информационных инфраструктурах организаций.

Согласно отчету о совместимости PCI Verizon от 2015 года, почти 80% всех компаний не проходят промежуточную оценку соответствия PCI, оставаясь уязвимыми перед кибератаками [12].

Прохождение аудита подтверждает, что компания руководствуется лучшими отраслевыми практиками для защиты от нарушения данных. Однако соответствие PCI - когда оно действительно достигнуто и поддерживается - не означает абсолютную безопасность. Более того, подавляющее большинство торговых организаций не соответствуют всем 12 требованиям PCI DSS полностью. Этот набор рекомендаций по обеспечению безопасности данных призван помочь бизнесу уменьшить количество уязвимостей и снизить риск, но это не означает, что риска нет и не защищает от ответственности в случае утечки данных. Существует родственный PCI DSS стандарт безопасности платежных приложений — Payment Card Industry Payment Application — Data Security Standard (PCI PA-DSS). Производители программного обеспечения, участвующего в обработке платежных транзакций, должны сертифицировать приложения по стандарту PA-DSS. По требованиям международных платежных систем Visa и MasterCard все торгово-сервисные предприятия (англ. Merchant) и поставщики услуг начиная с 1 июля 2012 года должны использовать только сертифицированные по стандарту PA-DSS платежные приложения. Контроль выполнения этого требования возложен на банки-эквайеры.

Стандарт PA-DSS распространяется на поставщиков приложений и иных разработчиков приложений, которые хранят, обрабатывают или передают данные держателей карт и (или) критичные аутентификационные данные (см. табл. 1).

Таблица 1. Данные платежных карт (Account Data)

Данные держателя карты	Критичные аутентификационные данные
– Основной номер держателя карты (PAN) – Имя держателя карты – Дата истечения срока действия карты – Сервисный код	– Полные данные дорожки магнитной полосы или ее эквивалент на чипе – CAV2/CVC2/CVV2/CID – PIN/PIN-блоки

Процесс контроля сохранности данных должен сопровождать все действия по обслуживанию платежных операции:

1. двусторонние платежные функции (авторизация и расчет);
2. ввод и вывод;
3. сбойные ситуации;
4. интерфейсы и подключения к другим файлам, системам и (или) платежным приложениям или компонентам приложений;
5. все потоки данных держателей карт;
6. механизмы шифрования;
7. механизмы аутентификации.

Для контроля выполнения требований PA-DSS необходимо разработать сервис мониторинга POS-сетей, который должен соответствовать следующим основным требованиям:

1. Все события должны отражаться в реальном времени. Это позволит быстро обнаружить и устранить проблему в безопасности.
2. Сервис мониторинга должен обеспечивать централизованное отображение всех событий (основание: PA-DSS 3.2 пункт 4.4).
3. Сервис мониторинга должен регистрировать как минимум следующие параметры для каждого события: идентификатор пользователя; тип события; дата и время; успешным или неуспешным было событие; источник события; идентификатор или название данных, системного компонента или ресурса (основание: PA-DSS 3.2 пункт 4.3).
4. Информирование о всех ошибках, произошедших на POS-устройствах.

Сервис мониторинг должен отображать как параметры работы самих POS-устройств (POS-терминалы, торговые системы и др.), так и параметры их окружения. Для успешного управления большим количеством устройств, наиболее эффективным решением является интеграция сервиса мониторинга, с системами администрирования POS-сетей. При этом сервис мониторинга должен выполнять следующие функции:

1. Информирование о статусе работы POS-устройства: время последнего сообщения, полученного от устройства; информирование о том, что устройство неактивно; время простоя устройства.
2. Информирование об изменении на устройстве пароля для доступа к системе администрирования.

3. Информирование об изменении статуса выполнения заданий, назначаемых для конкретного устройства в системе администрирования.
4. Информирование о ходе загрузки ПО на устройство.
5. Информирование о результатах установки ПО на устройство.
6. Информирование о несоответствии версии ПО устройства, версии последнего задания на обновление ПО устройства в системе администрирования. Подобный факт может свидетельствовать о смене ПО на устройстве третьей стороной и, следовательно, наличие рисков осуществления мошенничества на данном устройстве.
7. Информирование о ходе применения новой конфигурации на устройство.
8. Информирование о результатах применения новой конфигурации на устройство.
9. Информирование о несоответствии версии конфигурации устройства, версии последнего задания на обновление конфигурации устройства в системе администрирования. Подобный факт может свидетельствовать о внесение изменений в параметры работы устройств третьей стороной и, следовательно, наличие рисков осуществления мошенничества на данном устройстве.
10. Информирование о результатах обновления ключей безопасности на устройстве.
11. Информирование о ручном вводе ключа безопасности на устройстве (тип ключа, индекс ключа, контрольная сумма ключа).

Наиболее узким местом в обеспечении безопасности данных клиента в POS-сетях, являются платежные терминалы. Именно через них в систему поступают чистые данные платежных карт. Несмотря на то, что платежные терминалы достаточно серьезно защищены с помощью их физической архитектуре и операционной системы, PA-DSS предъявляет строгие требования к приложениям разворачиваемых на терминале. Следовательно, система мониторинга, должна осуществлять контроль за этими требованиями:

1. По истечению срока хранения данных держателей карт в терминале, сервисом мониторинга должно отображаться соответствующее сообщение. К сообщению должен прилагаться список тех мест, где хранятся небезопасные данные, а также инструкция для их удаления (основание: PA-DSS 3.2 пункт 2.1).
2. Информировать о каждом доступе / истории доступа / количество обращений в секцию ключей /к данным держателей карт / о неуспешных попытках логического доступа / о других действиях, совершенных с использованием административных полномочий платежного приложения (основание: PA-DSS 3.2 пункты 2.4, 4.1, 4.2).
3. Информировать о использовании и изменении механизмов идентификации и аутентификации приложения (включая, помимо прочего, создание новых учетных записей, расширение прав доступа и т. д.), а также всех изменениях, добавлениях, удалениях учетных

записей с правами суперпользователя (“root”) или администратора (основание: PA-DSS 3.2 пункт 4.2.5).

4. Информировать о инициализации, остановки или приостановки ведения журналов аудита (основание: PA-DSS 3.2 пункт 4.2.6).
5. Информировать о создании и удалении объектов системного уровня приложением либо посредством его функций (основание: PA-DSS 3.2 пункт 4.2.7).
6. Информировать об истекшем сроке ключей шифрования на терминале (основание: PA-DSS 3.2 пункт 2.5.4).
7. Информировать о наличии скомпрометированных ключей на устройстве (основание: PA-DSS 3.2 пункт 2.5.5).
8. Информировать оператора, о том, что на терминале существует пользователь, пароль которого не менялся более 90 дней (основание: PA-DSS 3.2 пункт 3.1.7).
9. Информировать о том, если учетная запись пользователя блокируется в результате непрекращающихся попыток подбора пароля / о том, если пользователь разблокирован и кем / о том, что пользователь ввел неверный пароль / о том, что пользователь запросил повторную активацию и одобрена она или нет и кем (основание: PA-DSS 3.2 пункт 3.1.10).

Описанная функциональность, позволит контролировать все действия, осуществляемые POS-устройствами данной сети в реальном времени. При этом будет сведен к минимуму риск утечки данных при помощи изменения параметров работы POS-устройств третьей стороной.

На рисунке 1, представлена концептуальная диаграмма компонентов системы мониторинга безопасности POS-сети.

3. Заключение

Проблема предотвращения мошенничества в сфере электронных платежей становится все более актуальной в связи с ростом безналичных расчетов и появлением новых угроз и способов несанкционированного доступа к информации. Для совершенствования систем защиты информации в процессе осуществления платежных операций все более актуальной становится решение задачи, мониторинга и обнаружения угроз в реальном времени. Одним из решений данной задачи может стать внедрение системы администрирования POS-сетей и ее интеграция с сервисом мониторинга. Сервис мониторинга, функциональные требования которого, описаны в данной работе, позволит оперативно обнаруживать угрозы безопасности личных данных пользователей, совершающих безналичный расчет при помощи платежных терминалов и эффективно их устранять.

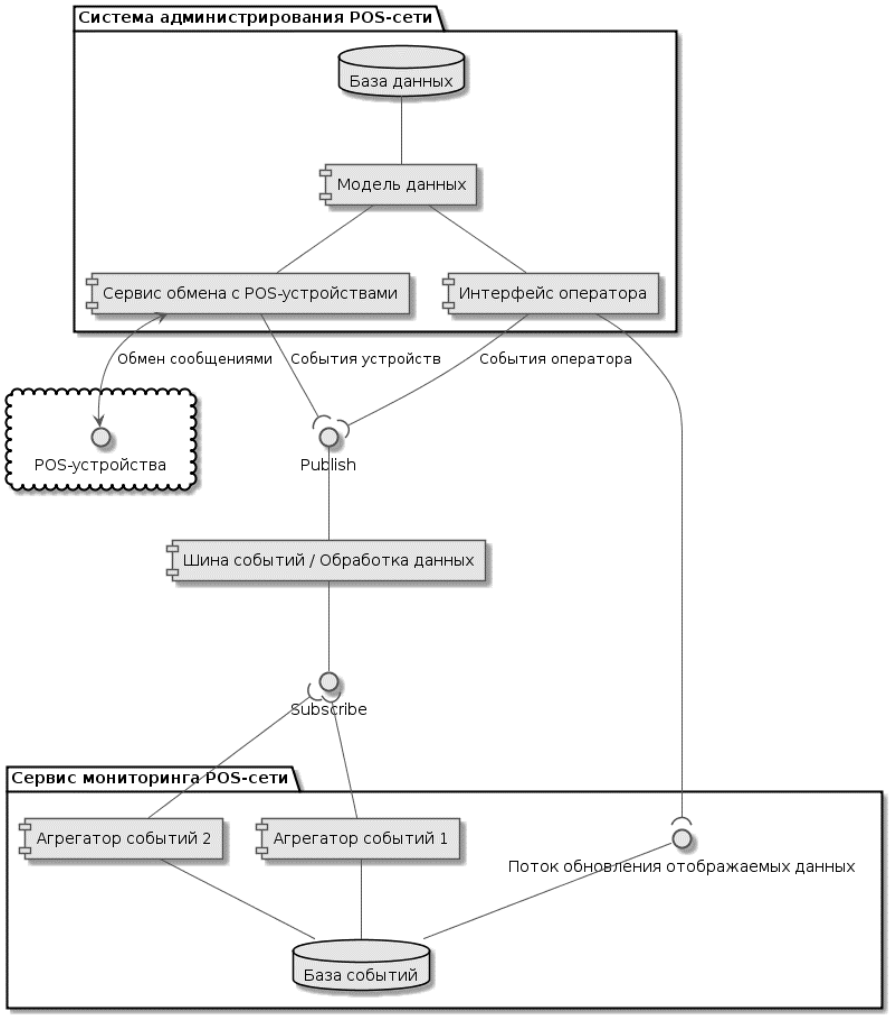

Рис. 1. Диаграмма компонентов системы мониторинга безопасности POS-сети

Предложенная концепция системы мониторинга безопасности функционирования POS-сетей в реальном времени предназначена для интеграции с системами администрирования POS-сетей. При успешном внедрении подобной системы предполагается существенное уменьшение рисков, связанных с эксплуатацией POS-оборудования, а также своевременный оперативный анализ текущего состояния сети.

Литература

[1] PricewaterhouseCoopers LLP. “2016 Global Economic Crime Survey”. 2016.
[2] National Retail Federation. “Retail Small Business Survey”. 2010.
[3] Trustwave SpiderLabs. “Trustwave Global Security Report 2012”. 2012.
[4] The PCI Security Standards. URL: https://www.pcisecuritystandards.org/pci_security/ (дата обращения: 01.05.2017).
[5] First Data Corporation. “What You Can Do to Prevent a Payment Card Data Breach”. 2014.
[6] Verizon. “Verizon 2014 PCI Compliance Report”. 2014.
[7] First Data. URL: https://www.firstdata.com/en_ie/home.html (дата обращения: 01.05.2017).
[8] NetworksPOS. URL: http://networkspos.com (дата обращения: 01.05.2017).
[9] TransLink.iQ - Transaction processing and POS terminal network management. URL: http://www.bs2.lt/en/software/iq-family-products/translinkiq/ (дата обращения: 01.05.2017).
[10] INETCO Solutions for POS Monitoring and Retail Application Management. URL: https://www.inetco.com/solutions/pos-retail-applications/ (дата обращения: 01.05.2017).
[11] Thor Olavsrud, “5 Ways to Improve Your PCI Compliance Program,” CIO magazine, February 27, 2014.
[12] Verizon. “Verizon 2015 PCI Compliance Report”. 2015.

The concept of security monitoring system for the real time POS networks functioning

D. V. Kozlov, N. P. Sadovnikova
Volgograd State University

The article analyzes the current situation in the detection fraud and cyberthreats prevention. It describes the existing solutions for fraud management and prevention in POS networks. The concept of monitoring the security of the real time POS networks functioning in is proposed. The article also describes the main functional requirements of the monitoring service and its integration with the system of POS networks administration.

Keywords: fraud analysis, proactive monitoring, information system, POS-networks