Основные сведения о кибератаке на почтовый сервис «Делойта»

6 октября 2017 года

По факту имевшей место кибератаки «Делойт» инициировал проведение проверки с целью оценки масштаба случившегося, определения возможного влияния на клиентов и других заинтересованных лиц, а также принятия соответствующих мер реагирования на киберугрозы. Ниже приведены основные факты относительно данного инцидента.

Злоумышленником были скомпрометированы параметры доступа к учетной записи и, как следствие, был получен доступ к единой платформе облачного почтового сервиса «Делойта». Обнаружив факт несанкционированного доступа к платформе почтового сервиса, мы запустили стандартную комплексную процедуру реагирования на подобные ситуации. Данная процедура подразумевает задействование команды специалистов по кибербезопасности и конфиденциальности как самого «Делойта», так и других компаний (в том числе компании «Мандиант»). Мы привлекли сторонних специалистов для того, чтобы как мы сами, так и наши клиенты и заинтересованные лица могли убедиться в том, что проверка была проведена тщательно и объективно. Командой специалистов были выполнены нижеследующие действия.

- **Незамедлительно были предприняты меры по пресечению и сдерживанию кибератаки.**
- **Была проведена оценка масштаба кибератаки.** Участниками команды были проверены записи в протоколах с целью понимания действий, совершенных злоумышленником на платформе почтового сервиса. Данная информация была использована для реализации мер реагирования на кибератаку.
- **Были определены цели, с которыми злоумышленник совершил несанкционированный вход.** Злоумышленник ставил себе целью осуществить вход на облачную платформу почтового сервиса. Данная система обособлена от других платформ «Делойта», в том числе от платформ, на которых хранятся данные клиентов, результаты совместной работы специалистов «Делойта», проектные технологии и другие необлачные почтовые системы. Действия злоумышленника не оказали влияния на работу ни одной из вышеперечисленных систем. По результатам расследования, проведенного нашими специалистами в области кибербезопасности совместно со сторонними экспертами, стало известно, что злоумышленник, в частности, стремился получить данные по активным параметрам доступа.
- **Была проведена проверка материалов, подвергшихся воздействию со стороны хакера.** Атаке подверглись неструктурированные данные, а именно электронные письма. Путем проведения тщательного анализа протоколов специалистам «Делойта» удалось определить, какие действия были фактически совершены злоумышленником. Было также установлено, что количество электронных сообщений, подвергшихся воздействию со стороны злоумышленника, составило незначительную часть от общего числа электронных сообщений, хранящихся на данной платформе. Мы последовательно проверили все электронные сообщения, попавшие под воздействие со стороны злоумышленника. Данная проверка осуществлялась вручную, без привлечения средств автоматизации, с тщательной оценкой характера информации, содержащейся в каждом электронном сообщении. Благодаря проведению внимательной проверки нами было установлено всего несколько случаев, когда под воздействие злоумышленника могли попасть активные параметры доступа, персональные данные и прочая секретная информация, оказывающая влияние на клиентов.
- **Клиенты, чьи данные попали под воздействие со стороны злоумышленника, были оповещены о кибератаке.** Сотрудники «Делойта» связались с каждым из весьма небольшого числа клиентов, чья информация попала под воздействие со стороны злоумышленника.
- **О кибератаке были уведомлены государственные учреждения.** Сотрудники «Делойта» незамедлительно начали оповещать государственные учреждения об имевшем место инциденте.
- **Были приняты дополнительные целенаправленные меры по дальнейшему повышению общего уровня архитектуры безопасности.** Мы расширили используемую централизованную систему управления привилегированным доступом и завершили развертывание системы многофакторной проверки подлинности, которая в момент кибератаки

находилась в процессе создания. На данный момент все пользователи облачной системы обмена электронными сообщениями, а также пользователи, имеющие повышенный уровень доступа, являются частью нашей системы многофакторной проверки подлинности.

Участниками команды было выявлено нижеследующее.

- **На данный момент у злоумышленника отсутствует доступ к системе «Делойта».** Специалистами «Делойта» при поддержке сторонних экспертов не было обнаружено признаков продолжения действий злоумышленника. Мы предприняли ряд важных мер по пресечению доступа злоумышленника к нашей среде, в том числе блокирование IP-адресов, отключение учетных записей, присвоение новых паролей, а также проведение расширенного мониторинга.
- **Ни экономической деятельности клиентов, ни возможности «Делойта» предоставлять клиентам услуги, ни потребителям ущерб нанесен не был.**

Проведенный нами тщательный анализ, а также постоянные значительные инвестиции в кибербезопасность подтверждают стремление «Делойта» к защите информации своих клиентов и заинтересованных лиц.