Security Awareness- Определение, История, Типы

Security Awareness – осведомленность о безопасности. На мой взгляд это одна из самых важных инвестиций, которые может и должна сделать компания. В данной статье я попробую рассказать все, что на мой взгляд нужно знать, чтобы защитить свой бизнес от растущих угроз.

Определение Security Awareness

Security Awareness – формальный процесс обучения сотрудников вопросам информационной безопасности. Данный процесс включает в себя:

- Программы по обучению сотрудников
- Индивидуальную ответственность за политику безопасности компании
- Меры по аудиту этих усилий
- Очевидно, что первый пункт является основным компонентом программы повышения осведомленности о безопасности, но столь же важно, чтобы сотрудники были подотчетны и были предприняты шаги для оценки эффективности мер безопасности организации.
- Осведомленность о безопасности может быть разбита на четыре этапа:
    - Определение текущего статуса
    - Разработка программы Security Awareness
    - Разворачивание указанной программы для сотрудников
    - Измерение прогресса, достигнутого программой и пересмотр ее при необходимости

Прежде чем начать описывать различные типы осведомленности о безопасности, давайте взглянем на историю, которая привела нас к этому моменту.

Краткая история безопасности

История кибербезопасности длится столько же, сколько и сам Интернет. С самого начала превращения интернета в основной используемый ресурс преступники использовали его в своих интересах.

Один из самых первых примеров этого особого вида преступлений произошел в начале 1980-х годов. Группа, известная как 414 (названная в честь кода их города Милуоки), была арестована за взлом примерно 60 различных компьютеров, включая устройства в Memorial Sloan-Kettering Cancer Center и Los Alamos National Laboratory.

Правительство быстро отреагировало на эту новую угрозу. Были приняты такие законы, как Computer Fraud and Abuse Act, чтобы предотвратить и наказать попытки этих злоумышленников. Также была сформирована группа реагирования на компьютерные инциденты, чтобы исследовать растущее число взломов и потенциальных методов защиты.

Десятилетие закончилось первой признанной версией червя. За атакой первого червя стоял Роберт Моррис. Даже в самом начале эти самораспространяющиеся вирусы были способны к огромным разрушениям. Фактически, он закрыл почти всю Всемирную паутину в то время. Вирус Морриса был также первой версией широко распространенной атаки DoS (отказ в обслуживании).

Эта и последующие атаки представляют интерес, поскольку они послужили толчком для большей части того, что мы сегодня называем кибербезопасностью. В результате были созданы CERT (группы реагирования на компьютерные инциденты). С этой атакой компании начали понимать,

насколько они действительно уязвимы. Примерно в это же время была придумана поговорка, которую мы все время слышим в сообществе кибербезопасности: «Профилактика лучше лечения».

В течение большей части 1990-х годов хакеры продолжали свои атаки, при этом большинство жертв были правительственными учреждениями и огромными транснациональными корпорациями. В конце концов, Интернет не был широко распространенным инструментом на данный момент.

Один из первых примеров взлома, который затронул широкую публику, произошел в 1997 году. Целью была поисковая система Yahoo!, хакеры утверждали, что «логическая бомба» будет взорвана на любом ПК с использованием Yahoo! на Рождество, если известный хакер Кевин Митник не будет освобожден из тюрьмы.

Требование было блефом.

Другой пример произошел в 1998 году; Bureau of Labor Statistics стало жертвой одной из первых версий спама, когда оно получило сотни тысяч информационных запросов.

В результате этой и других кибератак Министерство юстиции США создало National Infrastructure Protection Center. Его миссия состояла в том, чтобы защитить телекоммуникационные, транспортные и технологические системы страны от хакеров.

Подъем современного хакерства

В самом начале 2000-х годов хакерство превратилось в широко распространенную проблему, известную нам сегодня. Опять же, многое из этого обусловлено пропорциональным увеличением целей (например, все больше и больше людей используют Интернет).

В то же время хакерство стало намного проще. Прошли те времена, когда единственные люди, которые могли выполнять эти атаки, имели технические навыки, равные или превосходящие лучших программистов в мире.

Информация о проведении взломов получила широкое распространение. Тот, кто никогда даже не пытался совершить кибератаку, может стать реальной угрозой менее чем за месяц.

В 2005 году хакер по имени Альберт Гонсалес использовал свои способности, чтобы создать преступную организацию хакеров, своего рода цифровую организованную преступность, - чтобы украсть информацию с более чем 45 миллионов платежных карт, выпущенных TJX, американским ритейлером, которому принадлежит TJ Maxx и британская версия, TK Maxx.

Перед тем, как его поймали и приговорили к 20 годам тюремного заключения, отряд Гонсалеса нанес ущерб в размере 265 миллионов долларов.

Безопасность сегодня

Как вы, наверное, хорошо знаете, кибератаки не замедлились. В 2013 году нарушение мер безопасности Target стало еще одним шокирующим напоминанием миру о том, насколько уязвимы даже самые крупные корпорации. Около 40 миллионов клиентов провели дни после Дня благодарения, проверяя свои счета, чтобы узнать, украдены ли у них деньги.

Другая причина, по которой здесь проводится целевая атака, заключается в том, что уровень используемой сложности является еще одной вехой в истории кибербезопасности. В отличие от прямого нападения на TJX, преступники, которые преуспели в Target, знали о важности подхода.

Они выбрали стороннюю компанию, которая поставляла Target решения для отопления и вентиляции.

Хакеры также поняли, что наступил точный момент, когда они должны были нанести удар. Номера кредитных карт присутствовали и не были зашифрованы в памяти системы.

Опять же, это также показало деловому миру, что последствия такой атаки вызовут волнение во всех направлениях. Кибербезопасность теперь является проблемой на уровне совета директоров, так как после кражи генеральный директор Target фактически ушел в отставку.

Типы безопасности

Учитывая вышесказанное, должно быть совершенно ясно, что компании должны серьезно относиться к вопросам безопасности.

Однако все больше и больше хакеров добиваются успеха благодаря фишинговым атакам, направленным на сотрудников компаний.

Нисходящий подход

Одна очень важная особенность осведомленности о безопасности состоит в том, что сотрудники не просто должны знать, какие меры они должны предпринять, и применять их.

Любой человек, от менеджера до руководителя, будет легкой целью, если он не знает о возможности атак и о том, как насколько они могут быть успешны.

Бюджетирование для обеспечения безопасности

Хороший показатель того, серьезно ли компания относится к вопросам безопасности, можно найти в бюджете. Как относятся к осведомленности о безопасности в качестве приоритета в компании? Как это соотносится с другими способами распределения средств?

Если идея вашей компании об осведомленности о безопасности состоит в использовании уведомлений электронной почты, в которых вы время от времени напоминаете людям о возможности атаки, вы должны ожидать, что вскоре станете жертвой подобной атаки.

Необходимо понимать, что осведомленность о безопасности является лишь частью жизнеспособного плана защиты. Другие части будут включать в себя:

- Создание политики безопасности
- Оценка уязвимостей вашей компании
- Инвестирование в технологии безопасности

Однако нет ничего более важного, чем осведомленность о безопасности. Компании должны тратить столько же на эти инвестиции, сколько на программное обеспечение и другие виды технологий безопасности. Ведь ничто из этого не будет даже отдаленно полезным, если ваши люди - легкие цели для фишинговых атак.

Организационная структура, предназначенная для обеспечения безопасности

Необходимо помнить, что Security Awareness жизненно важно, потому что затрагивает всех в компании. Подобно нисходящему подходу, организационная структура, построенная вокруг безопасности, сделает работу каждого проще.

Если это вообще возможно, то у вас должна быть команда людей, которые несут ответственность за реализацию вашей программы обеспечения безопасности. По крайней мере, в вашей организации должен быть человек, который будет отвечать за эту работу.

В противном случае осознание безопасности становится рутинной работой, но никто не воспринимает эту работу всерьез. Команда или лицо, ответственное за обеспечение этой программы должны иметь полную поддержку исполнительной команды.

Создать план и сопутствующую документацию

План для каждой компании будет немного отличаться, но все же будет иметь и общие черты. Особенности вашего плана должны включать некоторые версии следующего:

- Изложение команды осведомленности безопасности и участвующих ролей
- Заявление о миссии программы осведомленности о безопасности, объясняющее ее необходимость
- Календарь мероприятий на весь год, который включает регулярные действия, а не только электронные письма с напоминаниями, предназначенные для того, чтобы сотрудники понимали общие угрозы и какова их роль в их предотвращении.
- Программы для новых сотрудников, которые объясняют программу осведомленности о безопасности и их роли
- Ссылки на процедуры и политики безопасности компании
- Опять же, все эти мероприятия будут немного отличаться в зависимости от конкретной компании, но некоторые общие версии должны присутствовать. Вы не можете позволить себе ошибиться, думая, что киберпреступники так или иначе не затронут вашу организацию.

Использование различных форм СМИ для усиления воздействия

В данной статье несколько раз затрагивалась тема электронных писем с напоминанием о безопасности. Это не значит, что электронная почта — это плохо. Каждый из нас нуждается время от времени в напоминании.

При этом вам следует использовать несколько форм мультимедиа, чтобы сообщения вашей компании об осведомленности о безопасности никогда не игнорировались.

Например, в вашем календаре событий должен быть специалист по безопасности в вашей компании, который выступает перед людьми и объясняет важные темы. Видео также могут быть отправлены по электронной почте. Естественно, при этом могут использоваться тесты. Могут использоваться физические напоминания в офисе. Этот список можно продолжать и продолжать, но суть не в том, чтобы успокаиваться на том, как вы доставляете сообщения об осведомленности о безопасности.

Напоминайте о последних атаках в новостях

Это чрезвычайно важная форма осведомленности о безопасности. Тем не менее, убедитесь, что вы выделяете все виды атак, а не только те, которые распространяются в национальных новостях. Цель этого подхода - показать вашим сотрудникам, насколько распространены эти атаки, как легко можно добиться успеха в вашей компании и каковы последствия этого.

По этой причине не просто выделите истории, которые освещаются в новостях. Сотруднику слишком легко думать: «Да, но мы не цель. Никто не будет беспокоить нас.

Найдите истории о компаниях вашего размера и / или в вашей отрасли. К сожалению, не похоже, что этих инцидентов будет не хватать.

Используйте профессионалов

Если в данный момент у вас нет абсолютно никаких мер по обеспечению безопасности, стоит подумать о том, чтобы воспользоваться услугами профессионала. Они помогут вам начать работу и убедиться, что вы быстро наверстаете упущенное.

Даже если вы вложили средства в политику обеспечения безопасности и другие меры, все равно неплохо время от времени привлекать независимого консультанта, чтобы посмотреть, есть ли области, в которых вы можете улучшить свою работу.

Но если все это так просто и очевидно, почему ж это очень слабо распространено на просторах СНГ?

На самом деле причина очевидна. Это обычная человеческая психология. «Украдут у соседа, у меня нечего». Любимая фраза нашего руководства, впрочем, а только ли руководства: «Нечего нам тут пугать! Вот когда взломают, тогда и будем думать!». Увы, это как в полиции: «Заявления об угрозе убийством не принимаем, когда убьют, тогда и приходите». «Нет трупа, нет проблемы!»

Причём более всего поражает то, что больше угроза, тем меньше на неё реагируют. Наверное, это просто срабатывает защита человеческой психики.

Но все же, что делать? На сегодня обучением в области Security Awareness занимается достаточно много учебных центров. Приводить их в статье я считаю излишним, ведь целью статьи является не реклама, а рассказ о том, что необходимо сделать!