KR&P | Адвокатское бюро
Ковалёв, Рязанцев и партнёры

Автор публикации:
Глушаков Виктор Васильевич
(Руководитель практики
частных клиентов, партнер)

ПРАКТИКА ЧАСТНЫХ КЛИЕНТОВ

Оглавление

Хищение конфиденциальной информации, которая хранилась на сервере компании, проверка правоохранителя, в результате которой была потеряна важная информация, контроль трафика и прослушивание телефонных переговоров.
Данные вопросы всё чаще звучат на встречах с клиентами.
В настоящем бюллетене я бы хотел обсудить с Вами вопросы «кибербезопасности» бизнеса и дать некоторые советы, как адвокат, которые, я надеюсь, помогут Вам застраховаться от потенциального риска подвергнуться преступному посягательству.

Челябинск, ноябрь 2016

454091, г. Челябинск, ул.Пушкина, 71,
офис 401, Бизнес центр «Пушкинский»

+7 (351) 245 42 31
+7 (351) 245 42 35

info@k-r-p.ru

https://www.facebook.com/KOVALEV.RYAZANTCEV.PARTNERY/
www.instagram.com/krp_lawfirm

1/ Кибербезопасность: основные зоны риска

ПРАКТИКА ЧАСТНЫХ КЛИЕНТОВ

В настоящее время при хранении и обмене информацией всё большее значение играют высокие технологии. Однако развитие таких технологий приводит не только к положительному, но и к отрицательному прогрессу, который выражается во всё более изощренных способов хищения информации.

Какая информация может понадобиться злоумышленнику?

1. Финансовая информация («пин-коды» карт, пароли и т.д.).
Самый обыденный способ мошенничества – попытка через информацию завладеть вашими деньгами.

2. Информация о сделках.
Например, информация о контрагентах, у которых Вы заказываете товар или которым его продаёте.

3. Конфиденциальная информация (о работниках, о выручке, о контрагентах – базы данных, переписка и т.д.).

Кто может попытаться похитить информацию?
1. Конкуренты
2. Мошенники
3.Правоохранительные органы / спецслужбы.
Самым распространенным пунктом в нашей практике был именно п. 3 – «Правоохранительные органы». Рисковый характер предпринимательской деятельности, в ходе которой правоохранитель всё чаще пытается вмешаться в бизнес-процессы, делает Вашу информацию очень ценным источником сведений, в том числе в отношении третьих лиц.

Факторы риска.

Внешние.
1. Политические мотивы.
2. Популярность брэнда и продуктов.
3. Близость к жертвам атаки (контрагент).
4. Конкуренция.
5. Агрессивная киберсреда (банковская сфера, он-лайн сервисы, он-лайн магазины).
6. Провокационное поведение компании / руководителя, бизнесмена.

Внутренние.
1. Присутствие компании в сети интернет.
2. Количество и доступность офисов.
3. Высокая текучесть кадров (высокий уровень лояльности к работникам).
4. Устаревшие технологии защиты.
5. Наличие легко монетизируемых данных («пин-коды», пароли).

2/ Советы адвоката

ПРАКТИКА ЧАСТНЫХ КЛИЕНТОВ

Основные способы, которыми злоумышленник может получить о Вас информацию.

1). Социальная инженерия. Например, получение информации о логине и пароле от человека в беседе или иным способом (от Вашего офис-менеджера).

2). Почтовая рассылка «фишинговых писем».
Вам на почту приходит письмо. Оно может быть как абсолютно глупым, так и якобы от потенциального делового партнера. Письмо может содержать ссылку, пройдя по которой вы установите на компьютер вредоносную программу. Письмо может содержать файл (это даже может быть документ «word»), открыв который, вы установите на компьютер вредоносную программу.

ВЫВОД – не открывать ссылки и файлы от незнакомых людей. Даже телефонный «прозвон» отправителя может не помочь – грамотные хакеры возьмут трубку, ответят, представятся отправителем, тем самым введя Вас в заблуждение о легальности письма и его вложении.

3). Вай-фай сети. Сидя в кафе, вы можете подключиться к сети «Билайн». Однако от «Билайна» здесь будет только название. По факту вы дадите абсолютный доступ к вашему компьютеру или телефону. **ВЫВОД – подключаться только к известному и проверенному вай-фай.**

4). Казуальный пример.
Хакер садится в здании, где у Вас офис. Раздаёт вай фай с тем же самым названием, что и у вашей корпоративной сети. Руководитель подключается к этой сети – компьютер под контролем у хакера.

5). Скомпрометированная флэшка или иной накопитель информации. Сейчас достаточно вставить зараженную флэшку в USB-порт и вредоносная программа автоматически запустится на компьютере.

ВЫВОД – не использовать незнакомые флэшки и иные накопители информации.

6). Кража пароля.
Самая простая кража – подбор. Если пароль –«12345», то его проще простого украсть.
Никому нельзя говорить логины и пароли. Желательно не хранить их на компьютере.

2/ Советы адвоката

ПРАКТИКА ЧАСТНЫХ КЛИЕНТОВ

7). Потеря телефона или ноутбука.
Утеря того или иного означает сто процентную утечку информации. Решение – зашифровать телефон и ноутбук. Шифрование отличается от кодирования. В этом вопросе лучше проконсультироваться у специалиста.

Активные меры безопасности.

В случае атаки мошенников и конкурентов, при отсутствии незаконного воздействия со стороны правоохранителя.

1. Пароли на всех устройствах.
Телефоны, компьютеры, вход в сетевые хранилища данных и др.

2. Дублировать всю информацию, которая имеется у компании / бизнесмена. Вынести информацию «за корпорацию».
Перенести информацию на внешние жесткие диски, которые хранить не в офисе.
По возможности основные накопители общей информации компании (сервера) хранить не в офисе, либо надежно защитить / спрятать.

3. Не прибегать к работе с «теневым» / пиратским программным обеспечением. Эти программы могут быть опасны.

4. Не заходить с рабочего компьютера на компрометирующие сайты (порно, различные он-лайн браузерные игры и т.д.). Не «загружать» на рабочий компьютер ненужные программы, игры, софт.

При наличии подозрений, что информация может быть необоснованно изъята с использованием «административного ресурса», или что делать, если к Вам пришли люди в масках.

В случае если были соблюдены ранее данные рекомендации, то на предприятии должна быть примерно следующая ситуация:

1. Все компьютеры и телефоны защищены паролем.

2. Сервер не находится в офисе, зашифрован или надежно спрятан.

3. Вся информация будет продублирована на внешних носителях, и потеря текущего сервера с информацией не принесёт вреда.

2/ Советы адвоката

ПРАКТИКА ЧАСТНЫХ КЛИЕНТОВ

Для защиты прав предприятия в продолжение данных мер необходимо:

- назначить ответственного человека, в чьи обязанности будет входить экстренное оповещение руководства, адвоката, и контрагентов о произошедшем. Именно в указанном порядке;

- обязательно вести фиксацию и документирование происходящего (фото-, видео-фиксация);

- нельзя хамить, грубить и оказывать сопротивление государственным органам;

- на требование о представлении пароля, лицо вправе отказать, сославшись на ст. 51 Конституции РФ, без дополнительных комментариев и КАКИХ-ЛИБО последствий.

- вызов адвоката.

В заключении набор «безопасных мес сенджеров», для обмена информацией:

1. «Wickr»;

2. «Aes Crypto»;

3. «Silent Phone».