От повышения осведомленности – к культуре безопасности

Андрей Жаркевич, *редактор ООО "Антифишинг"*
Виктор Сердюк, *генеральный директор АО "ДиалогНаука"*

В настоящее время у большинства успешных компьютерных атак есть одна общая черта: первичным вектором в них становятся не уязвимости в системах, а использование человеческого фактора, связанного с сотрудниками, подрядчиками или клиентами организаций. В основе таких атак лежат не технические методы, а социальная инженерия. В этой статье поговорим о том, что нужно для создания надежного "человеческого файрвола" и как в этом может помочь платформа "Антифишинг".

Воздействуя на слабые места людей с помощью психологических приемов, преступники убеждают сотрудников компаний выполнить нужные им действия. Вот лишь несколько примеров успешных атак:

1. 7 мая 2021 г. произошла кибератака на оператора крупнейшего в США топливопровода Colonial Pipeline. Злоумышленники использовали фишинговую схему для получения доступа к компьютерным системам компании: один из сотрудников перешел по ссылке в фишинговом письме и заразил информационные системы компании. В итоге компания была вынуждена заплатить выкуп в размере $5 млн, но при этом получила неработающий инструмент для расшифровки данных.

2. В декабре 2020 г. в Интернете были выставлены на продажу данные 16 тыс. клиентов инвесткомпании "Фридом Финанс", в том числе квалифицированных инвесторов. В свободном доступе оказались сведения о 50 из них: паспортные данные, адреса, данные о счетах в банках. Злоумышленники атаковали сегмент внутренней сети компании и похитили часть информации с локальных машин ряда сотрудников брокера в РФ.

3. В середине мая 2021 г. Национальная служба здравоохранения Ирландии (Health Service Executive, HSE) стала жертвой атаки шифровальщика Conti. Злоумышленники находились в сети HSE более двух недель и похитили 700 Гбайт файлов, включая конфиденциальную информацию о пациентах и сотрудниках, контракты, финансовые отчеты, платежные ведомости и многое другое. За расшифровку и удаление похищенных данных преступники требовали выкуп в размере $19,9 млн.

В таких условиях затраты на формирование навыков и культуры безопасного поведения сотрудников должны стать обязательной частью бюджета информационной безопасности.

О платформе

"Антифишинг" – платформа для формирования навыков противодействия всем видам атак на персонал компании. В состав платформы входят обучающие курсы, тесты, а также специальная методология и технологии для имитации некоторых видов атак. Это позволяет практически полностью автоматизировать работу HR- и ИБ-подразделений в части проведения и контроля результатов обучения, а также тренировки сотрудников в условиях, максимально приближенных к реальным инцидентам ИБ.

Как ведут себя люди во время атак

По данным исследований "Антифишинга", собранных в отчете о защищенности сотрудников в 2020 г., в среднем 37% людей открывают письма мошенников, а 79% из них совершают затем опасные для компании действия: вводят свои логины и пароли на сторонних сайтах, открывают потенциально опасные вложения или даже скачивают и устанавливают вредоносное ПО, замаскированное под обновления системы.

Почему обучения недостаточно

Очевидным способом решения проблемы человеческого фактора чаще всего становится проведение обучения. По этому пути идет значительная часть компаний во всем мире, но ожидаемого результата они не достигают. После года обучения лишь 9% сотрудников[1] не допускает ошибок в условиях имитации реальных атак.

Работа с сотрудниками, состоящая только из обучения на курсах, практически не влияет на их поведение во время атаки злоумышленников. Не удалось выявить корреляции между декларируемым качеством курсов, их дизайном, геймификацией и действиями сотрудников на практике в условиях имитированных атак.

Эти результаты отражают закон забывания Г. Эббингауза, в соответствии с которым обучение эффективно только в течение трех дней, а затем 90% материала забывается, если он не закреплен на практике.

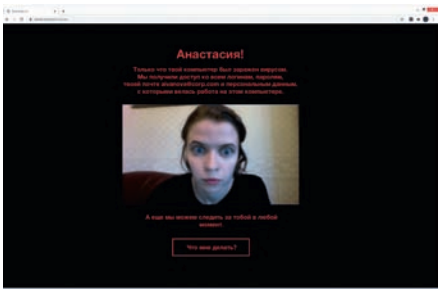
6 шагов к созданию культуры кибербезопасности

В комплект поставки платформы "Антифишинг" входят методические рекомендации по организации обучения и тренировок для персонала компании. Приведем наиболее важные шаги, выполнение которых, с нашей точки зрения, позволит укрепить корпоративную киберкультуру и выработать у сотрудников навыки безопасного поведения.

1. *https://antiphish.ru/news/report2020*

Шаг 1. Оцените ситуацию

Прежде чем принимать меры, нужно выяснить текущий уровень киберграмотности. Сделать это, например, можно посредством имитации некоторых видов атак, шаблоны которых поставляются вместе с платформой и адаптируются под каждую организацию. Имитированная атака полностью аналогична атаке мошенников, за исключением того, что вместо вредоносного кода сотрудник получает моментальную обратную связь с объяснением, что он сделал не так и как нужно действовать в подобной ситуации.



Платформа позволяет наглядно просмотреть, как действовали сотрудники при получении фишинговых писем, сколько человек открыли письмо, сколько запустили вложение или перешли по ссылке. На основе собранных данных система показывает, как сотрудники компании справляются с имитацией реальных хакерских атак.

Реализованная в "Антифишинге" система визуализации дает актуальную и объективную информацию об уровне подготовки пользователей – сотрудников компании, с позиций ИБ.

Шаг 2. Организуйте регулярное обучение

В составе "Антифишинга" имеется система электронного обучения, поддерживающая стандартный для LMS-систем формат SCORM. Это позволяет не только использовать входящие в комплект поставки адаптированные курсы "Антифишинга", но и добавлять уже имеющиеся в компании обучающие материалы, чтобы управлять ими из единого интерфейса.

Платформа интегрируется в корпоративную ИТ-инфраструктуру и получает данные о сотрудниках и организационной структуре из Active Directory или другой LDAP-совместимой службы каталогов, а также из кадровых систем. Это избавляет от рутинных операций по синхронизации "Антифишинга" с базой данных пользователей и позволяет всегда иметь актуальную картину состояния ИБ организации.

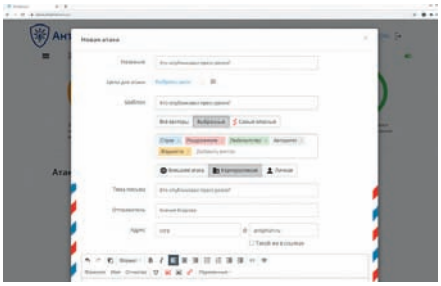
В составе платформы имеется планировщик, который автоматизирует назначение пользователям обучающих курсов и контроль их прохождения. Он позволяет назначать курсы для групп сотрудников по времени или по событиям-триггерам. Например, при появлении в системе нового пользователя можно назначить ему прохождение базового курса по информационной безопасности. Уведомление о назначении курсов направляется пользователям по электронной почте.

Система контролирует прохождение обучения, и администраторы системы в любой момент могут получить отчет о состоянии дел.

Шаг 3. Проведите серию имитированных атак

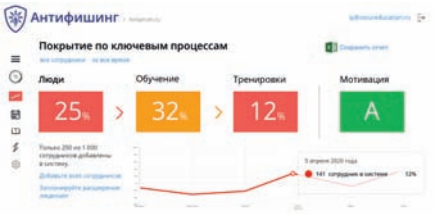
В составе платформы имеется модуль для управления имитированными атаками. Он позволяет отправлять пользователям письма в соответствии с разработанными экспертами "Антифишинга" шаблонами, чтобы выработать у сотрудников навык распознавания фишинговых атак и закрепить полученные знания на практике.

Вы можете предоставить сотрудникам простой и наглядный инструмент, с помощью которого они смогут выявить атаку и сообщить о ней в службу безопасности, например такой, как плагин "Антифишинга" для Microsoft Outlook:



Шаг 4. Проанализируйте результаты

Оценить результаты сотрудников можно с помощью встроенных показателей покрытия и других визуальных представлений:



Шаг 5. Выделите группы риска

Разные категории сотрудников имеют различные приоритеты с точки зрения рисков и процессов безопасности. Не всегда эти приоритеты отражаются организационной структурой: часто сотрудники из разных подразделений и отделов должны быть объединены в единую параллельную структуру, которая имеет свой приоритет и позволяет вести процессы особенным способом.

Для решения этой задачи и визуального представления разных категорий сотрудников в "Антифишинге" появилась возможность группировать сотрудников – объединять их без привязки к организационной структуре.

Сотрудников, которые представляют наибольший риск с точки зрения процессов безопасности, рекомендуется помещать в группу наиболее высокого приоритета.

Шаг 6. Повторите и автоматизируйте процессы

Закрепление усвоенного материала и фиксация выработанных навыков требуют регулярного повторения. Для этого можно воспользоваться встроенным в систему планировщиком, который дает возможность назначить повторное прохождение курсов с заданной периодичностью.

Проведение имитированных атак также следует повторять, используя шаблоны с разными вариантами психологического воздействия. Это обеспечивает формирование закрепления устойчивости к различным видам атак и обеспечивает высокий уровень бдительности у пользователей.

Группировка и все последующие действия с сотрудниками могут быть автоматизированы встроенными средствами платформы, а также через API "Антифишинга".

Из вышеизложенного можно сделать следующие выводы:

1. Устойчивость компании к компьютерным атакам определяется не только функциональностью технических средств защиты, но и уровнем киберграмотности людей.
2. Теоретические знания о кибератаках не помогают в случае реальных инцидентов ИБ.
3. Чтобы обеспечить эффективную защиту, необходимо обучить сотрудников принципам информационной безопасности и сформировать правильные навыки и поведение на тренингах/тренировках, которые проводятся в условиях, максимально приближенных к настоящим атакам.
4. Систематическое повторение цикла "обучение – тренировка – контроль" обеспечивает формирование долговременного тренда на закрепление навыков безопасного поведения и формирование сильной культуры безопасности в организации. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru