Роман СЕМЕНОВ
начальник отдела аудита и консалтинга компании ARinteg

МОЖНО ЛИ ЗАЩИТИТЬСЯ ОТ КИБЕРМОШЕННИКОВ?

Финансовая сфера всегда была привлекательна для различного рода мошенников. Видов мошеннических действий бесконечное множество. Они охватывают собой практически все направления деятельности банков. По-прежнему существуют и вооруженные налеты, и похищение банкоматов с деньгами, и многое другое. Но с появлением компьютеров мы шагнули в эпоху мошеннических действий с применением высоких технологий.

В повседневной жизни конечные потребители могут столкнуться с «ограниченным» набором противоправных действий: мошенничество с пластиковыми картами, хищения денежных средств при эксплуатации банк-клиента, атака на ресурсы компании и т.д.

На заре прихода пластиковых карт на российский рынок, виды хищения денежных средств были достаточно простыми. Как правило, злоумышленники пользовались повальной безграмотностью держателей пластиковых карт, ведь зачастую держатель писал PIN-код на оборотной стороне карты или держал записку с кодом в одном бумажнике с картой. Изъять карту у держателя было делом техники: начиная от банального хищения и заканчивая «ливанской петлей». Чуть позже появились скимминговые устройства для банкоматов, ложные PIN-пады и кардридеры. С появлением сети Интернет в ход пошли фишинговые сайты, различного вида «партнерские программы». Отдельно стоит отметить так называемое «дружеское мошенничество», когда реквизиты карты для оплаты через Интернет тех или иных услуг, или для получения наличных денег в банкоматах, использовал либо родственник, либо хороший знакомый держателя карты.

Но это были «атаки» на конечного держателя пластиковой карты. Ситуация резко изменилась в 2008 году с появлением первой версии банкоматного вируса. Да, он так же воровал данные пластиковых карт вместе с PIN-кодами, но это было только начало. Вирус постоянно преображался, и в итоге он «научился» осуществлять прямую выдачу денежных средств из банкоматов. Данный вид атаки стал более «экономически выгодным» для злоумышленников, нежели хищения денег со счетов владельцев пластиковых карт.

Также за последние несколько лет стали популярны вирусные атаки на системы дистанционного банковского обслуживания. И здесь тоже эволюция шагает огромными шагами. Если вначале злоумышленники пытались получить доступ к банк-клиенту юридических лиц, чтобы в дальнейшем осуществить нелегитимные операции по переводу денежных средств, то сейчас атакуются уже системы непосредственно банков. Если несколько лет назад целью атаки было незамедлительное получение прибыли, то сейчас стоимость самой атаки может значительно превышать финансовую выгоду, полученную в результате реализации. Речь идет о ныне «модных» атаках APT-класса (от англ. *Advanced Persistent Treats*). Это распределенные во времени атаки, которые рано или поздно достигнут результата. В своих действиях злоумышленники применяют абсолютно весь арсенал от DDoS-а до социальной инженерии. Под атакой отказа в обслуживании маскируются реальные проникновения в сеть предприятия, а при помощи социальных сетей изыскиваются способы заражения вирусами компьютеров сотрудников.

К сожалению, уже нельзя говорить о том, отобьется атакованное предприятие или нет. В настоящий момент можно говорить лишь о том, сколько продержится атакуемый объект. Рано или поздно его все равно взломают, и надо признать, что не существует абсолютной безопасности. Да, системы защиты не стоят на месте, но они зачастую вынуждены реагировать на уже сформировавшиеся угрозы. В настоящий момент лишь малая доля производителей вкладывает ресурсы в научные исследования атак, стараясь предугадать то, что может произойти. И во многих случаях время жизни атакуемого объекта зависит от того, насколько квалифицированно настроены системы защиты, насколько грамотно построена эшелонированная оборона. Здесь, безусловно, поможет привлечение внешних ИБ-аудиторов и консультантов, экспертиза которых формировалась в процессе решения полного спектра проблем построения защищенных информационных систем предприятий различной отраслевой принадлежности, различных масштабов бизнеса и различных ИБ-бюджетов.

О КОМПАНИИ

ARinteg имеет многолетний опыт успешных масштабных проектов в крупных российских банках. Среди наших клиентов Внешэкономбанк, Альфа-Банк, Связь-Банк, ВТБ 24, Промсвязьбанк и многие другие. Основные направления деятельности:

- Построение комплексных систем информационной безопасности
- Приведение информационной системы клиента в соответствие с требованиями регулирующих органов Российской Федерации
- Построение современной ИТ-инфраструктуры