Расследование компьютерных происшествий

Владимир Безмалый |
MVP Consumer Security, Microsoft Security Trusted Advisor,
cybercop@outlook.com

В условиях широкого развития информационных технологий, распространения скоростного доступа в Интернет информация становится не просто товаром, а весьма дорогим товаром. И понятно, что компьютеры и компьютерные сети на предприятиях все чаще вызывают пристальный интерес со стороны злоумышленников.

Стоимость услуг хакера
(источник: Group-IB)

Взлом сайта или форума	от $50
Гарантированный взлом почтового ящика Yandex, Mail, Rambler	от $45
DDoS-атака	от $100
Массовое внедрение троянского и шпионского ПО	от $100
Рассылка спама:	
400 000 компаний	$55
1 800 000 частных лиц	$100
90 000 компаний в Санкт-Петербурге	$30
450 000 частных лиц на Украине	$50
6 000 000 частных лиц в России	$150
4 000 000 адресов @ mail.ru	$200

Такие преступления, как несанкционированное вторжение, хищение персональных данных и учетных записей, финансовых данных, интеллектуальной собственности уже давно не редкость. На смену «школьникам», промышляющим взломом веб-страниц, приходят хорошо организованные группы профессионалов, доходы которых поражают воображение, достигая порой десятков миллионов долларов. Естественно, столь значительные средства (при минимальных издержках) позволяют преступникам расширять спектр незаконных активностей в области разработки технических средств, вовлекая в свои ряды специалистов из нужных им областей деятельности.

Злоумышленники привыкли к полной безнаказанности. Единственная проблема, стоящая на их пути, — обход очередного технического решения, а не возможность попасть на судебную скамью. Компьютеры могут использоваться в качестве инструментов для организации атак на компьютерные сети и уничтожения данных. Такие действия все чаще подвергают организации рискам правового и финансового характера, что нередко требует проведения в организации внутренних расследований компьютерных происшествий. (Я умышленно употребляю термин «происшествие», а не «преступление», так как расследование престу-

Организации следует сразу определиться, будет ли она проводить внутреннее расследование происшествия или обратится к внешним экспертам

плений в нашей стране остается прерогативой исключительно правоохранительных органов.)

Анализ действующего в России уголовного, уголовно-процессуального и административного законодательств показывает отсталость, неточность и противоречивость многих нормативных документов. Аналогичные недостатки характерны для научных, методических и учебных материалов по уголовному праву, криминалистике, судебной экспертизе, оперативно-разыскной деятельности и информатике. Отстает от времени в этом вопросе и корпоративный сектор.

Главные проблемы в сфере безопасности ИТ можно разделить на два сегмента (см. таблицу 1).

На корпоративном рынке устоялось мнение: корпоративная служба безопасности может все расследовать сама. А что оборудование для определенных видов экспертиз может стоить $200 тыс. и более, никого не интересует. Но, даже если принимается решение, что все расследования компьютерных происшествий будет проводить корпоративная служба информационной безопасности, необходимо учесть следующее.

Каким бы классным профессионалом ни был сотрудник службы ИБ, он не может постоянно отслеживать обновления базы правовых решений по компьютерным преступлениям, а от этого зависит, как именно необходимо настроить систему журналирования в информационных системах и выстроить процедуру реагирования на инциденты ИБ, чтобы они отвечали реальной проблематике и обеспечивали правовой сбор доказательств.

Для проведения расследования требуются специальное оборудование и программное обеспечение для компьютерной экспертизы, которое не так просто купить, да и стоимость его порой слишком высока.

Таблица 1.

	Проблемы в сфере безопасности ИТ
Государственные	Менталитет граждан
	Нет единой системы обмена информацией по инцидентам в сфере ИТ
	Киберпреступность не знает границ, а законы в области компьютерных преступлений в различных странах очень сильно отличаются. Более того, некоторые страны вообще не имеют законодательства в области ИТ-преступлений
	Отсутствие качественного образования в области подготовки специалистов по проведению расследований ИТ-преступлений
	Отсутствует сертификация специалистов в этой области
	Устаревшее законодательство в области ИТ-преступлений
	Недостаточная оперативность работы правоохранительных органов, возможность утечек, не всегда хорошая техническая подготовка лиц, проводящих расследование
Корпоративные	Упор на технические меры в области обеспечения ИБ
	Менталитет сотрудников служб информационной безопасности. Зачастую сотрудники ИБ предпочитают закрыть утечку, но не проводить расследование, чтобы не предавать огласке сам факт происшествия
	Нет единых стандартов по реагированию на инцидент
	Нет единых стандартов журналирования в информационных системах
	Неприменимость многих западных методик к российской действительности (на Западе корпорации заявляют о преступлениях в области ИТ в полицию, у нас зачастую стараются обойтись своими силами и замалчивают соответствующие факты, кроме того, некоторые западные методики проведения расследования не могут быть применены в России, так как противоречат законодательству)
	Сложность проведения компьютерной экспертизы. Зачастую в корпоративном секторе нет ни специалистов, ни соответствующего аппаратно-программного оборудования
	Закрытость информации по инцидентам в корпорациях

Расследование инцидента в области информационной безопасности может занять несколько месяцев, в течение которых сотрудник, проводящий расследование, будет оторван от текущей работы и его обязанности придется перераспределять среди других работников. А если штат мал или работники и так перегружены?

Если инцидент произошел по вине или недосмотру службы информационной безопасности, то стоит ли ждать объективной оценки случившегося?

Многие сотрудники ИБ-службы уверены, что в силах разрешить все сами, используя только технические и организационные средства. В итоге — количество инцидентов и ущерб от них растут, невзирая на увеличивающиеся бюджеты на ИБ.

Допустим, что 80% внутренних инцидентов ваша служба безопасности может расследовать сама (возьмем сказочную ситуацию, что дорогое оборудование и софт у нее для этого есть), но что делать с внешними инцидентами? В случае реального инцидента, связанного с расследованием

DDoS-атаки или мошенничества с IP-адреса, который является элитным зарубежным прокси-сервером, служба безопасности оказывается в тупиковой ситуации.

Таким образом, организации следует сразу определиться, будет ли она проводить внутреннее расследование происшествия или обратится к внешним экспертам. Вместе с тем следует понимать, что, если расследуемое происшествие имеет, на ваш взгляд, судебную перспективу, необходимо подключение правоохранительных органов на первоначальном этапе.

МОДЕЛЬ РАССЛЕДОВАНИЯ КОМПЬЮТЕРНЫХ ПРОИСШЕСТВИЙ

Уоррен Круз II (Warren G. Kruse II) и Джей Хэйзер (Jay G. Heiser), авторы книги "Computer Forensics: Incident Response Essentials" («Судебные исследования компьютеров: основы реагирования в случае происшествий»), утверждают, что процесс данного вида исследований включает в себя выявление, изъятие, сохранение, документальное оформление и расшифровку компьютерных носителей для проведения анализа доказательств и основных причин происшествия.

При работе с цифровыми доказательствами расследования сопроводительные процедуры осуществляются в четыре этапа:

- **Оценка ситуации.** Анализ рамок проводимого расследования и необходимых действий.
- **Сбор данных.** Сбор, защита и сохранение исходных доказательств.
- **Анализ данных.** Объем и качество изучения и сопоставления цифровых доказательств с событиями, достаточные для обращения в правоохранительные органы.
- **Отчет о расследовании.** Сбор и организация полученной информации, написание итогового отчета.

Прежде чем инициировать исследование, необходимо проконсультироваться у юристов, чтобы решить, стоит ли сообщать о происшествии в правоохранительные органы

Прежде чем инициировать исследование, необходимо проконсультироваться у юристов, чтобы решить, стоит ли сообщать о происшествии в правоохранительные органы.

УВЕДОМЛЕНИЕ ОТВЕЧАЮЩИХ ЗА ПРИНЯТИЕ РЕШЕНИЙ ЛИЦ И ПОЛУЧЕНИЕ РАЗРЕШЕНИЯ

Если в вашей организации не существует правил и процедур реагирования в случае компьютерных происшествий, необходимо:

1. уведомить ответственных за принятие решения лиц о факте происшествия и необходимости принятия решения о проведении расследования;
2. получить от принимающего решение лица письменное разрешение на проведение расследования.

Все действия в ходе расследования должны быть тщательно задокументированы, ведь в итоге данный документ может быть использован в суде.

Приоритетная задача расследования — предотвращение дальнейшего

Рекомендации по организации группы для проведения расследования:

- Руководителем группы должен быть человек, имеющий опыт работы в правоохранительных органах, осведомленный о том, как нужно проводить расследование. Следует помнить: если ваше происшествие будет рассматриваться в суде, квалификация и репутация этого человека будут подвергнуты проверке.
- Четко определите обязанности членов группы. Подумайте о взаимозаменяемости.
- В составе группы должен быть технический специалист соответствующего уровня, обладающий опытом проведения подобных расследований.
- Не экономьте на обучении специалистов, входящих в вашу группу.
- Численность группы должна быть минимальной. Это уменьшит вероятность утечки информации.
- Убедитесь, что каждый член группы прошел необходимую проверку, что вы можете ему безусловно доверять и он обладает необходимыми полномочиями.
- Если в организации отсутствует персонал с необходимыми навыками, обратитесь к сторонней группе, которой вы можете доверять.

ущерба организации (естественно, если отсутствует угроза государственной безопасности, а также здоровью или жизни людей).

Учтите, что все принимаемые вами решения могут быть (и, как правило, будут) подвергнуты сомнению в суде наряду с доказательствами.

Все действия в ходе расследования должны быть тщательно задокументированы, ведь в итоге данный документ может быть использован в суде

ИЗУЧЕНИЕ ПРАВИЛ И ЗАКОНОВ

Прежде чем браться за компьютерное расследование, необходимо изучить требования соответствующих законов, а также внутренних документов организации (если таковые есть), под действие которых подпадает проводимое расследование. Обратите внимание на следующие обстоятельства: достаточно ли у вас юридических полномочий для проведения таких действий? приняты ли в организации соответствующие нормы и процедуры в отношении прав на неприкосновенность личной жизни сотрудников, подрядчиков и других лиц, использующих сеть организации? определены ли в них условия, при которых разрешено осуществление наблюдения?

Во избежание ошибок при ведении расследования необходимо проконсультироваться с юристами, не повлечет ли расследование:

- угрозу сохранности персональных данных клиентов или нарушение других норм правового характера;
- ответственность за незаконный перехват электронной переписки и просмотр конфиденциальной информации клиентов.

Убедитесь, что вы учитываете требования по обеспечению конфиденциальности данных клиентов:

- все данные передаются по защищенным каналам;
- все данные хранятся на рабочих станциях, а не на серверах, причем они не должны быть легкодоступны;
- все данные, включая документацию, после закрытия расследования должны храниться в течение срока, определенного законом.

Если дело все же будет рассматриваться в суде, необходимо сохранять все цифровые и бумажные копии доказательств, а также цепочки обеспечения сохранности последних, для чего необходимо обеспечить сохранность поддающейся проверке документации, в которой будет указано, кто и когда работал с доказательством, а также место, дата и время сохранения этого доказательства. Необходимо также хранить доказательства в защищенном хранилище, иначе невозможно будет доказать их подлинность.

СОЗДАНИЕ ГРУППЫ ПРОВЕДЕНИЯ РАССЛЕДОВАНИЯ

В случае, если в организации принято решение проводить расследование самостоятельно, необходимо определить перечень лиц, которые будут этим заниматься (в идеале, конечно же, лучше сделать это заранее). Список группы таких лиц должен быть отнесен к конфиденциальной информации.

Чрезвычайно важно, чтобы группа была соответствующим образом организована и все ее члены имели соответствующую квалификацию. Кроме того, на период проведения расследования члены группы выводятся из подчинения своих непосредственных руководителей и переходят под начало только руководителя группы, который, в свою очередь, подчинен только руководителю организации. Безусловно, приведенные рекомендации не могут быть исчерпывающими, и в каждой организации этот сложный вопрос будет решаться по-своему. Однако очень надеюсь, что мои советы помогут вам успешно пройти все лабиринты расследования, избежав неверных шагов и скороспелых выводов.