УДК 004.056

В.Д. САЛЬНИКОВА

Национальный исследовательский ядерный университет «МИФИ», Москва

АВТОМАТИЗАЦИЯ ПРОЦЕССА ПОВЫШЕНИЯ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Целью статьи является обзор существующих автоматизированных решений, направленных на автоматизацию процесса повышения осведомленности работников в области информационной безопасности с учетом особенностей каждого решения.

Введение

По данным российской компании BI.ZONE с начала 2024 года общее количество фишинга выросло в 2,5 раза: как показывает опыт киберразведки BI.ZONE с электронного письма начинается 68% целевых атак [1]. На этом фоне эксперты считают особенно важным обучать персонал базовым принципам цифровой гигиены. Помимо этого, низкая стоимость и доступность инструментов организации фишинговых атак делает данный метод самым популярным у киберпреступников. Стоимость готовых фишинговых наборов в даркнете (DarkNet) варьируется от 30 до 1000 долл [2].

Постановка задачи

Для минимизации возникновения инцидентов и рисков, вызванных низкой осведомленностью, необходимо внедрять и оптимизировать процесс повышения осведомленности работников по вопросам информационной безопасности [3]. Оптимизация процессов возможна с помощью их автоматизации. Ниже представлен перечень отечественных и зарубежных решений для автоматизации процесса повышения осведомленности работников в вопросах информационной безопасности.

Для данного исследования были выбраны 6 решений (отечественных и зарубежных), на основе анализа открытых источников:

1. Kaspersky ASAP
2. МегаФон Security Awareness
3. Антифишинг
4. Phishman
5. Deteact Awareness
6. Syssoft Security Awareness

Пути решения проблемы

Для выбора оптимального автоматизированного средства повышения осведомленности, были определены следующие блок-факторы: облачное иностранное решение; отсутствие возможности легальной покупки лицензионного решения на территории РФ; возможность прохождения обучения менее, чем за год; продукт находится на рынке более 3-х лет; отсутствие возможности имитации фишинговых рассылок.

По итогу отбора из вышеуказанных решений с применением блок-факторов, были определены «лидирующие» решения:

1. Антифишинг 0 блок-факторов
2. Phishman 0 блок-факторов

Наиболее оптимальное решение под конкретную организацию определяется при детальном расчете KPI для каждого решения.

Заключение

В исследовании рассмотрены 6 комплексных решений автоматизации процесса повышения осведомленности работников в вопросах информационной безопасности. По итогам были определены два оптимальных решения, но выбор единственного сервиса возможен только при детальном исследовании каждой системы и определения KPI по конкретным запросам организаций.

Список литературы

1. BI.ZONE: общее количество фишинговых писем выросло в 2,5 раза с начала года // habr.com [Электронный ресурс] – Режим доступа: https://habr.com/ru/news/750234/ (дата обращения: 10.12.2023).

2. Сколько стоит организовать целевую кибератаку (Advanced Persistent Threat, APT) // www.anti-malware.ru [Электронный ресурс] – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/How-much-does-it-cost-to-organize-APT#part23 (дата обращения: 12.11.2023).

3. Корпоративный фишинг и спам в 2022 году: всё чаще атакуют HR-специалистов и бухгалтеров // www.kaspersky.ru [Электронный ресурс] – Режим доступа: https://www.kaspersky.ru/about/press-releases/2022_korporativnyj-fishing-i-spam-v-2022-godu-vsyo-chashe-atakuyut-hr-specialistov-i-buhgalterov (дата обращения: 30.11.2023).