DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.1.1

УДК 004.056.5
ББК 68.823

СИСТЕМА БЕЗОПАСНОСТИ POS-СЕТИ

Дмитрий Викторович Козлов

Аспирант кафедры САПР и ПК,
Волгоградский государственный технический университет
1mrdiko4@gmail.com
просп. Ленина, 28, 400033 г. Волгоград, Российская Федерация

Наталья Петровна Садовникова

Профессор кафедры информационной безопасности,
Волгоградский государственный университет
sadovnikova.natalia@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. В работе рассматривается подход к построению системы безопасности POS-сетей. Кроме того, дана концепция системы мониторинга и анализа угроз в POS-сетях и предложена ее архитектура.

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

Объем безналичных расчетов с каждым годом увеличивается. Соответственно растет количество POS-устройства и операций по их использованию и обслуживанию. Система электронных платежей представляет собой сложную структуру с множеством различных подсистем и элементов, распределенных на большой территории и требующих серьезных ресурсов для поддержки их функционального состояния. Мошенничество в сфере электронных платежей становится все более серьезной проблемой из-за роста безналичных платежей и появления новых угроз и методов несанкционированного доступа к информации POS-сетей. Защита информации в процессе совершения

платежных операций требует более жесткого контроля и определения угроз в оперативном режиме. Скорость определения и реагирования на киберугрозу зависит от того, сможет ли система предотвратить утечку критически важной информации. В неблагоприятном случае потери от мошеннической атаки растут экспоненциально с течением времени.

Основным стандартом информационной безопасности платежных карт является PCI DSS, который был принят в 2004 г. [4]. В стандарте представлены единые требования безопасности при передаче, хранении и обработки данных о держателях платежных карт. в информационных инфраструктурах организаций. Компаниям присваивается определенный уровень в зависимости от количества транзакций. Каждому уровню соответствует свой набор требований, которые должны выполняться. Стандарт предусматривает проведение ежегодных аудиторских проверок компаний, а также ежеквартальные сканирования сетей.

Стандарт безопасности платежных приложений Payment Card Industry Payment Application – Data Security Standard (PCIPA-DSS) предназначен для производителей программного обеспечения, участвующего в обработке платежных транзакций.

Большинство компаний не проходят оценку соответствия существующим стандартам и не могут считаться защищенными от кибератак, но даже полное соответствие требованиям PCI DSS и PA-DSS не означает абсолютную безопасность. Pos-устройствадостаточно серьезно защищены на уровне физической архитектуры и операционной системы, но существует потенциальная возможность несанкционированного доступа к данным через приложения, которые взаимодействуют с терминалом.

В связи с этим существует необходимость создания комплексной системы безопасности основанной на мониторинге и анализе событий POS-системы в режиме реального времени.

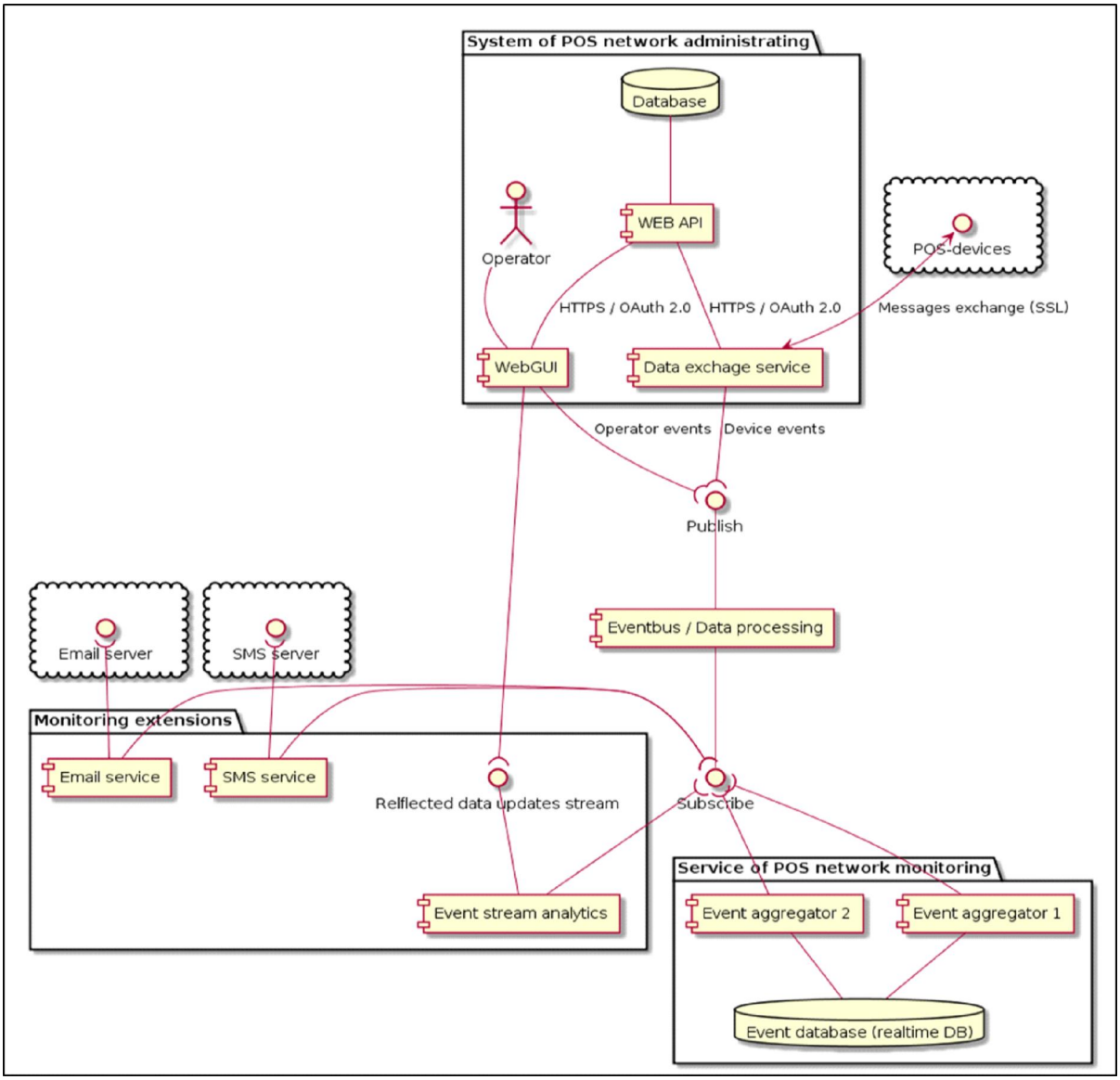
Прежде всего необходимо отметить, что контроль безопасности данных должен сопровождать все процессы, связанные с обслуживанием платежных операции:ввод и вывод информации, регистрация и обработка информации о сбоях, организация взаимодействия с платежными приложениями, шифрование, аутентификацию и пр.

Система безопасности должна быть интегрирована с системой администрирования POS-сети [2]. Для этого необходимо реализовать функции: оповещения операторов об инцидентах, зафиксированных в процессе работы POS-сети, анализа поведения пользователей и др. [5–7]. Система безопасности должна позволять добавлять новые типы анализируемых инцидентов и позволять оператору анализировать состояние сети в реальном времени с учетом всех возможных взаимодействий между ее структурными элементам. Кроме того, необходимо обеспечить высокую производительность системы состоящей из большого количества элементов (в районе 5–10 тысяч) и эффективный способ их отображения в общей структуре POS-сети [1–2].

На рисунке представлена архитектура системы безопасности POS-сети. Оператор системы администрирования получает всю необходимую информацию об объекте мониторинга (POS-оборудование, его состояние, конфигурацию и выполняемые им действия) в режиме онлайн. В то же время оператор получает всю необходимую информацию от самого устройства и других объектов, взаимодействующих с устройством.

Каждая операция, выполняемая устройством или выполняемая на устройстве, регистрируется и доставляется оператору в режиме реального времени. Собранная информация анализируется на наличие инцидентов, указывающих на наличие угрозы безопасности для системы.

Инциденты ранжируются по степени угрозы, и в соответствие с этим, определяются действия по их обработке. Это может быть информирование оператора о событии, отправка уведомлений, полная или частичная блокировка определенных функций (как отдельного устройства или всей системы) и т. д.



Архитектура системы безопасности POS-сети

СПИСОК ЛИТЕРАТУРЫ

1. Выбор способа отображения сети POS-устройств для построения эффективной системы мониторинга / Д. В. Козлов, Н. П. Садовникова, Л. В. Дружинина, Д. В. Петрова // Управление развитием крупномасштабных систем (MLSD'2018) : материалы Одиннадцатой Международной конференции, 1–3 окт. 2018 г., Москва, Россия. В двух томах. Т. II / под общ. ред. С. Н. Васильева, А. Д. Цвиркуна. – М. : ИПУ РАН, 2018. – С. 404–406.

2. Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ (ред. от 27.12.2019) : (с изм. и доп., вступ. в силу с 01.02.2020). – Электрон. текстовые дан. – Режим доступа: http://ivo.garant.ru/#/document/12125267/paragraph/1/highlight/кодекс российской федерации об административных правонарушениях от 3012 2001 n 195-фз:3. – Загл. с экрана.

3. Козлов, Д. В. Концепция системы контроля безопасности функционирования POS-сетей в реальном времени / Д. В. Козлов, Н. П. Садовникова // Информационное общество: образование, наука, культура и технологии будущего. – 2017. – № 1. – С. 44–51.

4. Стандарт безопасности платежных приложений (PA-DSS), версия 3.0.

5. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – Электрон. текстовые дан. – Режим доступа: http://ivo.garant.ru/#/document/12148555/paragraph/3471/doclist/0/selflink/0/highlight/самоубийство интернет:0. – Загл. с экрана.

6. RU (домен). – Электрон. дан. – Режим доступа: http://www.tadviser.ru/index.php/Статья:.Ru_(домен).

7. 78 % населения страны: как Интернет проникает в Россию. – Электрон. дан. – Режим доступа: https://www.gazeta.ru/tech/2019/09/18/12658993/mediascope.shtml. – Загл. с экрана.

REFERENCES

1. Kozlov D.V., Sadovnikova N.P., Druzhinina L.V., Petrova D.V. Vybor sposoba otobrazheniya seti POS-ustroistv dlya postroeniya effektivnoi sistemy monitoringa [Choosing how to Display a Network of POS Devices to Build an Effective Monitoring System]. Vasileva S.N., Cvirkuna A.D., eds. *Upravlenie razvitiem krupnomasshtabnykh sistem (MLSD'2018) Materialy odinnadtsatoy mezhdunarodnoy konferentsii. V 2 tomakh. Tom 2* [Management of the Development of Large-Scale Systems (MLSD' 2018). Proceedings of the Eleventh International Conference, October 1–3, 2018, Moscow, Russia. In Two Volumes. Vol. II]. Moscow, 2018, pp. 404-406.

2. *Kodeks Rossiyskoy Federatsii ob administrativnykh pravonarushenijakh» ot 30.12.2001 no. 195-FZ (red. ot 27.12.2019) (s izm. i dop., vstup. v silu s 1.02.2020)* ["Code of the Russian Federation on Administrative Offenses" Dated December 30, 2001 N 195-FZ (As Amended on December 27, 2019) (with amendments and add., intro. effective from 1.02.2020)]. URL: http://ivo.garant.ru/#/document/12125267/paragraph/1/highlight/kodeks rossijskoj federacii ob administrativnyh pravonarushenijah ot 30 12 2001 n 195-fz:3.

3. Kozlov D.V., Sadovnikova N.P. Kontseptsiya sistemy kontrolia bezopasnosti funktsionirovaniya POS-setey v realnom vremeni [The Concept of a Control System of Safety of Functioning of POS Networks in Real Time]. *Informatsyonnoe obshchestvo: obrazovanie, nauka, kultura i tekhnologii budushchego*, 2017, no.1, pp. 44-51.

4. *Standart bezopasnosti platezhnykh prilozhenij (PA-DSS), versija 3.0* [The Security Standards for Payment Applications (PA-DSS), Version 3.0].

5. *Federalnyj zakon ot 27 iyulya 2006 g. № 149-FZ "Ob informatsii, informatsyonnykh tekhnologiyakh i o zashchite informatsii"* [Federal Law of July 27, 2006 no. 149-FZ "About Information, Information Technologies and Information Protection"]. URL: http://ivo.garant.ru/#/document/12148555/paragraph/3471/doclist/0/selflink/0/highlight/samoubijstvo internet:0.

6. *RU (domen)* [RU (Domain)]. URL: http://www.tadviser.ru/index.php/Stat'ja:.Ru_(domen).

7. *78 % naseleniya strany: kak Internet pronikaet v Rossiyu* [78% of the Country's Population: how the Internet Gets into Russia]. URL: https://www.gazeta.ru/tech/2019/09/18/12658993/mediascope.shtml.

SECURITY SYSTEM OF POS-NETWORK

Dmitriy V. Kozlov

Postgraduate Student, CAD Department,
Volgograd State Technical University
1mrdiko4@gmail.com
Prosp. Lenina, 28, 400005 Volgograd, Russian Federation

Natalia P. Sadovnikova

Professor, Information Security Department,
Volgograd State University
sadovnikova.natalia@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. The volume of non-cash payments increases every year. Accordingly, the number of POS devices and operations for their use and maintenance is growing. The electronic payment system is a complex structure with many different subsystems and elements distributed over a large territory and requiring significant resources to support their functional state. Fraud in the field of electronic payments is becoming an increasingly serious problem due to the growth of non-cash payments and the emergence of new threats and methods of

unauthorized access to information in POS networks. Information protection in the process of making payment transactions requires tighter control and identification of threats in the online mode. The speed of detecting and responding to cyber threats depends on whether the system can prevent critical information from leaking. In an adverse case losses from a fraudulent attack grow exponentially over time.

The work studies the existing technologies for implementing the system of security control over functioning of POS networks in real time and analyzes them in detail. Besides, the concept of the system of monitoring and analysis of threats in POS networks is given, and its architecture is offered.

Key words: POS-networks, information security, monitoring, SIEM-system, analysis of threats.