Человеческий фактор в информационной безопасности

Выполнила:
Е.П. Иванова

Г. Холм 2022

Широко признано, что сотрудники организации часто являются слабым звеном в защите своих информационных активов. Информационная безопасность не получила достаточного внимания с точки зрения влияния человеческого фактора.

Человеческий фактор оказывает огромное влияние на успех и неудачу усилий по обеспечению и защите предприятий, услуг, систем и информации. Если безопасность системы упускается разработчиком, ИТ-система становится уязвимой, и может быть эксплуатируемой злоумышленником. Атакующие, используя социальную инженерию, пытаются получить конфиденциальную информацию, нацеливаясь на уязвимости людей — то есть, слабые стороны в организации благодаря особенностям и поведению людей.

Повышенные угрозы информационной технологии привели к новым решениям, ориентированным на технологические средства, в то время как исследования, связанные с человеческим фактором, были ограничены. Организации зачастую игнорируют человеческий фактор. Исследование безопасности от Cisco Systems показало, что пользователи, которые работают дистанционно, все равно будут участвовать в действиях, которые угрожают системе безопасности. Изучение поведения сотрудников показало, что получив подозрительное электронное письмо, 37% не только откроют электронную почту, но и пройдут по ссылке, в то время как 13% откроют прикрепленный файл. Кроме того, после получения обычного письма, 42% переходили по ссылке и предоставляли конфиденциальную информацию, а 30% открывали файл, который предположительно улучшил бы производительность компьютера.

Человеческие факторы

Человеческие и организационные факторы могут быть связаны с технической информационной безопасностью.

Факторов, влияющие на безопасность компьютера делятся на две категории, а именно человеческий фактор и организационный фактор. Человеческие факторы является важнее других факторов. Они делятся на следующие группы:

1. - факторы, которые относятся к управлению, а именно рабочая нагрузка и некачественная работа персонала;
2.- факторы, связанные с конечным пользователем.

1. Недостаток мотивации

Многие организации считают, что сотрудников необходимо мотивировать на безопасное поведение с информационными активами, и руководство должно быть в состоянии определить, что мотивирует их персонал.

2. Недостаток осведомленности

Недостаток осведомленности связан с отсутствием общих знаний об атаках. Общие примеры отсутствия осведомленности могут быть следующими: пользователи не знают, как определить шпионские программы и шпионское ПО и как важно указывать надежный пароль. Они не могут защитить себя от кражи личных данных, а также как контролировать доступ других пользователей к их компьютеру.

3. Убеждение

Общими примерами рискованного убеждения являются следующие: пользователи считают, что установка антивирусного программного обеспечения решает их проблемы по защите информации.

4. Неграмотное пользование технологиями

Даже самая лучшая технология не может преуспеть в решении проблем информационной безопасности без непрерывного человеческого сотрудничества и эффективного использования этой технологии. Общие примеры ненадлежащего использования технология заключается в следующем: создание несанкционированной реконфигурации систем, доступ к паролям других, получение недопустимой информации. Риски в области компьютерной безопасности можно классифицировать несколькими способами: превышение привилегий, ошибки и упущения, отказ в обслуживании, социальная инженерия, несанкционированный доступ, хищение личных данных, фишинг, вредоносные программы и несанкционированные копии.

Пример значимости человеческого фактора в обеспечении безопасности на практике

Результаты внедрения в компании «Почта Банк» системы распознавания лиц, построенной на платформе VisionLabs LUNA.

Биометрические технологии используются «Почта Банком» в процессах аутентификации при доступе персонала банка и партнеров к ресурсам (всего примерно 70 тыс. человек), а также при обслуживании клиентов (которых более 4,5 млн). Охват клиентов — физических лиц стопроцентный.

Среди клиентов — юридических лиц использование распознавания лиц реализуется по желанию (примерно 20% из них отказываются от применения технологии).

В системе задействована база данных с результатами обработки более 10 млн изображений уникальных реальных лиц, которые одновременно используются для обучения самой системы. Один сервер системы в состоянии обрабатывать до 100 обращений в секунду, затрачивая не более 2 секунд на каждое обращение.

Статистика эксплуатации системы за 2016 год:

предотвращено 4,5 тыс. нарушений с использованием одних и тех же фотографий клиентами с разными именами;
остановлено 9,2 тыс. потенциально мошеннических действий — обращений по утерянным или украденным паспортам (в том числе с выявлением мошенников по базе данных системы), ошибок персонала при вводе клиентских данных;
задержано четверо мошенников, пытавшихся использовать поддельные документы;
предотвращено около 600 попыток использования чужих учетных записей.

Заменив в двухфакторной аутентификации подтверждение через передачу одноразовых паролей по SMS, система распознавания лиц позволила за год сэкономить около 3,5 млн рублей.

Внедренная система, по прогнозам, помогла предотвратить потерю от мошенничества примерно в сумме 1,5 млрд рублей.

За тот же период система позволила сэкономить более 15 тыс. часов рабочего времени сотрудников фронт-линии за счет автоматизации процесса аутентификации 46 тыс. клиентов, изменивших в 2016 году те или иные анкетные данные.

Вывод

Существует постоянная битва между хакерами и специалистами по безопасности. К сожалению, непредсказуемость поведения человека может уничтожить самые безопасные информационные системы.

Организации должны развивать и поддерживать культуру, в которой ценят позитивное поведение в области безопасности. Им необходимо привить свою культуру, чтобы безопасность начиналась и заканчивалась каждым человеком, связанным с их инфраструктурой, их бизнесом и их услугами.