УДК 331.108.2, 004.056

УГРОЗЫ КАДРОВОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. СРЕДСТВА БОРЬБЫ С ПРОМЫШЛЕННЫМ ШПИОНАЖЕМ

М.В. Ульянов, Д.О. Ульянова, студенты гр. ИТм-191, I курс
Научный руководитель: В.В. Меркурьев, к.э.н., доцент
Кузбасский государственный технический университет имени Т.Ф. Горбачева, г. Кемерово

Кадровая безопасность - это обеспечение экономической безопасности предприятия за счет снижения рисков и угроз, связанных с недоброкачественной работой персонала, его низкой квалификацией и взаимоотношениями внутри коллектива.

Угрозы кадровой безопасности могут быть внутренними и внешними. Примеры внутренних угроз:

- несоответствующая квалификация сотрудников;
- плохая организация системы управления персоналом;
- низкая организация системы обучения;
- отсутствие системы мотивации;
- ошибки в планировании ресурсов персонала;
- снижение количества рационализаторских предложений и инициатив;
- уход ведущих сотрудников;
- сотрудники отвлечены решением внутренних задач;
- полное отсутствие корпоративная политика;
- не доскональная проверка кандидатов при приеме на работу.

Примеры внешних угроз:

- предложения работы сотрудникам от фирм конкурентов;
- воздействие на сотрудников извне;
- попадание сотрудников в различные виды зависимости;
- инфляционные процессы (невозможно не учитывать при расчете заработной платы и прогнозировании ее динамики).

Добывание сведений через персонал организации

Есть множество способов получения конфиденциальной информации через сотрудников фирмы. Чтобы противодействовать злоумышленнику, необходимо сформировать определенные навыки у сотрудников.

Основной способ получения необходимой информации - сотрудничество работника фирмы со злоумышленником. Работник помогает ему:

- желание отомстить начальству или кому то из коллег, а также из-за увольнения.
- в следствии единого мнения со злоумышленником, а также по причине дружеских либо иных отношений;

- будучи убежденным в необдуманных действиях или безнравственностью руководства фирмы;
- принуждение к сотрудничеству через обман, шантаж, физическое насилие.

Но способ набирающий огромную популярность является использование персонала для неосознанного сотрудничества, т.е. применение социальной инженерии.

Социальная инженерия.

Социальная инженерия - совокупность приёмов, методов и технологий создания такого пространства, условий и обстоятельств, которые максимально эффективно приводят к конкретному необходимому результату, с использованием социологии и психологии

Обучение и повышение осведомленности в области безопасности должны быть сосредоточены на сценариях риска, которые включают человеческий фактор. Дайджест по нарушениям данных Verizon за 2017 год показал, что 90% инцидентов с потерей данных имеют фишинговую или социальную составляющую. Стоимость утечки данных как для крупных, так и для малых и средних предприятий продолжает расти. В дополнение к финансовым потерям необходимо учитывать и репутационные издержки. Недавний опрос PCIpay показал, что пятая часть американских потребителей никогда не возвращается к нарушенным брендам, а опрос RSA показал, что 62% обвиняют компанию в первую очередь в случае нарушения данных, а не хакера.

Компании с процессами аутентификации, брандмауэрами, VPN и программным обеспечением для мониторинга сети по-прежнему широко открыты для атаки, если сотрудник невольно выдает ключевую информацию. Обучение безопасности и осведомленность включает в себя человеческий элемент, жизненно важный для выживания предприятия. Простая социальная инженерная атака, такая как телефонный звонок (вишинг), может иметь разрушительные последствия.

Вишинг-Простой, но опасный вектор атаки социальной инженерии

Вишинг, широко известный как голосовой фишинг или телефонная провокация, быстро становится одним из самых опасных векторов атаки социальной инженерии. Сотрудники отдела обслуживания клиентов, отдела продаж и отдела кадров очень уязвимы для подобных атак.

Обучение и осознание жизненно важны

Инвестиции в образование в области безопасности, обучение и осведомленность жизненно важны для выживания предприятия. Имитированные атаки вишинга являются эффективным способом доступа к вашему предприятию. Ключевые приемы из имитации атак на крупные корпарации:

- звонки более успешны во второй половине дня;
- пятница - самый уязвимый день для сотрудников.

Значение симулированного вишинга очевидно. Только с этими двум приемами предприятие имеет полезную информацию для внедрения улучшений безопасности. Как отметил Крис Хаднаги из DerbyCon "Ваша команда

будет более уязвимой в пятницу.", например, предоставляемый компанией Social-Engineer, LLC, может оказать помощь этими 4 специфическими способами:

- имитированные атаки являются эффективным способом оценки уязвимостей;
- обширная отчетность предоставляет действенные данные об ответах сотрудников на различные сценарии атаки вишинга;
- определите, какие отделы или сотрудники наиболее уязвимы;
- основываясь на результатах оценки вишинга, разработайте непрерывный процесс оценки и обучения для успешной борьбы с атаками вишинга;

Создание культуры безопасности должно быть основной ценностью для любого предприятия. Всего один телефонный звонок может привести к разрушительным последствиям для предприятия. Инвестируйте и внедряйте многоуровневую подготовку и осведомленность в области безопасности. Не упускайте из виду человеческий фактор. Научите сотрудников распознавать угрозы вишинга и реагировать на них.

Произойдет утечка данных. Тем не менее, риск и затраты для вашего предприятия могут быть снижены с помощью эффективного обучения безопасности и осведомленности, которая включает человеческий элемент.

Основной способ защиты от социальной инженерии - это повышения навыков сотрудников. Сотрудники компании должны быть ознакомлены с опасностью раскрытия персональных данных сотрудников и конфиденциальной информации компании, а также о способах предотвращения утечки данных. У каждого сотрудника организации, в зависимости должности, должны быть инструкции, о том какую информацию можно разглашать, а какую строго запрещено. Кроме того, необходимо выделить следующие правила:

- Учетные данные сотрудника- это собственность компании.

При трудоустройстве сотрудникам необходимо разъяснить, что выданные логины и пароли запрещено использовать во вне рабочих целях (на web-сайтах, для личной почты и т.п.), передавать третьим лицам, которые не имеют на это право. Например, сотрудники одного отдела знают учетные данные друг друга для выполнения какой-либо работы.

- Обязательно необходимы при поступлении на работу и регулярные повышения знаний сотрудников в информационной безопасности.

Плановое проведение таких обучений позволит сотрудникам ознакамливаться с новыми методами социальной инженерии и быть готовыми противостоять им, а так же пополнять свои знания по информационной безопасности.

- В обязательном порядке должны быть регламенты и инструкции по информационной безопасности, к которым у сотрудников есть полный доступ.

Например, в регламенте можно прописать, какие действия предпринимать при попытке третьих лиц запросить либо заполучить данные сотрудников.

- На компьютерах сотрудников всегда необходимо иметь актуальное антивирусное программное обеспечение.
- В сети компании необходимо использовать системы криптографической защиты от атак из внешней сети.
- Проведение инструктажа со всеми сотрудниками на тему: «как вести себя с посетителями».

Посетитель всегда должен находиться с кем либо из сотрудников компании. При встрече неизвестного посетителя, сотрудник должен в корректной форме узнать, с какой целью посетитель находится в данном помещении и где его сопровождение. При необходимости сотрудник должен сообщить о неизвестном посетители в службу безопасности.

- Необходимо максимально ограничить права пользователя в системе.

Например, внести ограничение доступа к web-сайтам и запретить использование съемных носителей. В следствии данного ограничения уменьшается риск попадания в локальную сеть организации троянов и других вирусов.

Заключение.

Даже не профессиональный анализ способов получения информации о предприятии показывает, что любому предприятию необходим тщательный отбор кадров. Постоянное обучение в сфере защиты информации и противодействию злоумышленников. Укрепление психологического здоровья каждого сотрудника.

Список литературы:

1. Роберт Чалдини, "Психология влияния".
2. Абрамов Г.В., «Средства методы защиты информации».