Хакерская атака. Как юротдел может предотвратить утечку данных компании

Денис Алехин
Адвокат, младший партнер ZKS

Узнаете: *из-за чего сотрудники поддаются на уловки хакеров и как избежать уголовного дела.*

Только в этом году произошло сразу несколько громких утечек информации: хакеры получили доступ к данным Почты России, Яндекс.Еды, ретейлера DNS и других компаний. Атаки грозят не только крупному бизнесу: взламывают и менее известные компании. Причем действуют зачастую через сотрудников, которые по неосторожности помогают злоумышленникам. И хотя у компании в этом случае будет статус потерпевшего, все равно она рискует получить претензии: иски от субъектов персональных данных, проверки Роскомнадзора. А если хакеры получат доступ к коммерческой тайне — могут шантажировать и угрожать продать информацию конкурентам. Чтобы этого избежать, советуем не только полагаться на технические способы защиты, но и объяснять сотрудникам правила кибербезопасности, разработать документы, которые дисциплинируют. Как это сделать, читайте далее.

Из-за чего сотрудники случайно помогают хакерам и подпадают под уголовку

Зачастую вредоносные программы взлома не справляются с информационной защитой компании. Тогда злоумышленники используют метод социальной инженерии: психологически

воздействуют на сотрудников компании и вынуждают их передать конфиденциальную информацию или предоставить к ней доступ. Например, направляют сотруднику письмо с зараженной ссылкой. Или представляются работником отдела информационной безопасности и вынуждают дать логин и пароль от учетной записи.

Так, в мае этого года злоумышленник получил доступ к базе данных сотен сотрудников американской компании. После этого связался с ней и заявил, что представился службой поддержки и убедил одного из сотрудников дать удаленный доступ к рабочему компьютеру. Хакер угрожал обнародовать данные, если не получит 250 тыс. долл.

Есть случаи, когда в действиях сотрудника следователи увидят состав преступления.[УК] Это возможно, если правила работы с компьютерной информацией зафиксировали в локальных нормативных актах и инструкциях, ознакомили с ними сотрудника, но тот умышленно или неосторожно эти правила нарушил. Например, предоставил посторонним доступ, установил нелицензионное программное обеспечение, изменил настройки компьютера, отключил противовирусную защиту.

УК Ст. 274 УК

При этом должно наступить два последствия. Во-первых, хакер уничтожил, заблокировал, модифицировал или скопировал информацию. Во-вторых, компании причинили ущерб на сумму более 1 млн руб. Речь о расходах, которые понесла компания, чтобы восстановить работу информационных систем. К примеру, на восстановление доступа к базе данных после смены паролей, на покупку оборудования взамен изъятого у нарушителя.

Сотрудников, чьи действия поспособствовали хакерской атаке, могут в лучшем случае оштрафовать на сумму до 500 тыс. руб., а в худшем — лишить свободы на два года. Чтобы не допустить

За какие действия хакеров привлекают к уголовной ответственности

Самое частое киберпреступление в отношении компаний — хакерская атака. Ее могут совершать, к примеру, с помощью вредоносных программ, файловых вирусов, фишинга. Они действуют на наиболее уязвимые объекты: операционные системы, браузеры, офисные приложения. В таких действиях злоумышленников есть признаки преступления — неправомерного доступа к компьютерной информации, но только если уничтожили, заблокировали, модифицировали либо скопировали компьютерную информацию. За это лишают свободы на срок до двух лет, а если действовали из корыстной заинтересованности или причинили крупный ущерб — до четырех лет.

При этом «чистое хакерство», когда злоумышленник только ознакомился с информацией или действовал исключительно из личного интереса, состава этого преступления не образует. В большинстве случаев действия хакеров содержат признаки преступления по статье 273 УК: создание, использование и распространение вредоносных программ, с помощью которых и получили неправомерный доступ. За это лишают свободы на срок до четырех лет. Если была корыстная заинтересованность или крупный ущерб — до пяти.

Источники: ст. 272, 273 УК

ситуацию, когда сотрудники по неосторожности помогли взломать данные компании, советуем разработать совместно с IT-отделом стратегию защиты от хакеров и ознакомить с ней коллег.

Как юротделу предотвратить утечку данных

Чтобы избежать взлома, советуем не ограничиваться техническими мерами защиты, которыми занимаются IT-специалисты компании. Важно разработать правила работы с компьютерной информацией внутри компании и ознакомить с ними всех сотрудников. Это задача юротдела, но для консультаций по техническим вопросам понадобится привлечь коллег-айтишников.

Рекомендуем начать с разработки локального акта — правил эксплуатации средств хранения, обработки или передачи компьютерной информации внутри компании. В нем перечислите запреты для сотрудников. К примеру, нельзя загружать и самостоятельно устанавливать ПО, обновлять программы, допускать к работе посторонних, заходить в сеть через неслужебный канал доступа.

Советуем отдельно прописать, как действовать, если надо передать данные кому-либо, в том числе и сотрудникам безопасности. Например, указать, что это можно делать исключительно по конкретному каналу связи. Еще в акте следует назначить ответственного за соблюдение правил кибербезопасности. После того как директор утвердит правила, необходимо ознакомить с ними всех сотрудников компании под подпись.

Еще стоит проработать текст должностных инструкций отдельных сотрудников, к примеру, работающих с финансами. В их инструкции также внесите обязанности, ограничения и запреты, которые связаны с компьютерной информацией. Затем ознакомьте сотрудников с обновленными должностными инструкциями.

Что делать, если данные компании уже украли

Если хакерская атака уже произошла, советуем незамедлительно заявить о преступлении в правоохранительные органы. Так компания получит статус потерпевшего со всеми его правами, в том числе с правом предъявить гражданский иск. Киберпреступления подследственны всем органам, которые ведут предварительное следствие, — СК, МВД и ФСБ. В системе МВД раскрытием киберпреступлений занимается Управление «К». Чтобы определить, куда подавать заявление, сверьтесь с правилами подследственности по статье 151 УПК.

В заявлении необходимо не только подробно описать ситуацию, но и сослаться на документы, которые подтвердят ваши сведения. Копии этих документов приложите к заявлению. Среди них могут быть, например, выписки по счетам, если произошло хищение, перечень технических устройств, доказательства ущерба, результаты служебного расследования. Его рекомендуем проводить параллельно с подачей заявления и затем направлять следователям новые документы и информацию, которую получите. Также советуем сразу представить список сотрудников, у которых есть доступ к данным, приказы об их назначении, должностные инструкции.

Стоит подготовиться к тому, что правоохранители произведут выемку смартфонов и компьютерных устройств для компьютерно-технических экспертиз. Это обусловлено тем, что на устройствах могут быть программы дистанционного банковского обслуживания, вирусы, данные о звонках от злоумышленника. Перед выемкой телефоны необходимо перевести в авиарежим, а компьютеры в режим гибернации. Кроме того, подготовьтесь, что правоохранительные органы будут допрашивать свидетелей — сотрудников компании ◆

Как сотрудникам минимизировать риски хакерской атаки

1. Ознакомьтесь с локальными актами, которые регламентируют вопросы кибербезопасности, и с должностной инструкцией
2. Не используйте рабочие устройства в неслужебных целях
3. Проверяйте письма, которые поступают на рабочую почту, особенно если они содержат ссылки на сторонние ресурсы. В случае сомнений лично свяжитесь с отправителем и убедитесь, что он направлял сообщение
4. Незамедлительно сообщайте ответственным лицам, к примеру, системному администратору, о возможной уязвимости устройств, например, об уведомлениях о вирусах или обновлении ПО
5. Передавайте конфиденциальные сведения только после того, как убедитесь, что получатели — действительно сотрудники компании и имеют право доступа к сведениям. В случае сомнений обратитесь в службу безопасности или к руководству компании