НАУЧНЫЙ ЖУРНАЛ
НАУКА И МИРОВОЗЗРЕНИЕ

ПРОЦЕСС РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

Чарыева Дунягозел Джанмурадовна

Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Агаева Дурли Мовлямовна

Преподаватель, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Чуриев Максат Меретмухаммедович

Старший преподаватель кандидат технических наук, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

Аллалыева Селби Максадовна

Студент, Международного университета нефти и газа имени Ягшыгелди Какаева, г. Ашхабад Туркменистан

В предыдущей главе вы познакомились с тремя столпами, которые поддерживают ваш уровень безопасности, а два из них (обнаружение и реагирование) напрямую связаны с процессом реагирования на компьютерные инциденты. Чтобы укрепить основы своей безопасности, вам необходимо иметь четко выстроенный процесс реагирования на инциденты. Этот процесс будет определять, как обрабатывать инциденты в области безопасности и быстро реагировать на них. У многих компаний есть процесс реагирования на инциденты, но они не в состоянии постоянно пересматривать его, чтобы учесть уроки, извлеченные в ходе предыдущих инцидентов, и, кроме того, многие не готовы обрабатывать инциденты в облачной среде. В этой главе мы рассмотрим следующие темы:

-процесс реагирования на компьютерные инциденты;

-обработка инцидентов;

-деятельность после инцидента.

Процесс реагирования на компьютерные инциденты

Существует множество отраслевых стандартов, рекомендаций и передовых методик, которые могут помочь вам создать собственный ответ на инцидент. Вы по-прежнему можете использовать их в качестве справочных материалов, чтобы убедиться, что охватили все соответствующие этапы для своего типа бизнеса. В качестве справочного материала в этой книге мы будем использовать реагирование на инцидент в области компьютерной безопасности (CSIR) – публикация 800-61R2 из Национального института стандартов и технологий

Причины иметь в своем распоряжении процесс реагирования на компьютерные инциденты

Прежде чем углубиться в детали самого процесса, важно изучить терминологию, а также определить конечную цель при использовании реагирования на компьютерный инцидент как части улучшения стратегии безопасности. Почему это важно? Используем вымышленную компанию, чтобы дать ответ на этот вопрос.

На приведенном ниже рис. 1 показана временная шкала событий (2), которая заставляет службу технической поддержки информировать о проблеме и запускать процесс реагирования.

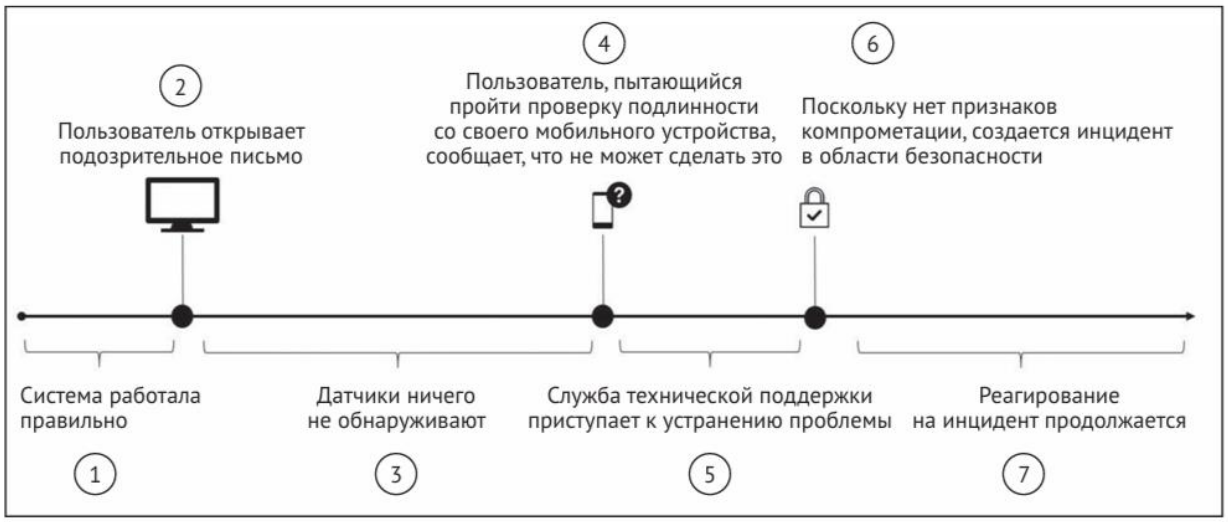

Рис. 1

В следующей таблице приведены некоторые соображения, касающиеся каждого шага в этом сценарии:

Шаг	Описание	Соображения по поводу безопасности
1	Хотя на диаграмме сказано, что система работает правильно, важно извлечь уроки из этого события	Что считается нормальным? У вас есть исходные данные, которые могут дать вам доказательства того, что система работает правильно? Вы уверены, что нет никаких доказательств компрометации до того, как письмо было открыто?
2	Фишинговые письма по-прежнему являются одним из наиболее распространенных методов, используемых киберпреступниками, чтобы побудить пользователей щелкнуть по ссылке, которая ведет на вредоносный/скомпрометированный сайт	В то время как в наличии должны быть технические средства безопасности для обнаружения и фильтрования данного типа атак, пользователей нужно научить идентифицировать фишинговые письма

Шаг	Описание	Соображения по поводу безопасности
3	Многие из традиционных датчиков (IDS/IPS), используемых в настоящее время, не способны идентифицировать инфильтрацию и дальнейшее распространение по сети	Чтобы повысить уровень безопасности, вам необходимо улучшить технические средства контроля безопасности и сократить разрыв между заражением и обнаружением
4	Это уже часть побочного ущерба, нанесенного этой атакой. Учетные данные были скомпрометированы, и у пользователя возникли проблемы с аутентификацией	Должны существовать технические средства контроля безопасности, позволяющие ИТ-специалистам сбрасывать пароль пользователя и в то же время обеспечивать многофакторную аутентификацию
5	Не каждый инцидент связан с безопасностью; поэтому важно, чтобы служба технической поддержки выполнила начальную диагностику с целью изолировать проблему	Если бы технические средства контроля безопасности (шаг 3) смогли идентифицировать атаку или, по крайней мере, предоставить какое-либо свидетельство подозрительной активности, службе технической поддержки не пришлось бы устранять проблему – она могла просто следовать за процессом реагирования
6	На данный момент служба технической поддержки делает то, что должна, собирает доказательства того, что система была скомпрометирована, и сообщает о проблеме	Служба технической поддержки должна получить как можно больше информации о подозрительной деятельности, чтобы обосновать причину, по которой они считают, что это инцидент, связанный с безопасностью
7	На этом этапе вступает в дело процесс реагирования на компьютерные инциденты. Он следует своим собственным путем, который может варьироваться в зависимости от компании, отраслевого сегмента и стандарта	Важно документировать каждый отдельный этап процесса и после разрешения инцидента учитывать извлеченные уроки с целью повышения общего уровня безопасности

Хотя в предыдущем сценарии есть много возможностей для улучшения, в этой вымышленной компании есть кое-что, чего не хватает многим другим компаниям во всем мире, – само реагирование на компьютерный инцидент. Если бы не процесс реагирования, специалисты службы технической поддержки исчерпали бы свои усилия по устранению неполадок, сосредоточившись на проблемах инфраструктуры. Компании, у которых есть хорошая стратегия безопасности, имеют в своем распоряжении процесс реагирования на инциденты.

Они также обеспечат соблюдение следующих рекомендаций:

- весь IT-персонал должен быть обучен, чтобы знать, как справиться с инцидентом в области безопасности;

- все пользователи должны быть обучены основам безопасности, чтобы выполнять свою работу качественно и избежать заражения;

- должна быть интеграция между системой технической поддержки и командой реагирования на инциденты, чтобы обмениваться данными;

- этот сценарий может иметь некоторые вариации, которые могут создать различные проблемы, требующие преодоления. Один из вариантов заключается в том, что на шаге 6 не будет обнаружено никаких признаков компрометации. В этом случае служба технической поддержки без труда продолжит устранение проблемы. Что, если в какой-то момент все снова заработает нормально? Это вообще возможно? Да, возможно;

- когда злоумышленник проникает в сеть, обычно он хочет оставаться невидимым, распространяя свое влияние дальше с одного хоста на другой, подвергая риску множество

систем и пытаясь повысить привилегии путем компрометации учетной записи с привилегиями уровня администратора. Вот почему так важно иметь хорошие датчики не только в сети, но и в самом хосте. При наличии хороших датчиков вы сможете не только быстро обнаружить атаку, но и определить потенциальные сценарии, которые могут привести к неизбежной угрозе нарушения

- в дополнение ко всем только что упомянутым факторам следует отметить, что некоторые компании скоро поймут, что им необходим процесс реагирования на компьютерные инциденты, чтобы соответствовать правилам, применимым к отрасли, к которой они относятся. Например, FISMA требует, чтобы федеральные агентства имели процедуры для обнаружения, сообщения и реагирования на инциденты в области безопасности.

Создание процесса реагирования на компьютерные инциденты

Хотя процесс реагирования на компьютерные инциденты зависит от компании и ее потребностей, существуют некоторые фундаментальные аспекты, которые будут одинаковыми в разных отраслях.

На приведенном ниже рис. 2 показаны основные области процесса реагирования на компьютерные инциденты.

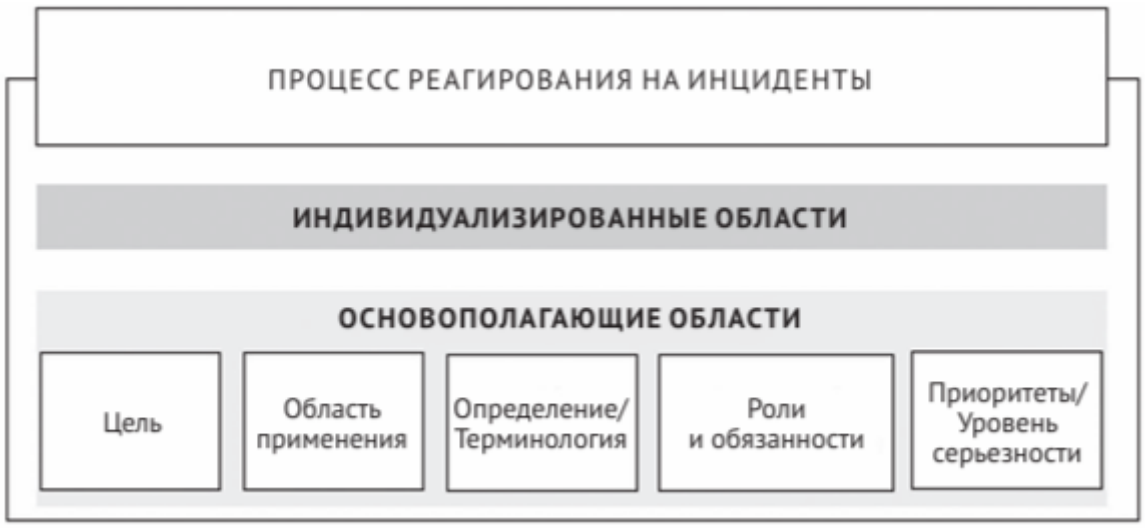

Рис. 2

Первый шаг для создания процесса реагирования на компьютерный инцидент – это определение цели. Другими словами, нужно ответить на вопрос: какова цель этого процесса? Хотя это может показаться лишним, т. к. название, кажется, говорит само за себя, важно очень четко понимать цель процесса, чтобы все знали о том, чего мы пытаемся добиться с его помощью.

Как только вы определили цель, вам нужно поработать над областью применения. И опять вы начинаете с ответа на вопрос, который в данном случае звучит так: к кому относится этот процесс?

Хотя процесс реагирования на компьютерные инциденты обычно охватывает всю компанию, в некоторых сценариях он может также охватывать отделы. По этой причине важно, чтобы вы определили, это процесс для всей компании или нет.

Каждая компания может по-разному воспринимать инцидент в области безопасности, поэтому крайне важно определить, что представляет собой этот инцидент, и привести примеры.

Наряду с этим компании должны создать свой собственный глоссарий с определениями используемой терминологии. Различные отрасли будут иметь разную терминологию. Если эти наборы терминов относятся к инциденту в области безопасности, они должны быть задокументированы.

В процессе реагирования на компьютерные инциденты роли и обязанности имеют решающее значение. Без надлежащего уровня полномочий весь процесс находится в опасности.

Важность уровня полномочий при реагировании на инциденты становится очевидной, если рассмотреть вопрос: у кого есть полномочия конфисковывать компьютер для проведения дальнейшего расследования? Определяя пользователей или группы с таким уровнем полномочий, вы гарантируете, что вся компания знает об этом, и если произойдет инцидент, группе, которая применяет эту политику, не будут задавать вопросы.

Когда инцидент признается критическим? Как вы будете распределять свою рабочую силу, когда произойдет инцидент? Следует ли выделить больше ресурсов для инцидента «А» по сравнению с инцидентом «В»? Почему? Это толь ко некоторые примеры вопросов, на которые нужно ответить, чтобы определить приоритеты и уровень опасности угрозы.