УДК 004 **Информационные технологии**

Кокимбаев Темирлан Байгалыйулы, *студент, Казахский национальный университет имени аль-Фараби, Казахстан, г. Алматы*

Сауанова Клара Тагаевна, *кандидат технических наук, и.о. доцента, Казахстан, г. Алматы*

РАЗРАБОТКА СИСТЕМЫ НЕПРЕРЫВНОГО МОНИТОРИНГА СЕРВИСОВ ОРГАНИЗАЦИИ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ

Аннотация: Сегодня ИТ-организации сталкиваются с беспрецедентной проблемой обеспечения безопасности и оптимизации ИТ-инфраструктуры, которые усложняются год за годом. Ввиду того, что в больших организациях подразделениям информационной безопасности становится тяжело контролировать все изменения, появляются системы непрерывного мониторинга, которые в свою очередь обеспечивают уникальный подход к сетевой безопасности и управлению уязвимостями. Это позволит заранее выявить и устранять потенциальные уязвимости до того, как они перерастут в инциденты информационной безопасности.

В связи с этим, в этой статье будут описаны ключевые моменты для разработки системы непрерывного мониторинга.

Ключевые слова: сеть интернет, непрерывный мониторинг безопасности**,** разработка системы.

Abstract: Today, IT organizations are faced with an unprecedented challenge of securing and optimizing their IT infrastructure, which is becoming more complex year after year. As IT security teams find it difficult to control all changes in large organizations, continuous monitoring systems are emerging, which in turn provide a unique approach to network security and vulnerability management. This will allow

potential vulnerabilities to be identified and addressed in advance before they escalate into information security incidents.

In this regard, this article will describe the key points for developing a continuous monitoring system.

Key words: Internet, continuous security monitoring, system development.

Непрерывный мониторинг безопасности (CSM) — это подход к анализу угроз, который автоматизирует мониторинг средств управления информационной безопасностью, уязвимостей и других киберугроз для поддержки решений по управлению рисками организации.

Непрерывный мониторинг является важной частью процесса управления рисками. Кроме того, общая архитектура безопасности организации и связанная с ней ИС безопасности контролируют обеспечение того, чтобы процессы во всей организации находились на приемлемом уровне риска, независимо от любых изменений. Своевременная, актуальная и точная информация очень важна, особенно когда ресурсы ограничены и организациям необходимо расставлять приоритеты в своих усилиях [1].

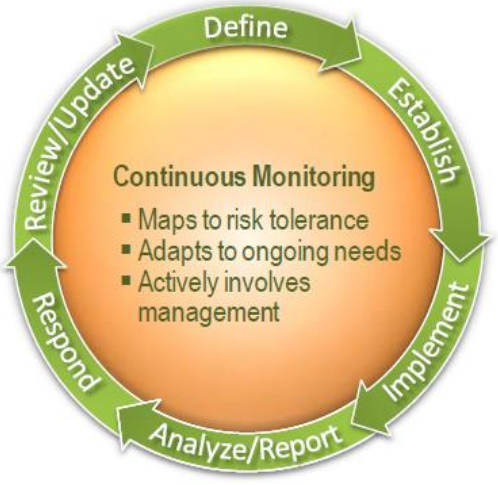

Рисунок 1 – Процессы непрерывного мониторинга

Чтобы лучше реагировать на новые угрозы и уязвимости, архитектуры безопасности организаций, возможности оперативной безопасности и процессы управления всегда развиваются. Непрерывный мониторинг регулярно

пересматривается на предмет соответствия, и при необходимости, пересматривается для повышения прозрачности активов и осведомленности об уязвимостях. Это позволяет управлять безопасностью информационной инфраструктуры организации на основе дополнительных данных и повышать стабильность организации [2].

Мониторинг на организационном уровне не может быть эффективно осуществлен только с помощью ручных процессов или только с помощью автоматизированных процессов. Если используются ручные процессы, они будут повторены и протестированы для обеспечения последовательной реализации. Использование автоматизированных процессов, включая автоматизированные средства поддержки (сканеры уязвимостей, сетевые сканеры), может сделать процесс непрерывного мониторинга экономически эффективным, последовательным и эффективным.

Система будет написана на языке Java с использованием Spring framework.

Архитектура приложения будет выглядеть следующем образом:

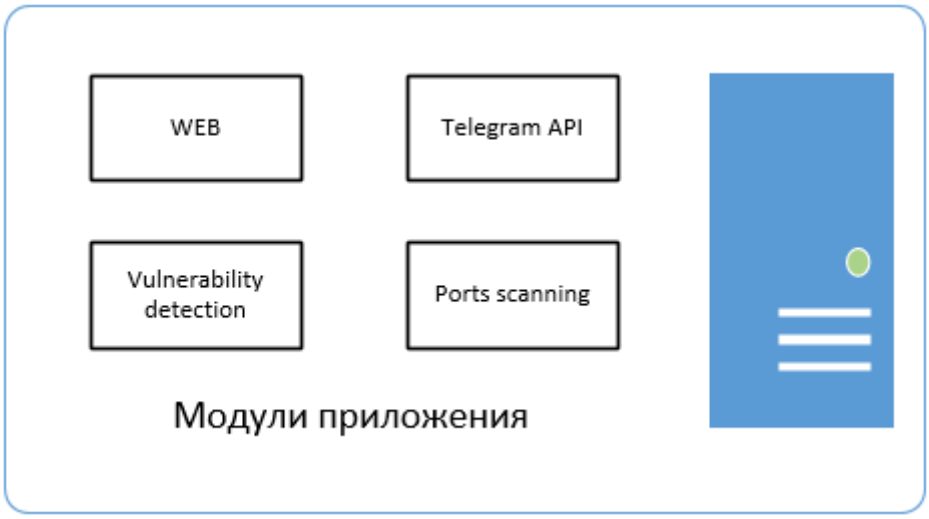

Рисунок 2 – Архитектура приложения

Приложение будет развернута на CentOS и будет состоят из 4 модулей:

1. Модуль Telegram – бота.
2. Модуль сканирования портов на уровне сети внешних сервисов организации.
3. Web модуль.

4. Модуль выявления уязвимостей.

Модуль сканирования портов на уровне сети внешних сервисов организации

Функционал данного модуля будет обеспечивать сканирование внешних портов организации. Вся информация по открытым портам будет отправляться в БД для последующего анализа и рассылки уведомлений для бизнес владельцев [3].

Web модуль

В данном модуле будет реализована возможность мониторинга открытых портов и уязвимостей посредством веб-приложения. Архитектура веб-приложения будет построена по принципу MVC.

Модуль выявления уязвимостей

Функционал данного модуля будет обеспечивать сканирование внешних сервисов на выявления различных типов уязвимостей. Информация по наличии уязвимостей будет хранится в БД для последующего анализа и рассылки уведомлений для бизнес владельцев [4].

Модуль работы с Telegram – ботом

Для работы с Telegram-ботом, использована библиотека - Telegram Bot Java Library. Целью данного модуля – является управление системой посредством мессенджера Telegram. В Telegram – боте будет реализована возможность запуска сканирование и получение результатов. Также будет настроен “таймер”, по которому будут приходить уведомления о состояние открытых портов и уязвимостях во внешних сервисах организации.

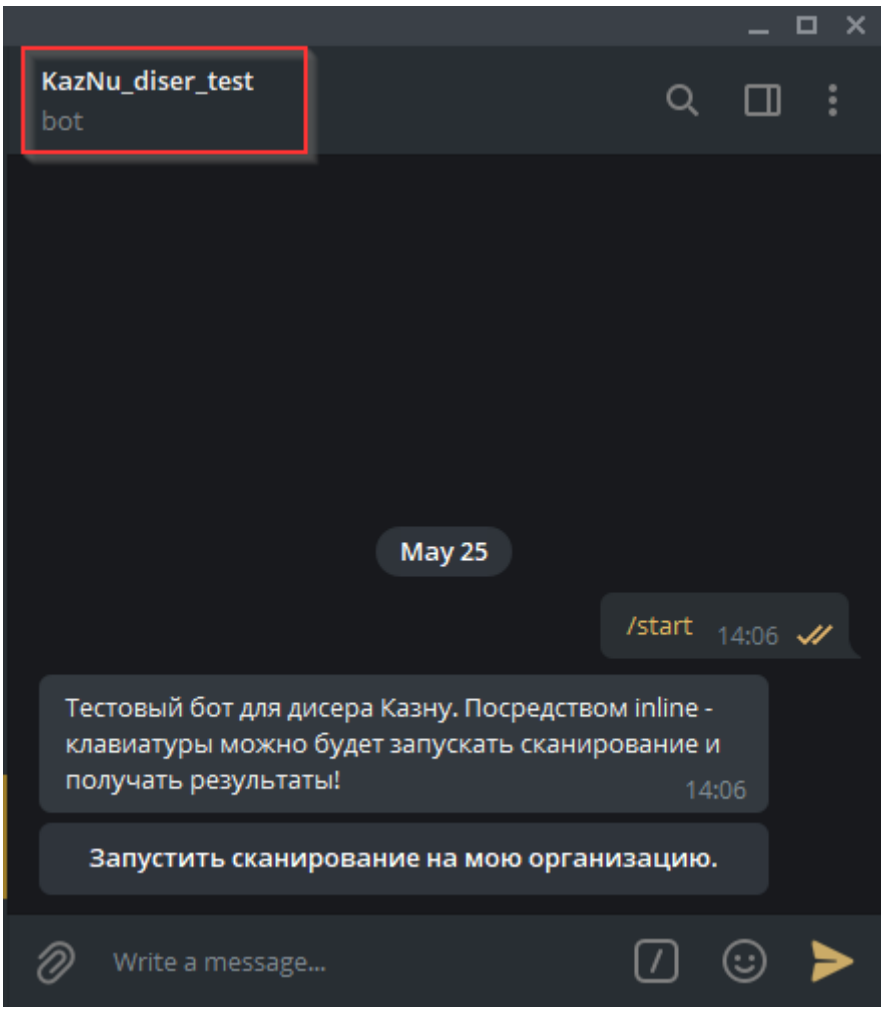

Рисунок 3 – Тестовый запуск бота

Библиографический список:

1. Dafydd Stuttard, Marcus Pinto- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition (PET-CON 2009.1). - Wiley; 2nd edition (дата обращения 27. 09. 2011).

2. Ruiz-Martinez, A. A survey on solutions and main free tools for privacy enhancing Web communications [Text] / A Ruiz-Martinez // Journal of Network and Computer Applications. - 2012. - Vol. 35, iss. 5. - P. 1473-1492.

3. Peter Kim - The Hacker Playbook 2: Practical Guide To Penetration Testing - CreateSpace Independent Publishing Platform (дата обращения 20. 06. 2015).

4. Paco Hope, Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast 1st Edition - O'Reilly Media; 1st edition (дата обращения 27.10.2008).