УДК 343.98

НЕОТЛОЖНЫЕ ДЕЙСТВИЯ В ОРГАНИЗАЦИИ ПОСЛЕ ИНЦИДЕНТА В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гайстер С.В.,
студент, Финансовый университет, Москва, Россия
sergeygaister@yandex.ru

Аннотация. *Сегодня имеются веские основания полагать, что применяемые в настоящее время большинством организаций меры не обеспечивают необходимого уровня безопасности субъектов, участвующих в процессе информационного взаимодействия, и не способны в необходимой степени противостоять разного рода воздействиям с целью доступа к критичной информации и дезорганизации работы информационных систем. Целью данной статьи является изучение рекомендаций для организаций, пострадавших от инцидентов в сфере информационной безопасности (ИБ), на основе исследования Национального центра по защите инфраструктуры США. Формулируется немедленная последовательность действий при обнаружении инцидента в рамках российской действительности.*

Ключевые слова: *компьютерная криминалистика; инциденты ИБ; информационная безопасность организации.*

IMMEDIATE ACTIONS IN THE ORGANIZATION AFTER THE INCIDENT IN THE SPHERE OF INFORMATION SECURITY

Gaister S.V.,
student, Financial University, Moscow, Russia
sergeygaister@yandex.ru

Abstract. *Today, there are strong reasons to believe that the measures currently applied by most organizations do not provide the necessary level of security for the actors involved in the information communication process and are not able to withstand the necessary effects in order to access critical information and work disorganization information systems. The purpose of this article is to study recommendations for organizations affected by incidents in the field of information security (IS), based on the study of the National Center for Infrastructure Protection in the United States. An immediate sequence of actions is formulated when an incident is detected within the framework of Russian reality.*

Keywords: *computer forensics; IS incidents; information security of the organization.*

Научный руководитель: ***Крылов Г.О.,*** *доктор физико-математических наук, профессор, Финансовый университет.*

Введение

Любое фундаментальное техническое или технологическое новшество, предоставляя возможности для решения одних социальных проблем и открывая широкие перспективы для развития личности и общества, всегда вызывает обострение старых или порождает новые, ранее неизвестные проблемы, становится источником новых потенциальных опасностей.

Бурное развитие средств вычислительной техники, с одной стороны, открыло перед человечеством небывалые возможности по автоматизации умственного труда и привело к созданию большого числа разного рода автоматизированных информационных и управляющих систем, к возникновению принципиально новых так называемых информационных технологий. С другой стороны, всеобщая компьютеризация породила и новые компьютерные преступления, наносящие ущерб едва ли не больше традиционных.

Неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах наносят серьезный материальный и моральный урон многим субъектам (государству, юридическим и физическим лицам), участвующим в процессах автоматизированного информационного взаимодействия.

Жизненно важные интересы этих субъектов, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их экономических, политических и других сторон деятельности, конфиденциальная коммерческая и персональная информация, была бы постоянно легко доступна и в то же время надежно защищена от неправомерного ее использования: нежелательного разглашения, фальсификации, незаконного тиражирования, блокирования или уничтожения.

Компьютерная криминалистика и ее особенности

Компьютерной криминалистикой называется отрасль криминалистики, рассматривающая раскрытие и расследование преступлений, связанных с компьютерной информацией, методы и технические средства получения и исследования доказательств, связанных с компьютерной информацией [1].

В компьютерной криминалистике изучаются:

- криминальная практика — способы и инструменты совершения преступлений в области компьютерной информации, последствия, следы, личность преступника;
- оперативная, следственная и судебная практика по преступлениям в области компьютерной информации;
- методы экспертного исследования компьютерной информации — программ и данных;
- возможность использования новых разработок в IT-сфере для совершения компьютерных преступлений, а также для предотвращения и раскрытия таких преступлений.

Особенностью компьютерной криминалистики по сравнению с традиционной является в первую очередь то, что цифровые доказательства не воспринимаются непосредственно органами чувств человека. Поэтому эти следы достаточно сложно продемонстрировать участникам уголовного судопроизводства — следователю, прокурору, судье, присяжным и т.д. Для такой демонстрации требуется специальное оборудование и программное обеспечение.

Неотложные действия после инцидента

Инцидент в информационной системе компании не должен оказаться неожиданностью для службы безопасности. В организации должен существовать совместный план службы безопасности и отдела автоматизации по реагированию в критических ситуациях. При составлении этого плана может оказаться очень полезным зарубежный опыт. Так, Национальный центр по защите инфраструктуры США (National Infrastructure Protection Center) сформулировал рекомендации для организаций, пострадавших от инцидентов. Эти рекомендации NIPC вполне применимы и в российских условиях, поэтому приводятся здесь в полном объеме [2].

1. Реагируйте быстро. Установите контакт с правоохранительными органами. Поиск следов часто невозможен, если до уведомления правоохранительных органов или вашего собственного отдела информационной безопасности прошло много времени.

2. Если вы не уверены, какие действия следует предпринять, то ни в коем случае не останавливайте системные процессы и не изменяйте файлы. Это может уничтожить следы вторжения.

3. Строго следуйте всем предписанным процедурам (если ваша организация имеет возможность расследования компьютерных инцидентов).

4. Для любых контактов по поводу расследования пользуйтесь только телефоном. Помните, что злоумышленник может просматривать вашу электронную почту.

5. Немедленно свяжитесь с отделом информационной безопасности вашей организации. Быстрая техническая экспертиза очень важна для предотвращения дальнейших поломок и обеспечения сохранности возможных улик.

6. Рассмотрите вопрос об оснащении входящих телефонных линий аппаратурой АОН. Полученная таким путем информация может оказаться решающей для выявления источника вторжения.

7. Заранее укрепляйте контакты с адвокатской конторой, командой аварийного реагирования, правоохранительными органами. Предварительные контакты помогут обеспечить немедленное реагирование этих подразделений.

8. Сделайте копии всех файлов, которые хакер может изменить или стереть. Если вы предоставите эти копии файлов экспертам, их выводы помогут следователю установить, когда и каким образом было осуществлено вторжение.

9. Определите основные точки для поиска потенциальных улик. Обеспечьте сохранность улик. Неверно оформленные возможные вещественные и информационные улики могут потерять доказательственное значение.

10. Не вступайте сами в контакт с подозреваемым нарушителем.

Фактически эти «десять заповедей» должны стать настольным документом каждого сотрудника отдела ИБ. Следование им может в дальнейшем существенно облегчить расследование.

Действия по приведенным выше рекомендациям проводятся как до, так и во время и после инцидента. На их основе можно сформулировать немедленную последовательность действий по обнаружению инцидента:

- Немедленно доложить начальнику отдела ИБ.
- Предварительно выяснить причину инцидента (сбой, ошибки).
- При наличии признаков умышленных противоправных действий оценить, окончено ли вторжение.
- По возможности, не препятствовать действиям злоумышленника до установления его личности.
- Не допустить распространения слухов и панических настроений в организации.
- Установить примерное местонахождение злоумышленника. В случае, когда вторжение осуществляется изнутри организации, принимать меры по задержанию с поличным.

Большая часть этих соображений интуитивно понятна. Следует прокомментировать лишь два момента.

Во-первых, в большинстве случаев системные администраторы стараются немедленно прекратить действия злоумышленников. При этом те понимают, что обнаружены, и пытаются скрыть следы противоправной деятельности. Так, в крупной подмосковной торговой фирме системный администратор обнаружил на одном из компьютеров «троянскую» программу. Администратор принял немедленные меры — удалил программу с зараженного компьютера, а также установил, на какой адрес электронной почты программа передавала информацию. По этому адресу администратор направил гневное письмо, пригрозив обратиться в ФСБ. В результате, когда личность хакера, использовавшего «троянскую» программу, была установлена, какие-либо доказательства его вины отсутствовали [3]. Правильным поведением в такой ситуации было бы не предпринимать никаких действий, которые могли бы насторожить злоумышленника, вплоть до его задержания.

Во-вторых, во многих организациях излишне нервно реагируют на возникший инцидент. Кроме тех, кто должен быть оповещен об инциденте, новость (как правило, в весьма преувеличенном виде) узнают все знакомые системного администратора, секретарей руководства и т.д. Не получившие информацию из первых рук замечают непривычную суету и крайне нетипичное поведение руководства фирмы. В отсутствие достоверной информации среди персонала по-

являются весьма странные слухи, активное обсуждение которых окончательно сбивает организацию с рабочего ритма. Естественно, таким путем информация может попасть и к злоумышленникам, подготовившим инцидент. В идеальном случае об инциденте должны узнать только его непосредственные очевидцы, ИБ и руководство организации. Даже если инцидент повлек полное или частичное прекращение функционирования автоматизированной системы, следует сообщить персоналу благовидный предлог для остановки работы (например, случайный сбой на сервере, плановый ремонт, установка нового программного обеспечения и т.д.). Ни в коем случае нельзя допустить утечки информации к клиентам организации, посетителям и другим случайным лицам.

Разумеется, секретность на начальном этапе не означает, что факт инцидента обречен навсегда остаться в тайне. Напротив, после установления причины инцидента и выявления злоумышленников соответствующее сообщение в средства массовой информации и всему персоналу организации может дать хороший профилактический эффект от новых попыток неправомерного доступа к информации.

Заключение

Изучение рекомендаций для организаций, пострадавших от инцидентов в сфере ИБ, на основе исследования Национального центра по защите инфраструктуры США, помогло сформулировать последовательность действий в условиях российских реалий, которые могут дать наилучший результат для помощи правоохранительным органам при дальнейшем расследовании.

Список источников

1. *Федотов Н.Н.* Форенсика — компьютерная криминалистика. М.: Юридический мир, 2012.
2. *Steve Bunting, William Wei.* The Official EnCe: EnCase Cartified Examiner. Wiley Publishing, 2015.
3. *Тененбаум Э.* Компьютерные сети. СПб.: Питер, 2013.

ИНФОРМБЮРО

«КАСПЕРСКИЙ» ВНЕ ЗАКОНА В США

США применили санкции в отношении очередной российской компании. «Лаборатория Касперского» представляет угрозу для безопасности, считают американские власти. Какими будут потери для «Касперского»? Госучреждениям США запретили использовать продукцию «Лаборатории Касперского». Об этом объявило Министерство внутренней безопасности США. Использование продукции российской компании должно быть полностью прекращено в ближайшие три месяца. В министерстве заявили, что продукция «Касперского» представляет угрозу безопасности и может быть использована для взлома. Насколько сильным ударом это будет для производителя антивируса?

В самой «Лаборатории Касперского» говорят, что обвинения в адрес компании основаны на ложных и неточных данных, достоверных свидетельств не представлено. Информация, поступающая в «Лабораторию Касперского» от клиентов, полностью защищена в соответствии с законом и отраслевыми стандартами, заявили в компании.

Kaspersky Lab считает решение властей США политическим и намерена его опротестовать. Об этом заявил в интервью Business FM вице-президент «Лаборатории Касперского» по связям с государственными органами Антон Шингарёв.

Специальный помощник президента США Дональда Трампа и координатор Белого дома по вопросам кибербезопасности Роб Джойс назвал «неприемлемым риском» установленные на правительственных компьютерах продукты разработчика антивирусного программного обеспечения. Тем временем посольство России в США заявило, что решение американской стороны по антивирусу Касперского — это недобросовестная конкуренция, которая «вызывает крайнее сожаление».

ПО «Касперского», скорее всего, стояло на компьютерах во второстепенных госструктурах США, считает заместитель руководителя Лаборатории по компьютерной криминалистике Group-IB Сергей Никитин: «Если мы говорим про какие-то, действительно, важные объекты органов власти в США, то там у них очень жесткие требования к производителю. Но кроме действительно важных узлов есть еще огромное количество сопутствующей инфраструктуры, где все не так жестко, и там могли стоять любые антивирусы, любых вендоров по всему миру. Продукт был конкурентоспособный, интересный. Все современные антивирусы для полноценной работы активно обмениваются данными о работе компьютера с сетью».

Источник: Business FM