УДК 004.056

СОВМЕЩЕНИЕ МЕТОДОЛОГИЙ МЕНЕДЖМЕНТА И МОНИТОРИНГА ВНЕШНЕЙ ПОВЕРХНОСТИ АТАКИ ДЛЯ ЭФФЕКТИВНОГО УПРАВЛЕНИЯ КИБЕРРИСКАМИ

Дмитриева И.Н. (СПбГУТ им. проф. М. А. Бонч-Бруевича)
Научный руководитель – кандидат технических наук Миняев А.А.
(СПбГУТ им. проф. М. А. Бонч-Бруевича)

Введение. В условиях цифровой трансформации и сопутствующего экспоненциального роста сетевой инфраструктуры владельцы крупных корпораций стремительно расширяют свое присутствие в Интернете. В связи с соответствующим ростом цифровых активов внедрение практик результативной кибербезопасности становится критически важным [1]. Атаки на инфраструктуру начинаются с выявленных уязвимых точек входа, расположенных на внешней поверхности. Управление Внешней поверхностью атаки (ВПА) — это многоэтапный процесс непрерывного детектирования, мониторинга и управления цифровыми активами, доступными извне и подключенными к Интернету, с целью выявления потенциальных векторов атак и принятия мер по снижению рисков. Проектирование и внедрение методологий бизнес-менеджмента в сочетании с подходами для управления ВПА позволит обеспечить защиту конфиденциальных данных и гарантировать надежную защиту внешнего периметра, подвергающихся успешным кибератакам. В настоящей работе рассматриваются методологии менеджмента при управлении ВПА, основные компоненты этого процесса, включая выбранные инструменты, а также преимущества, которые позволит предоставить организациям в условиях цифровой среды будущего.

Основная часть. В условиях многоэтапных тщательно продуманных кибератак и сложных киберугроз, мониторинг цифрового периметра и эффективное управление киберрисками становится приоритетом для обеспечения кибербезопасности. Существующие методологии менеджмента бизнес-процессов и IT-процессов предоставляют структурированный подход к управлению ресурсами и процессами, однако, часто не учитывают специфические аспекты мониторинга и управления ВПА [3]. Данная работа закладывает эксперимент, в рамках которого удается совместить методологии менеджмента с инструментами мониторинга активов внешней поверхности атаки. Эксперимент служит теоретическим базисом для создания комплексного подхода к управлению и мониторингу ВПА. В качестве фундамента для построения системы мониторинга рассматриваются open-source инструменты, позволяющие сформировать технологический универсальный инструмент (англ. Multi-tool) как экономически эффективное и масштабируемое решение [1].

Целью исследования является разработка концепта модели управления ВПА, интегрирующей лучшие практики менеджмента IT- и бизнес-процессов и современные инструменты мониторинга, для повышения эффективности выявления и устранения уязвимостей, а также снижения киберрисков, связанных с актуальными угрозами.

Внедрение методологий менеджмента для мониторинга внешней поверхности атаки (ВПА) может столкнуться с несколькими основными вызовами, которые будут рассмотрены в перспективных исследованиях [2]:

1. Низкая осведомленность об активах, входящих в состав инфраструктуры. Динамически расширяющаяся инфраструктура может привести к недостаточному покрытию поверхности инструментами мониторинга, что затрудняет выявление уязвимостей и потенциальных точек входа для злоумышленников [3].
2. Высокая сложность интеграции разнородных и многофункциональных инструментов. Большое количество разрозненных инструментов и источников телеметрии усложняет процесс анализа и расследования инцидентов [3].
3. Требования к автоматизации процессов при реагировании на потенциально критичные

периметральные инциденты. Многие процессы в SOC остаются неавтоматизированными, что может привести к ошибкам при экспертной оценке угроз.
4. Управление теневыми активами. Растущее количество неконтролируемых цифровых активов, которые могут быть уязвимыми. Каждый актив требует тщательной инвентаризации и мониторинга, что представляет собой заведомо сложную задачу.
5. Успешное внедрение Security Awareness. Уровень осведомленности сотрудников о правилах кибербезопасности и общая культура безопасности в организации зачастую существенно влияют на безопасность компании [4].
6. Нелинейные и быстрые изменения процессов. Внедрение новых технологий и методологий может вызвать сопротивление со стороны сотрудников, что требует эффективного управления изменениями и качественного обучения пользователей [4].

Выводы. Совместное использование методологий управления процессами и современных инструментов для мониторинга активов формирует синергию, которая значительно повышает эффективность мониторинга и контроля внешней поверхностью атаки. Это достигается за счет оптимизации процессов практиками современного менеджмента, улучшения аналитики, а также повышения уровня осведомленности участников бизнес-процессов организации. Интеграция подходов является важным шагом для обеспечения надежной защиты ИТ-инфраструктуры от внешних угроз и реализации киберрисков.

Список использованных источников:

1. Исследование инструментов кибербразведки по открытым источникам для оценки доступности информационных активов организации: вып. квалиф. раб. на соискание степ. бкл. по спец. 10.03.01 / И. Н. Дмитриева; научный руководитель А. А. Миняев; Санкт-Петербургский гос. ун-т телекоммуникаций им. проф. М. А. Бонч-Бруевича, Кафедра ЗСС. – 2023. – 105 с. URL: http://lib.sut.ru/jirbis2_spbgut
2. Проведение анализа угроз при мониторинге внешней поверхности атаки объектов КИИ / "Научный аспект №6-2024" - Информ. Технологии URL: https://na-journal.ru/6-2024-informacionnye-tekhnologii/13607-provedenie-analiza-ugroz-pri-monitoringe-vneshnei-poverhnosti-ataki-obektov-kii
3. Greeshma M. R., Adarsh Nair Mastering Information Security Compliance Management. - First published: August 2023 изд. - Birmingham: Published by Packt Publishing Ltd, 2023. - 193 с.
4. Katharine Jarmul Practical Data Privacy. Enhancing Privacy and Security in Data. - April 2023: First Edition изд. - Printed in the United States of America.: Published by O’Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, 2023. - 345 с.

Дмитриева И.Н. (автор) Подпись

Миняев А.А. (научный руководитель) Подпись