ОБЩИЕ ВОПРОСЫ [1]

ВАС ВЗЛОМАЛИ?!

Что делать руководству компании?

1 ВЫ МОЖЕТЕ ПОДТВЕРДИТЬ ИНЦИДЕНТ[2]?

Есть ли какие-либо доказательства (артефакты), что у вас инцидент? Если нет, то не стоит тратить время на мероприятия из чек-листа.

2 ОТКУДА ВЫ УЗНАЛИ ОБ ИНЦИДЕНТЕ?

От своих подчиненных, из СМИ, от государственных органов, от ИБ-компании, «ходят слухи»...

3 НАЗНАЧИТЬ ОТВЕТСТВЕННОГО ЗА РАССЛЕДОВАНИЕ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТ

В идеале это должен быть заместитель руководителя организации по вопросам информационной безопасности, CIO (ИТ-директор), CISO (директор по информационной безопасности/ кибербезопасности).

4 НАДЕЛИТЬ ОТВЕТСТВЕННОГО ЗА РАССЛЕДОВАНИЕ И РЕАГИРОВАНИЕ НЕОБХОДИМЫМИ ПОЛНОМОЧИЯМИ И ВЫДЕЛИТЬ НЕОБХОДИМЫЕ РЕСУРСЫ

5 УБЕДИТЕСЬ, ЧТО В МЕСТАХ СОВЕРШЕНИЯ ИНЦИДЕНТА ЕСТЬ НЕОБХОДИМЫЙ ПЕРСОНАЛ

Очень важно, чтобы в расследовании принимали участие не только специалисты по кибербезопасности, но и ИТ-специалисты, без которых эффективное расследование и реагирование невозможно.

6 УТОЧНИТЬ У ОТВЕТСТВЕННОГО, СПОСОБНА ЛИ ЕГО КОМАНДА СВОИМИ СИЛАМИ ПРОВЕСТИ РАССЛЕДОВАНИЕ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТ

Речь не только о технических, но и о юридических аспектах расследования инцидента, сбора доказательной базы и взаимодействия с правоохранительными или регулирующими органами.

7 ПРИНЯТЬ РЕШЕНИЕ О ПРИГЛАШЕНИИ ВНЕШНИХ ЭКСПЕРТОВ ПО РАССЛЕДОВАНИЮ И РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ

8 ОЦЕНИТЬ КРИТИЧНОСТЬ ПОСЛЕДСТВИЙ ДАННОГО ИНЦИДЕНТА

Финансовые, репутационные, юридические риски, а также ущерб жизни и здоровью людей, экологии, культурным ценностям и т. п. Не забудьте оценить последствия не только для своей компании, но и, возможно, для клиентов, партнеров и контрагентов, а также отрасли и страны. Относится ли данный инцидент к недопустимым для вашего бизнеса событиям?

ОБЩИЕ ВОПРОСЫ [1]

9 **ОЦЕНИТЬ, КАКИЕ КРИТИЧЕСКИЕ ДЛЯ БИЗНЕСА СЕРВИСЫ И ПРОЦЕССЫ ПОСТРАДАЛИ В РАМКАХ ИНЦИДЕНТА**

10 **ПРИНЯТЬ РЕШЕНИЕ ОБ ИЗОЛЯЦИИ/ОТКЛЮЧЕНИИ/ОСТАНОВКЕ СКОМПРОМЕТИРОВАННЫХ БИЗНЕС- ИЛИ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ**

11 **ПРИНЯТЬ РЕШЕНИЕ, ТРЕБУЕТСЯ ЛИ ЗАПУСК ПРОЦЕССА ВОЗБУЖДЕНИЯ УГОЛОВНОГО ДЕЛА**

От этого решения будет зависеть процесс реагирования, расследования, сбора доказательств, общения с регулирующими органами и т. п.

13 **ОПОВЕСТИТЕ ИТ И ИБ, ЧТО ИМ МОЖЕТ ПОТРЕБОВАТЬСЯ ЗАНИМАТЬСЯ РАССЛЕДОВАНИЕМ И РЕАГИРОВАНИЕМ В КРУГЛОСУТОЧНОМ РЕЖИМЕ**

Продумайте вопрос мотивации/компенсации работы во внеурочное время. Это можно поручить ответственному за расследование и реагирование на инцидент, если он обладает необходимыми ресурсами.

12 **ОПРЕДЕЛИТЬ РЕГУЛЯРНОСТЬ И ПОРЯДОК ВСТРЕЧ С ОТВЕТСТВЕННЫМ ЗА РАССЛЕДОВАНИЕ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТ**

Относительно текущего статуса инцидента, хода его расследования, принятых мер, необходимых к принятию решений и т. п.

ДЛЯ ЗАМЕТОК

[1] Обратите внимание, ряд перечисленных в чек-листе задач должны/могут выполняться параллельно, что отражено на временной шкале в конце документа.

[2] На уровень руководства организации обычно выносятся только критические инциденты или недопустимые события, имеющие серьезные или катастрофические последствия для деятельности компании.

ВНЕШНИЕ КОММУНИКАЦИИ [3]

ВАС ВЗЛОМАЛИ?!

Что делать руководству компании?

1 СФОРМИРОВАТЬ КОМАНДУ АНТИКРИЗИСНОЙ КОММУНИКАЦИИ[4]

В нее должны войти (минимальный состав): ИТ/ИБ-директор (человек, ответственный за реагирование на инцидент и расследование); генеральный директор (и/или его зам); руководитель, отвечающий за внешние коммуникации; руководитель, отвечающий за внутренние коммуникации; юрист; директор по маркетингу (брендингу); директор по развитию бизнеса (если речь идет о специфических инцидентах, затрагивающих конкретный бизнес-процесс, то в команду также могут быть включены ответственные за бизнес-процесс).

2 ПРИНЯТЬ РЕШЕНИЕ О ТОМ, СООБЩАТЬ ИЛИ НЕТ ОБ ИНЦИДЕНТЕ КЛИЕНТАМ

В случае принятия решения не сообщать об инциденте, помните, что этот факт обычно все равно становится достоянием гласности (чем серьезнее инцидент, тем больше шансов на это). Подумайте, как вы будете реагировать в случае опубликования сведений об инциденте после вашего отказа признавать его.

3 ПРИНЯТЬ РЕШЕНИЕ О ТОМ, СООБЩАТЬ ИЛИ НЕТ ОБ ИНЦИДЕНТЕ РЕГУЛИРУЮЩИМ ОРГАНАМ (ФСБ РОССИИ, РОСКОМНАДЗОР, БАНК РОССИИ, МИНЦИФРЫ РОССИИ И Т. П.)

Если вы субъект критической информационной инфраструктуры, финансовая организация, или инцидент связан с персональными данными, в том числе биометрическими.

4 В СЛУЧАЕ РАНЕЕ ПРИНЯТОГО РЕШЕНИЯ О ВОЗБУЖДЕНИИ УГОЛОВНОГО ДЕЛА СООБЩИТЬ В ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ (МВД РОССИИ, ФСБ РОССИИ)

5 ПРИНЯТЬ РЕШЕНИЕ О ТОМ, СООБЩАТЬ ИЛИ НЕТ ОБ ИНЦИДЕНТЕ ПАРТНЕРАМ И КОНТРАГЕНТАМ

6 ПРИНЯТЬ РЕШЕНИЕ О ТОМ, СООБЩАТЬ ИЛИ НЕТ ОБ ИНЦИДЕНТЕ ИНВЕСТОРАМ И АКЦИОНЕРАМ

Уточните требования биржи и законодательства о публичных компаниях в юрисдикции расположения биржи и стран присутствия вашей компании.

7 ПРИНЯТЬ РЕШЕНИЕ О ТОМ, СООБЩАТЬ ИЛИ НЕТ ОБ ИНЦИДЕНТЕ ИНЫМ ЗАИНТЕРЕСОВАННЫМ ЛИЦАМ, ВКЛЮЧАЯ СМИ[5]

ВНЕШНИЕ КОММУНИКАЦИИ [3]

8 **СОГЛАСОВАТЬ ПОДГОТОВЛЕННОЕ КОМАНДОЙ АНТИКРИЗИСНОЙ КОММУНИКАЦИИ ЗАЯВЛЕНИЕ ДЛЯ СМИ И ИНЫХ ЗАИНТЕРЕСОВАННЫХ ЛИЦ С ОТВЕТАМИ НА КЛЮЧЕВЫЕ ВОПРОСЫ**

Возможные вопросы: «Что и как произошло?», «Какие данные/процессы пострадали?», «Уведомили ли вы все заинтересованные стороны?», «Что вы делаете для нейтрализации последствий инцидента и его неповторения в будущем?».

9 **ПРИНЯТЬ РЕШЕНИЕ О ТОМ, СООБЩАТЬ ЛИ ДЕТАЛИ ОБ ИНЦИДЕНТЕ ПРОАКТИВНО ИЛИ ТОЛЬКО ОТВЕТИТЬ НА ВОПРОСЫ ЗАИНТЕРЕСОВАННЫХ ЛИЦ**

10 **ОПРЕДЕЛИТЬ ЛИЦ, ИМЕЮЩИХ ПРАВО КОММЕНТИРОВАТЬ СИТУАЦИЮ С ИНЦИДЕНТОМ ОТ ИМЕНИ КОМПАНИИ**

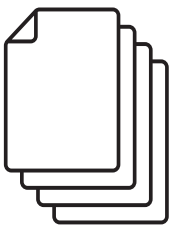
Если это не определено в плане антикризисной коммуникации. Уведомить всех работников/служащих о запрете любых внешних коммуникаций на тему инцидента, за исключением лиц, имеющих на это право.

11 **ОСУЩЕСТВИТЬ ВСЕ НЕОБХОДИМЫЕ ВНЕШНИЕ КОММУНИКАЦИИ В СООТВЕТСТВИИ С РАНЕЕ ПРИНЯТЫМИ РЕШЕНИЯМИ**

12 **УТОЧНИТЬ У ОТВЕТСТВЕННОГО ЗА РАССЛЕДОВАНИЕ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ, ВЫШЛИ ЛИ ВЫМОГАТЕЛИ НА СВЯЗЬ И С КАКИМИ ТРЕБОВАНИЯМИ**

13 **ПРИНЯТЬ РЕШЕНИЕ О ПРИГЛАШЕНИИ ЭКСПЕРТА, КОТОРЫЙ БУДЕТ ВЕСТИ ПЕРЕГОВОРЫ С ВЫМОГАТЕЛЯМИ**

ДЛЯ ЗАМЕТОК



[3] Внешние и внутренние коммуникации обычно реализуются параллельно.

[4] Многие из описанных в этом разделе задач могут быть частью планов антикризисной коммуникации и реагирования на инциденты.

[5] Последовательность принятия решений об уведомлении заинтересованных лиц зависит от важности каждой из категорий интересантов и определяется самостоятельно.

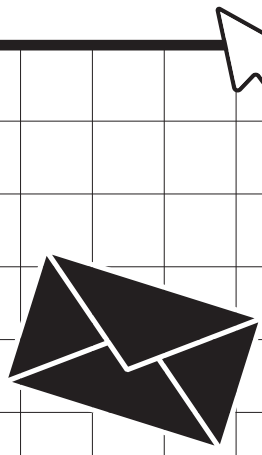
ВНУТРЕННИЕ КОММУНИКАЦИИ

ВАС ВЗЛОМАЛИ?!

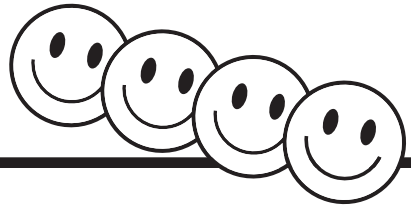
Что делать руководству компании?

1 **ИНФОРМИРОВАТЬ СОВЕТ ДИРЕКТОРОВ ОБ ИНЦИДЕНТЕ И ЕГО СТАТУСЕ**

В случае наличия совета директоров.



2 **ПРИНЯТЬ РЕШЕНИЕ О ТОМ, ЧТО СООБЩАТЬ РАБОТНИКАМ/СЛУЖАЩИМ КОМПАНИИ ОТНОСИТЕЛЬНО ИНЦИДЕНТА**



3 **ДОВЕСТИ ВМЕСТЕ С HR ДО РАБОТНИКОВ/СЛУЖАЩИХ КОМПАНИИ ИНФОРМАЦИЮ ОТНОСИТЕЛЬНО ИНИЦИДЕНТА, ОПРЕДЕЛЕННУЮ РАНЕЕ**

В формате видео-конференц-связи, внутренней рассылки или публикации на внутреннем корпоративном портале.

ЮРИДИЧЕСКИЕ ВОПРОСЫ

1 **ОЦЕНИТЬ ВМЕСТЕ С ЮРИДИЧЕСКОЙ СЛУЖБОЙ ЮРИДИЧЕСКИЕ ПОСЛЕДСТВИЯ ИНЦИДЕНТА**

Например, штрафы от регулирующих органов или штрафные санкции за нарушение контрактных обязательств.

2 **ОЦЕНИТЬ ВМЕСТЕ С ЮРИСТАМИ ПОСЛЕДСТВИЯ ОТКАЗА ОТ УВЕДОМЛЕНИЯ ОБ ИНЦИДЕНТЕ ЗАИНТЕРЕСОВАННЫХ ЛИЦ**

В том числе регулирующих органов (ФСБ России, Банк России, Роскомнадзор, Минцифры России и т. п.)

3 **ОЦЕНИТЬ ВМЕСТЕ С ЮРИСТАМИ ПОСЛЕДСТВИЯ ПЕРЕГОВОРОВ С ВЫМОГАТЕЛЯМИ И ВЫПЛАТ В ИХ АДРЕС**

В случае принятия такого решения. Окончательно решать вопрос с выплатой выкупа вам, но лучше не поощрять вымогателей дальше совершать преступления. Помните, что в ряде случаев и юрисдикций оплата вымогателям может сама по себе рассматриваться как уголовное преступление (финансирование экстремизма и терроризма, нецелевое расходование средств и т. п.).

ФИНАН-
СОВЫЕ
ВОПРОСЫ

ВАС ВЗЛОМАЛИ?!

Что делать руководству компании?

1 **ОБЕСПЕЧИТЬ ФИНАНСИРОВАНИЕ ПРОЦЕССА РЕАГИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ПОСЛЕ ИНЦИДЕНТА**

2 **ЕСЛИ У ВАС ПРИОБРЕТЕНА УСЛУГА СТРАХОВАНИЯ КИБЕРРИСКОВ, ЗАЯВИТЬ СТРАХОВОЙ КОМПАНИИ О НАСТУПЛЕНИИ СТРАХОВОГО СЛУЧАЯ**

3 **ОЦЕНИТЬ ВМЕСТЕ С ФИНАНСОВЫМ ДИРЕКТОРОМ ПОСЛЕДСТВИЯ ИНЦИДЕНТА, КОТОРЫЕ МОГУТ ПОТРЕБОВАТЬ ОТРАЖЕНИЯ В ФИНАНСОВОЙ ОТЧЕТНОСТИ**

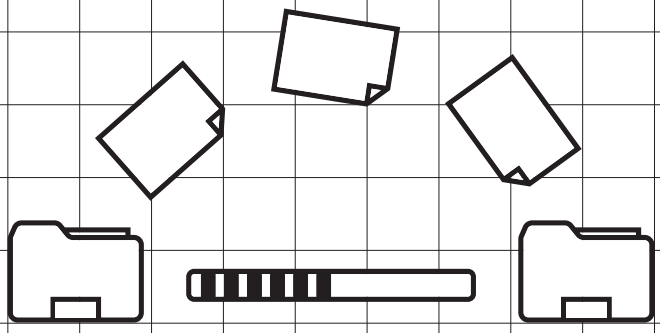
4 **ПРИНЯТЬ РЕШЕНИЕ О ВЫПЛАТЕ ВЫМОГАТЕЛЮ ВЫКУПА**

Определите предел суммы, которую вы готовы заплатить (если готовы).

5 **ОЦЕНИТЬ ВМЕСТЕ С ФИНАНСОВЫМ ДИРЕКТОРОМ ПОСЛЕДСТВИЯ ВЫПЛАТЫ ВЫМОГАТЕЛЯМ, А ТАКЖЕ СПОСОБ ТАКОЙ ВЫПЛАТЫ**

Выплата вымогателям обычно проводится в криптовалюте. Иногда для проведения оплаты могут быть привлечены внешние консультанты и компании.

ДЛЯ ЗАМЕТОК



ДЕЙСТВИЯ ПОСЛЕ ИНЦИДЕНТА

ВАС ВЗЛОМАЛИ?!

Что делать руководству компании?

1 УБЕДИТЬСЯ, ЧТО ИНЦИДЕНТ ИСЧЕРПАН

При отсутствии соответствующей экспертизы можно воспользоваться услугами внешних компаний (Compromise Assessment / ретроспективный анализ).

2 ИЗУЧИТЬ ВЫВОДЫ ОТЧЕТА О РАССЛЕДОВАНИИ ИНЦИДЕНТА И ОЦЕНИТЬ ПРИЧИНЫ ПРОИЗОШЕДШЕГО

По окончании расследования и реагирования.

3 ОЦЕНИТЬ ОКОНЧАТЕЛЬНЫЕ ПОСЛЕДСТВИЯ ИНЦИДЕНТА

Финансовые, репутационные, юридические, а также ущерб жизни и здоровью людей, экологии, культурным ценностям и т. п.

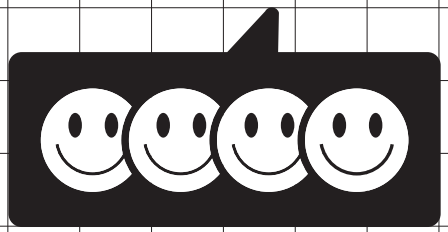
4 СООБЩИТЬ ОБ ОКОНЧАТЕЛЬНЫХ РЕЗУЛЬТАТАХ РАССЛЕДОВАНИЯ ИНЦИДЕНТА В РАМКАХ ВНЕШНИХ И ВНУТРЕННИХ КОММУНИКАЦИЙ

Всем аудиториям, которым были отправлены первичные уведомления об инциденте.

5 ПРИНЯТЬ РЕШЕНИЕ О НЕОБХОДИМОСТИ ПЕРЕСМОТРА СТРАТЕГИИ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ В ОРГАНИЗАЦИИ НА ОСНОВЕ ИЗВЛЕЧЕННЫХ УРОКОВ

Включая пересмотр планов обеспечения ИБ и ИТ, реагирования на инциденты, обеспечения непрерывности бизнеса, планов восстановления, организационно-штатной структуры, функций ИБ и ИТ, имеющихся в их распоряжении ресурсов и т. п.

ДЛЯ ЗАМЕТОК



КОГДА МОЖНО ПРЕКРАТИТЬ ДЕРЖАТЬ ИНЦИДЕНТ В ФОКУСЕ ВНИМАНИЯ[6]?

1 **ВНЕШНИЙ ХАКЕР «ВЫБИТ» ИЗ ИНФРАСТРУКТУРЫ ИЛИ ВНУТРЕННИЙ НАРУШИТЕЛЬ ИЗОБЛИЧЕН**

2 **ПЛАН РЕАГИРОВАНИЯ НА ИНЦИДЕНТ РЕАЛИЗОВАН ПОЛНОСТЬЮ**

При условии, что у вас изначально был хороший и протестированный план реагирования.

3 **ПОСЛЕДСТВИЯ ИНЦИДЕНТА НЕЙТРАЛИЗОВАНЫ**

Помните, что некоторые последствия, например финансовые или репутационные, могут проявляться достаточно долго. В этом случае имеет смысл раз в квартал или полугодие уточнять статус инцидента у ответственного лица.

4 **УГОЛОВНОЕ ДЕЛО/ СЛЕДСТВИЕ ЗАВЕРШЕНО**

Если оно было возбуждено/ инициировано.

5 **ПРИГЛАШЕННЫЕ ВНЕШНИЕ ЭКСПЕРТЫ ПО РАССЛЕДОВАНИЮ И РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ ПОДТВЕРДИЛИ ОКОНЧАНИЕ ИНЦИДЕНТА**

Если ранее было принято решение о привлечении внешних экспертов по расследованию и реагированию на инциденты.

[6] Прекращение контроля зависит от множества факторов, включая тип инцидента.

ВРЕМЕННАЯ ШКАЛА КЛЮЧЕВЫХ ВЕХ В РАССЛЕДОВАНИИ И РЕАГИРОВАНИИ НА ИНЦИДЕНТ