Почему кампании по повышению уровня безопасности проваливаются

Контролируемые фишинговые атаки оказывают гораздо большее влияние

Исследования и общественное мнение о кампаниях по обеспечению безопасности и о том, почему они проваливаются, сводят проблему к недостатку участия руководства. Они предполагают, что стратегия компании неверна, руководители не увлечены ею, цели бизнеса и безопасности не совпадают, или что политики были неэффективными ...

Эти причины безусловно, имеют смысл, но на самом деле не отражают «человеческий» элемент. Кампании по повышению безопасности проваливаются, потому что они не связаны с вашими сотрудниками. Проще говоря, никто не думает, что люди будут настолько равнодушны. Существует ложная уверенность в том, что такие типы атак происходят с другими организациями или с другими людьми, и люди, которые не справляются с атаками социальной инженерии, должны быть недалекими. Разве не так?

Общество часто изображает жертв таких видов преступлений как некомпетентных. По моему опыту, этих людей дразнят коллеги, которые просто довольны, что это случилось не с ними.

Правда же состоит в том, что ошибки случаются, иногда люди не останавливаются и не думают, но никто не может быть непогрешимым для изощренных типов атак, которые, к сожалению, становятся все более распространенными.

Недостаток обслуживания клиентов

Ваш персонал хорошо обучен и стремится быть полезным — это присуще тому, как компании хотят, чтобы сотрудники вели себя. Предугадывать потребности клиентов до того, как они узнают, что у них есть эти потребности, является важным навыком, который весь персонал, работающий с клиентами, развивает за годы работы. Большинство крупных организаций выживают не только благодаря своей продукции, но и по услугам, которые они предоставляют вместе с ними. Спрашивать клиента почти неслыханно; ведь клиент всегда прав, верно? Хорошее обслуживание клиентов является ценным товаром для вашей организации, но оно также может быть опорой для злоумышленника.

Что поставлено на карту?

Кампании по повышению безопасности, основанные на бесконечных слайдах или плакатах PowerPoint в ванных комнатах и на кухне вашего офиса, являются пассивной рекламой. Это скучные идеи, которые мало что могут сделать, чтобы заинтересовать ваших сотрудников. Все слишком распространенные попытки применить юмор к сценарию только преуменьшают серьезность того, чем может грозить организации такое нарушение. Непосредственное нарушение, которое может вызвать некорректное поведение, и количество денег, которое может быть потеряно, может быть катастрофическим. Это также необходимо учитывать перед психологическим и культурным воздействием, которое оно может оказать на ваш бизнес.

В конце концов, если электронная почта была подделана, чтобы выглядеть так, как будто она пришла с внутренней учетной записи электронной почты, внезапно общение перестает быть священным. Культура, над которой вы так усердно трудились, разрушается, как если бы дом был ограблен.

Лучший способ избежать такого — это предотвратить подобные атаки. В конце концов, мы уже знаем, что кампании по повышению уровня безопасности являются в лучшем случае липкой,

вернее прилипчивой информацией, а в худшем - всего лишь средством обескураживания людей или использования юмора для унижения жертв таких нападений.

Неосведомленность о безопасности

Если вы загрузили эту статью, вы сначала проверили, какой тип файла вы загружали? Вы всегда так делаете? Если вы работаете в сфере безопасности, я надеюсь, что ответ - да, конечно! А теперь вопрос, сколько из ваших коллег, друзей и членов семьи делают так же? Знают ли они, что означают буквы после точки?

Для того чтобы система безопасности работала, необходимо выполнить две ключевые вещи:

- **Образование**
    - Образование — это не то же самое, что паранойя, хотя здоровое чувство паранойи жизненно важно. Сотрудники должны научиться задавать вопросы обо всем, что требует от них перехода по ссылке или открытия вложения. Простые вещи, такие как разница между HTTP и HTTPS в браузере, должны быть общеизвестны в вашей организации. С точки зрения бизнеса фишинговые атаки также должны быть включены в планы аварийного восстановления или обеспечения непрерывности бизнеса, которые также должны быть доступны для сотрудников.
- **Осознание / Сроки**
    - Это может показаться тривиальным, в конце концов, но на самом деле, повышение осведомленности не так легко осуществить. Кроме того, решающее значение имеет время. Плакат на стене на кухне, пока я готовлю себе чашку чая, исчезнет из моей головы к тому времени, когда я вернусь за свой стол, пробираясь сквозь кучу электронных писем, требующих моего немедленного внимания. Осведомленность практически равна нулю. Я получаю электронное письмо с сообщением о том, что мои данные для входа в систему скоро истекают, я нажимаю на ссылку, ввожу свои данные и ничего не вспоминаю об этом, когда происходит ошибка. Мало ли я понимаю, что я только что скомпрометировал свой аккаунт – и, если что-то кажется ненадежным, я слишком стесняюсь об этом сказать.

Есть несколько ключевых областей, которые необходимо рассмотреть под эгидой «Обучение осведомленности в области безопасности». Некоторые из них, такие как четкие политики и политики обработки данных, должны быть частью внутренних процессов. Другие, такие как осведомленность о фишинг-атаках, гораздо сложнее для понимания, так как они не обязательно думают об обучении, которое они прошли, когда они читают свои электронные письма. В этом случае сроки являются проблемой. Крайне важно включить безопасность в практику работы вашего бизнеса, чтобы она стала частью обычной практики бизнеса.

Осведомленность о безопасности - культурный сдвиг

Кампании, как и проекты, по определению заканчиваются. Осведомленность о безопасности должна быть интегрирована в бизнес так, чтобы она стала обычной частью бизнеса, а не чем-то, что было зарегистрировано, а затем забыто. Лучший способ обучить людей - заставить их думать. Мир рекламы имеет многомиллионные бюджеты, и даже тогда сколько из них действительно останутся с вами? Компании просто не могут позволить себе роскошь маркетинга идеи фишинг-атак: у большинства из них нет на это бюджета, и шансы на успех даже в краткосрочной перспективе не очень высоки.

В индустрии безопасности широко известно, что человеческий фактор чаще всего является одним из самых слабых звеньев. Менталитет обновления до последней версии или применения патча является распространенным и логичным способом просмотра проблем - и ИТ-сообщество полно

очень логичных и умных людей. Однако человеческий фактор или более мягкая сторона ИТ-безопасности могут оставаться загадкой.

Чтобы безопасность была предметом рассмотрения, она должна стать частью социальной нормы в вашей организации. Должна существовать культура, которая не пытается обвинять людей, которые совершают ошибки, а вместо этого задает вопросы о том, как и почему произошла ошибка, и ищет способы контроля и механизмы, чтобы она не повторилась в будущем.

Оглянитесь в прошлое

Понимание того, каким типам атак подвержена ваша организация, является первым шагом. Если ваши бизнес-записи касаются инцидентов, то это будет хорошим началом. Извлекая уроки из прошлого, вы можете начать формировать будущее. Если, например, большинство инцидентов — это вирусы, которые были установлены на компьютерах ваших пользователей, то рекомендуется пересмотреть ваше антивирусное программное обеспечение. Также стоит рассмотреть, как произошли эти инциденты.

Точно так же, как вы проверяете внутреннюю реакцию вашего бизнеса на непрерывность бизнеса, вы должны проверять реакцию своих сотрудников на фишинговые атаки. Фишинг — это область, где многие компании подвержены атакам, поэтому контролируемые фишинговые атаки могут быть отличным инструментом. Они могут не только сообщать правлению о потенциальных инцидентах (в разбивке по департаментам или местам), но и сообщать лицам, которые щелкнули по поддельной ссылке, что они были обмануты, создавая большую чувствительность и осведомленность о подозрительных электронных письмах.

Существует ряд подходов, которые в сочетании могут значительно снизить восприимчивость ваших сотрудников к фишинговым атакам:

- Регулярно выполняйте контролируемые фишинговые атаки, чтобы повысить уровень осведомленности о таких опасностях и снизить вероятность того, что сотрудники будут щелкать подозрительные ссылки в сообщениях электронной почты. При регулярном проведении таких проверок сотрудники учатся с подозрением относиться ко всем неожиданным электронным письмам, содержащим ссылки на сторонние веб-сайты.
- Выполните целевое обучение после оценки. Основываясь на данных каждой контролируемой фишинг-атаки, постарайтесь определить тенденции уязвимости в организации. Используйте эти данные для обучения наиболее уязвимых областей бизнеса с помощью обучения безопасности, чтобы максимизировать эффективность ваших бюджетов обучения.
- Просмотрите внутренний ответ после каждой оценки. Определите ключевые области, которые требуют улучшения. Первоначальная атака была обнаружена командой безопасности? Если нет, определите причину этого и устраните ее путем введения / изменения политик и процедур, а также исследуйте технические решения для поддержки идентификации атак, таких как внедрение IDS, IPS или решений для мониторинга электронной почты.

Вывод

Лица, которые не смогли устоять против атак социальной инженерии, не должны рассматриваться как нечто уникальное; им скорее всего просто не повезло. Чтобы понимание безопасности было успешным, оно должно быть внедрено в культуру вашей организации. Без соответствующего контекста сообщения безопасности от постеров или презентаций теряются. Следует поощрять культуру безупречности, чтобы ваши сотрудники могли предупредить вас, если они чувствуют, что была допущена ошибка. Вы можете учиться на собственных ошибках - инциденты могут и должны

регистрироваться - и тогда они могут дать вам представление о типах проблем безопасности, с которыми сталкивается ваша организация.

Образование и осведомленность о безопасности, успешно принятые в вашей организации, могут оказать ощутимое положительное влияние. С точки зрения окупаемости инвестиций, контролируемые фишинговые атаки позволяют увидеть, что количество сотрудников, подверженных этим атакам, уменьшается на 25% и более. Большинство организаций должны увидеть общее снижение восприимчивости не менее чем на 90% после года ежеквартально контролируемых оценок фишинга.

Однако не стоит и переоценивать обучение, ведь привыкнув к вашим шаблонам фишинговых атак, люди просто не будут реагировать на другие. Мало того, они могут считать, что это тоже тренировка, а значит даже если и пропустят фишинговое послание, то ничего страшного.

Кроме того, нужно понимать, что любое обучение это всего лишь одна из технологий безопасности, а не «золотая пилюля». Обеспечить безопасность может лишь сочетание организационных, программно-технических мер и обучения.