

1 Организация реагирования на чрезвычайные ситуации (инциденты)

Реагирование на возникающие чрезвычайные ситуации (инциденты), связанные с нарушением информационной безопасности, является таким же важным направлением работы, как и построение системы защиты и предотвращения нарушений. Под инцидентом, как правило, понимается какое-либо отклонение от нормального процесса использования информационных ресурсов и функционирования информационных систем, повлекшее ущерб для определенных информационных активов предприятия или непосредственно создающее угрозу нанесения такого ущерба.

Чрезвычайная ситуация (инцидент), связанная с нарушением информационной безопасности, может быть обусловлена:

- разрушительным воздействием на весь имущественный комплекс предприятия при возникновении стихийных факторов (наводнение, пожар, землетрясение и пр.) или целенаправленном нападении (подрыв, поджог, разрушение зданий и помещений и пр.);
- негативным воздействием исключительно на информационные ресурсы предприятия (как правило, осуществляемым удаленно, с использованием телекоммуникационных каналов).

В общем случае организационные процедуры (регламенты) реагирования на чрезвычайные ситуации должны включать в себя:

- регламенты альтернативных процессов обработки информации (в том числе, возможно, и без использования средств автоматизации) на период выхода из строя основных информационных ресурсов;
- определение групп персонала, ответственных за выполнение тех или иных функций в случае возникновения чрезвычайной ситуации, а также определение процедур взаимодействия между группами и отдельных групп с руководством предприятия;

- техническую и организационную документацию, необходимую для восстановления информационных систем и данных после чрезвычайной ситуации;
- порядок хранения архивных (резервных) копий данных и программных приложений обработки данных в местах, защищенных от механических воздействий, краж, наводнений, пожаров и пр. (в т.ч., возможно, в местах, территориально удаленных от основных мест хранения и обработки информации);
- соглашения с поставщиками программных и аппаратных средств, входящих в информационную инфраструктуру предприятия, о срочной поставке компонент, вышедших из строя и требующих замены в случае чрезвычайной ситуации.

Процесс реагирования на такого рода инциденты включает в себя четыре основных этапа:

- 1) Обнаружение нападения.
- 2) Локализация нападения.
- 3) Идентификация нападающих;
- 4) Оценка и последующий анализ процесса нападения и его обстоятельств.

2 Обнаружение атак и распознавание вторжений

Обнаружение атак и распознавание вторжений, как правило, является инженерно-технической задачей, решаемой при помощи специальных программных и иногда аппаратных средств. В частности, обнаружение может осуществляться на основе анализа сетевого трафика и журналов (лог-файлов), в которых фиксируются различные действия. Обнаружение может осуществляться на основе т.н. сигнатур – формализованных наборов признаков определенных вирусов, типов атак и пр. Также, очевидно, источником информации о нарушениях являются сообщения пользователей об отклонениях

в работе информационных систем и появление явных негативных последствий произошедших нарушений.

Для обеспечения своевременного обнаружения нарушений предприятие должно организовать постоянную (при необходимости – круглосуточную) работу специалистов, отвечающих за разрешение инцидентов. Для этого может быть выбран один из возможных подходов.

1) Организация собственной дежурной службы, состоящей из компетентных специалистов, несущих посменное дежурство и оснащенных средствами мобильной связи.

2) Привлечение сторонней организации, специализирующейся на оказании подобных услуг.

При этом сотрудники предприятия должны знать номера телефонов и иные способы связи, при помощи которых они могли бы оперативно сообщать дежурным специалистам обо всех происшествиях. Важность организации как можно более оперативного информирования специалистов по безопасности и, соответственно, как можно более оперативного реагирования обусловлена тем, что обнаружение нападения и начало противодействия в то время, как само нападение еще продолжается, в большинстве случаев может быть гораздо более эффективным, чем реагирование после окончания нападения.

Выявление нарушений может быть осуществлено не только по явным признакам, таким как сообщения пользователей о прекращении функционирования отдельных элементов информационных систем, одновременное использование одной учетной записи на нескольких рабочих станциях или явное обнаружение вирусов в данных, передаваемых по локальной сети, но и по некоторым косвенным признакам (аномальным явлениям), которые в отдельных случаях могут свидетельствовать (а могут и не свидетельствовать) о нарушениях. Примерами таких косвенных свидетельств могут быть:

– использование информационных систем и определенных учетных записей в нехарактерное время (рано утром, поздно вечером и пр.);

Тема 2.6 – Чрезвычайные ситуации (инциденты)
(Управление информационной безопасностью)

- резкое нехарактерное повышение нагрузки на информационные системы или их отдельные элементы (сегменты сети, хранилища данных и пр.);
- изменение характера поведения пользователей (например, последовательности определенных действий при использовании информационной системы) и пр.

Для более эффективного анализа таких косвенных признаков и интерпретации различных фактов специалистам по реагированию на инциденты может понадобиться анализ функциональности информационных систем и взаимодействие аналитиков департамента информационной безопасности с пользователями (изучение особенностей их работы). Также для автоматизации такого анализа могут быть использованы специальные программные средства, автоматически осуществляющие статистический анализ сетевого трафика и других элементов информационной инфраструктуры и сигнализирующие при обнаружении аномальной активности, для того чтобы администраторы могли провести дальнейший качественный анализ выявленных отклонений и при необходимости предпринять активные ответные действия. В целом, разработка и совершенствование таких средств анализа в составе комплексных систем обнаружения вторжений является одним из перспективных направлений развития средств защиты информации.

Таким образом, основной задачей на начальном этапе реагирования является определение характера нарушений и достоверное установление того, что выявленные аномальные события, действия и характеристики являются действительно нарушениями, а, например, не проявлением особенностей работы программного обеспечения.

Одним из важнейших организационных аспектов реагирования на инциденты (и, в частности, на отдельные сигналы о некоторых происшествиях) является то обстоятельство, что может происходить более или менее частое поступление ложных сигналов (ошибочных или специально спровоцированных) о некоторых происшествиях, и реакция персонала

департамента информационной безопасности со временем может постепенно ослабевать (так же как, например, может притупиться внимание при частых ложных срабатываниях охранной сигнализации). В частности, по оценке некоторых специалистов, в среднем в 90% случаев, когда пользователи сообщают о том, что, по их мнению, компьютер заражен вирусом, они ошибаются. В связи с этим при организации реагирования на инциденты необходимо уделить особое внимание психологической подготовке персонала, отвечающего за реагирование, а также по возможности анализировать причины появления таких ложных сигналов и предотвращать их в дальнейшем.

Также значимым вопросом организации работы с пользователями в ситуациях реагирования на инциденты является то, что взаимодействие между пользователями и группами реагирования, а также различных групп реагирования между собой по возможности необходимо осуществлять по специальным защищенным каналам связи.

3 Локализация и устранение последствий

Локализация и устранение последствий является основным этапом, в рамках которого, собственно, осуществляется реагирование на инцидент. На этом этапе происходит:

- определение конкретных параметров нарушения (нападения), его характера (конкретных сегментов сети, серверов, групп рабочих станций, приложений, затронутых нападением);
- предварительный анализ действий нарушителя и сценария произошедшего (происходящего) нападения, алгоритма работы появившегося вируса и пр.;
- блокирование действий нарушителя (если нарушение является длящимся);
- блокирование (полное или частичное) работы информационной системы (сервера, базы данных, сегмента сети и пр.) с целью недопущения

дальнейших разрушительных действий, распространения вредоносных программ или утечки конфиденциальной информации.

Прекращение нападения и восстановление нормальной работы информационных систем может потребовать скоординированных действий не только самих сотрудников департамента информационной безопасности, но и:

- специалистов ИТ-подразделений, отвечающих за атакуемые информационные сервисы;
- пользователей атакованных информационных систем;
- предприятий-партнеров, имеющих отношение к атакованным информационным ресурсам;
- разработчиков и поставщиков атакованных информационных систем;
- поставщиков телекоммуникационных услуг, через которых осуществляется атака;
- сторонних консультантов, специализирующихся на соответствующих проблемах информационной безопасности.

Одним из наиболее важных обстоятельств работы на данном этапе является то, какими полномочиями обладает специалист (дежурный), отвечающий за реагирование на инциденты. В частности, необходимо заранее предусмотреть возможность оперативного самостоятельного отключения тех или иных информационных сервисов специалистами по реагированию на инциденты (самостоятельно, либо через соответствующее ИТ-подразделение). Особую важность имеет способность ответственных специалистов оперативно оценить ситуацию, провести ее анализ (в большинстве практических ситуаций это необходимо будет делать по неполным данным о нападающей стороне) и принять решение о приостановке работы тех или иных информационных сервисов, до выявления и устранения угроз и/или введения в действие дополнительных средств противодействия вторжениям. При принятии такого решения необходимо учитывать (как правило, на основе экспертных оценок) как возможный ущерб, который может быть вызван выявленным нарушением,

так и возможный ущерб от остановки информационных сервисов, которая (остановка) может быть осуществлена с целью предотвращения ущерба от действий нападающей стороны. Характерным примером такой ситуации является нападение на систему электронной торговли, когда нападающая сторона может нанести серьезный ущерб (похитить конфиденциальную информацию участников торговых сделок, самостоятельно совершить незаконные сделки от имени участников торговой системы и пр.), а остановка сервиса с целью предотвращения такого ущерба может привести к потерям, связанным с упущенной выгодой от несовершенных сделок и ущербом для деловой репутации. Другим примером такой ситуации является реагирование на распределенные атаки типа "отказ в обслуживании" (Distributed Deny of Service, DDoS), часто осуществляемые на серверы в сети Интернет, когда может быть необходимо на некоторое время полностью отключить сервер как в ущерб пользователям, так и в ущерб владельцам информационных ресурсов, расположенных на сервере.

Основой для принятия решений может быть заранее сформированный перечень (справочник) возможных основных инцидентов и признаков нарушений (проникновений), в котором может быть приведена оценка рисков суммарных потерь и рекомендованные действия для каждого типа нарушений (в том числе и перечень ситуаций, когда необходимо осуществить отключение сервисов во избежание утечки или нарушения целостности информации, являющейся наиболее критичной для всей деятельности предприятия).

4 Идентификация нападающего

Идентификация нападающего (или источника распространения вредоносных программ) является важным шагом в процессе реагирования, следующим непосредственно за локализацией нападения. В случае если нападение осуществлялось из локальной сети предприятия, при надлежащем соблюдении внутренних режимных правил эта задача может оказаться относительно легкой. В случае если нападение было совершено извне, задача

идентификации нападающих принципиально усложняется и в некоторых ситуациях проблема становится практически неразрешимой.

Как правило, для обнаружения источника нападения необходимо:

- детально изучить все технические аспекты нападения;
- провести качественный анализ процесса нападения в контексте функционирования атакуемой системы защиты информации;
- организовать взаимодействие со сторонними организациями, которые могут содействовать в идентификации нападающего.

Одной из наиболее важных задач анализа процесса нападения является установление той информации, которая была известна нападающим до начала нападения и которой они воспользовались для осуществления этого нападения. В частности, в процессе такого анализа с определенной степенью уверенности можно установить, что до начала нападения злоумышленникам были известны:

- информация о структуре и составе атакуемой информационной системы (используемые программные и аппаратные средства, их архитектура и используемые настройки);
- сведения о режиме работы организации и функционирования отдельных элементов информационной системы. Сведения о регламенте некоторых бизнес-процессов предприятия;
- конкретные идентификационные данные (имена пользователей, пароли), необходимые для проникновения в информационную систему и/или правила (алгоритмы) их генерации.

Обобщение всех этих сведений может помочь установить, какие контакты были у нападающих с атакуемой компанией (а каких не было), и, сопоставляя факты, а также пользуясь методом исключения, постараться ограничить круг лиц, которые потенциально могли быть причастны к организации данного инцидента.

В свою очередь, проведение такого анализа будет возможно только в том случае, если все информационные системы и системы защиты информации

настроены надлежащим образом (в частности, в них ведутся все необходимые системные журналы) и системные данные не были повреждены в процессе нападения.

Вторым важным направлением организационной и аналитической работы при установлении (идентификации) нападающих, совершивших нападение извне, является взаимодействие с администраторами систем (телекоммуникационных сетей, компьютеров, использовавшихся в качестве прокси-серверов, и пр.), с использованием которых было осуществлено нападение. Подходы к такому взаимодействию в каждом конкретном случае, скорее всего, будут индивидуальными и могут зависеть от политики раскрытия информации администрации той сети или узла, через который осуществлялась атака. Также могут быть предприняты действия для того, чтобы в судебном порядке или с привлечением правоохранительных органов обязать администрации таких сетей и узлов предоставить необходимую информацию, связанную с произошедшим нападением.

Процесс идентификации должен по возможности проводиться с учетом того, что впоследствии необходимо будет использовать информацию о нападающих как доказательство в уголовном процессе. В частности, при снятии (копировании) необходимых лог-файлов с атакованных компьютеров представителями правоохранительных органов, ведущими следствие по данному делу, должны быть соблюдены все процессуальные формальности, предусмотренные уголовно-процессуальным законодательством. Одной из особенностей процедуры изъятия доказательств у потерпевшей стороны в этом случае является то, что понятые, присутствующие при изъятии, должны по возможности иметь хотя бы общее представление о смысле производимой процедуры. Также на этом этапе при необходимости может быть проведена технико-криминалистическая экспертиза компьютерных систем.

5 Оценка и анализ процесса нападения и его обстоятельств

Одним из заключительных шагов процесса реагирования на инцидент является оценка и анализ процесса нападения и его обстоятельств. Этот анализ необходимо проводить в контексте целей и задач функционирования всего предприятия, с учетом результатов работы по идентификации лиц, совершивших нападение. Основные задачи аналитической работы на данном этапе:

- анализ целей и мотивов, нападавших;
- анализ фундаментальных (организационных и технических) причин, которые сделали нападение возможным и успешным (если оно было успешным);
- анализ последствий (в том числе и долгосрочных) нападения для всей деятельности предприятия;
- анализ и оценка работы персонала и взаимоотношений с предприятиями-партнерами (в том числе и с поставщиками информационных систем и средств защиты информации).

Результатом анализа должны быть выводы, которые могут послужить основой для организационной работы в различных направлениях:

- корректировка и уточнение политики информационной безопасности предприятия;
- проведение дополнительной работы с персоналом предприятия (наказания, поощрения, дополнительное обучение и пр.);
- проведение дополнительной работы с персоналом департамента информационной безопасности предприятия, а также персоналом ИТ-служб;
- пересмотр взаимоотношений с контрагентами предприятия (покупателями, поставщиками, партнерами по НИОКР и пр.), имеющими доступ к его защищаемой информации или информационным системам;
- привлечение сторонних консультантов по информационной безопасности и специалистов по средствам защиты информации;

– инициирование технического переоснащения отдельных участков информационной инфраструктуры предприятия.

Таким образом, анализ и всесторонняя оценка инцидентов является отправной точкой для реализации комплекса мер по совершенствованию системы обеспечения информационной безопасности на предприятии. Все эти меры должны в будущем снизить вероятность аналогичных инцидентов, а также уменьшить вероятность нанесения существенного ущерба в случае их повторения.

Важной составляющей анализа нападения также является оценка ущерба от произошедшего нарушения информационной безопасности. Ущерб может быть оценен одновременно с нескольких точек зрения и зависит от характера возникшей внештатной ситуации. Наиболее простым для количественной экономической оценки является прямой ущерб: затраты на восстановление утраченной информации (могут быть рассчитаны на основе трудоемкости работ по восстановлению информации и данных о средней стоимости рабочего времени соответствующих специалистов), затраты на замену скомпрометированных паролей, кодов и ключей, стоимость поврежденного оборудования, штрафные санкции за разглашение конфиденциальной информации (если такие санкции, например, были предусмотрены договорами с подрядчиками, поставщиками или заказчиками) и пр. Также в оценке нуждается упущенная выгода, которая может быть связана как с непосредственным прекращением (приостановкой, замедлением) текущих операций предприятия, так и с долгосрочным (перспективным) негативным влиянием возникшей внештатной ситуации – потерей доверия к предприятию, приводящей к оттоку заказчиков, формированием негативного имиджа предприятия и пр. Отдельно также может быть оценено падение рыночной стоимости предприятия – его акций (если речь идет о предприятии, акции которого котируются на биржевом рынке).

Наиболее сложным для оценки является моральный ущерб и последствия от разглашения информации личного характера (например, сведений,

составляющих врачебную тайну). Конкретные суммы морального ущерба, как правило, могут быть установлены по результатам судебных разбирательств с отдельными лицами, которым такой ущерб был нанесен, либо процедур досудебного урегулирования конфликтов (на основе требований пострадавших лиц).

6 Заключительные этапы процесса реагирования

Заключительным этапом процесса реагирования также является устранение негативных последствий нападения – локализация ущерба, причиненного произошедшим нарушением. Эта работа может включать в себя:

- смену скомпрометированных паролей отдельных пользователей;
- переустановку поврежденных операционных систем, а также поврежденного программного обеспечения;
- восстановление нарушенной конфигурации (настроек) программного обеспечения и операционных систем;
- восстановление поврежденной информации (баз данных, файлов), как из ранее созданных резервных копий, так и другими способами.

В процессе восстановления работоспособности информационных систем на некоторое время могут быть задействованы резервные (альтернативные) аппаратные и программные платформы.

Кроме того, необходимым завершающим шагом может быть дополнительная информационная работа, которая может в себя включать:

- рассылку пользователям информации о произошедших инцидентах (в виде специальных писем и бюллетеней);
- передачу некоторых сведений о нападении в средства массовой информации;
- передачу сведений о нападении крупным группам реагирования на инциденты, связанные с информационной безопасностью (таким как, например, CERT/CC), а также в научно-исследовательские центры, занимающиеся проблемами защиты информации;

– дополнительную информационную работу с поставщиками информационных систем и подрядчиками, осуществлявшими их поставку, внедрение и настройку.

С точки зрения распределения обязанностей по выполнению отдельных функций в рамках процесса реагирования на инциденты, одним из эффективных и достаточно широко используемых подходов к организации реагирования на инциденты является построение централизованной системы реагирования на инциденты, когда одна группа реагирования обслуживает несколько подразделений или предприятий. В частности, такой подход реализован в Министерстве обороны США (он был описан в одной из предыдущих лекций), где несколько централизованных групп реагирования на инциденты обслуживают множество войсковых подразделений. Централизованные группы реагирования могут создаваться для обслуживания различных предприятий и организаций. Это могут быть компании, входящие в крупный холдинг, организации, входящие в одну исследовательскую сеть, университеты и исследовательские организации одной страны, клиенты поставщика определенных продуктов или услуг и т.д. Для объединения усилий различных групп реагирования был создан специальный Форум групп реагирования на инциденты и обеспечения безопасности (Forum of Incident Response and Security Teams, FIRST), на интернет сайте которого (<http://www.first.org/>) можно найти полный список его участников. При этом все функции по реагированию не могут быть переданы в централизованную группу реагирования – в каждом конкретном случае необходимо детально разграничить полномочия, ответственность и функции, выполняемые предприятием самостоятельно, и функции, выполняемые централизованной группой. Договоренность между централизованной группой реагирования и группой реагирования (специалистами по безопасности) самого предприятия должна предусматривать не только разграничение функций, но и описывать основные процедуры взаимодействия в процессе реагирования на инцидент.