National Institute of
Standards and Technology
U.S. Department of Commerce

Специальная публикация 800-61
Пересмотр 2

Компьютерная безопасность Руководство по обработке инцидентов

Рекомендации национального института стандартов и технологий

Paul Cichonski
Tom Millar
TimGrance
Karen Scarfone

Специальная публикация NIST 800-61
Пересмотр 2

Руководство по обработке инцидентов компьютерной безопасности

Рекомендации Национального института стандартов и технологий

Paul Cichonski
Отдел компьютерной безопасности
Лаборатория информационных технологий
Национальный институт стандартов и технологий
Гейтерсбург, Мэриленд

Tom Millar
Команда готовности к компьютерным чрезвычайным ситуациям Соединенных Штатов
Национальный Отдел кибербезопасности
Министерство национальной безопасности

Tim Grance
Отдел компьютерной безопасности
Лаборатория информационных технологий
Национальный институт стандартов и технологий
Гейтерсбург, Мэриленд

Karen Scarfone
Scarfone Cybersecurity

КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Август 2012

Министерство торговли Соединённых штатов Америки

Rebecca Blank, ВРИО министра

Национальный институт стандартов и технологий

Patrick D. Gallagher,
Заместитель министра торговли по стандартам и технологиям и директор

Отчёты по технологиям компьютерных систем

Лаборатория информационных технологий (ITL) в Национальном институте стандартов и технологий (NIST) продвигает американскую экономику и общее благосостояние, обеспечивая техническое лидерство для национальной инфраструктуры измерений и стандартов. ITL разрабатывает тесты, методы испытаний, справочные данные, осуществляет подтверждения концепций реализации и технический анализ, чтобы продвинуть разработку и продуктивное использование информационных технологий. Обязанности ITL включают разработку управленческих, административных, технических и физических стандартов и руководств для обеспечения рентабельной безопасности и приватности информации не связанной с национальной безопасностью в федеральных информационных системах. Специальные публикации 800-серии содержат информацию относительно исследований, руководств и усилий ITL, направленных на повышение безопасности информационных систем, и её совместных работ с отраслями, правительством и академическими организациями.

Полномочия

Эта публикация была разработана NIST в соответствии с его обязанностями, установленными согласно Закону об управлении безопасностью федеральной информации (FISMA), Общественный закон (P.L). 107-347. NIST является ответственным за разработку стандартов и руководств по информационной безопасности, включая минимальные требования для федеральных информационных систем, но такие стандарты и руководства не должны применяться к системам национальной безопасности без специального санкционирования соответствующих федеральных должностных лиц, осуществляющих полномочия по таким системам. Это руководство непротиворечиво с требованиями Циркуляра A-130 Министерства управления и бюджета (OMB), Раздел 8b (3), *Обеспечение безопасности информационных систем агентств*, как указано в Циркуляре A-130, Приложение IV: *Анализ ключевых разделов*. Дополнительная информация предоставлена в Циркуляре A-130, Приложение III, *Безопасность федеральных автоматизированных информационных ресурсов*.

Ничто в этой публикации не должно использоваться в противоречие со стандартами и руководствами, определёнными Министром торговли в соответствие с его законными полномочиями как обязательные для федеральных агентств. Также, это руководство не должно быть интерпретировано как изменение или замена существующих полномочий Министра торговли, Директора OMB или какого-либо другого федерального должностного лица. Это руководство было подготовлено к использованию федеральными агентствами. Эта публикация может быть также использована на добровольной основе неправительственными организациями и это не попадает по действие авторского права. Однако упоминание приветствовалось бы NIST.

Специальная публикация Национального института стандартов и технологий 800-61 Пересмотр 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-61 Revision 2, 79 pages (Aug. 2012) CODEN: NSPUE2
CODEN: NSPUE2

Некоторые коммерческие сущности, оборудование или материалы могут быть указаны в этом документе, чтобы описать экспериментальную процедуру или концепцию соответственно. Такое указание не предназначено, чтобы означать рекомендацию или одобрение NIST, а также оно не предназначено, чтобы означать, что сущности, материалы или оборудование - обязательно наилучшие имеющиеся по предназначению.

В этой публикации могут быть ссылки на другие разрабатываемые в настоящее время публикации NIST в соответствии с возложенными на него обязанностями, установленными законом. Информация в этой публикации, включая концепции и методологию, может использоваться Федеральными агентствами ещё до завершения этих сопутствующих публикаций. При этом, пока каждая публикация не завершена, продолжают применяться текущие требования, руководства и процедуры, где они существуют. Для целей планирования и обеспечения перехода, Федеральные агентства могут тесно следить за разработкой NIST этих новых публикаций.

Организации поощрены рассматривать все предварительные публикации во время периодов публичного обсуждения и предоставлять обратную связь NIST. Все публикации NIST, помимо указанных выше, доступны по http://csrc.nist.gov/publications.

Комментарии к этой публикации могут быть представлены в:

Национальный институт стандартов и технологий
Для: Отдел компьютерной безопасности, лаборатория информационных технологий
100 Bureau Drive (Mail Stop 8930), Gaithersburg, MD 20899-8930

Резюме

Реагирование на инциденты компьютерной безопасности стало важным компонентом программ по информационным технологиям (ИТ). Поскольку выполнение эффективного реагирования на инциденты является сложным мероприятием, установление успешной способности реагирования на инциденты требует существенного планирования и ресурсов. Эта публикация помогает организациям в установлении способности по реагированию на инциденты компьютерной безопасности и обработке инцидентов эффективно и продуктивно. Эта публикация предоставляет руководство по обработке инцидентов, особенно для анализа связанных с инцидентами данных и определения соответствующей реакции на каждый инцидент. Руководство может использоваться независимо от конкретных аппаратных платформ, операционных систем, протоколов или приложений.

Ключевые слова

инцидент компьютерной безопасности; обработка инцидента; реагирование на инциденты; информационная безопасность

Признательность

Авторы, Paul Cichonski из Национального института стандартов и технологий (NIST), Tom Millar из Компьютерной команды готовности к чрезвычайным ситуациям Соединенных Штатов (US-CERT), Tim Grance из NIST и Karen Scarfone из Scarfone Cybersecurity хотят поблагодарить своих коллег, которые пересмотрели проекты этого документа и способствовали его техническому содержанию, включая John Banghart из NIST; Brian Allen, Mark Austin, Brian DeWyngaert, Andrew Fuller, Chris Hallenbeck, Sharon Kim, Mischel Kwon, Lee Rock, Richard Struse, and Randy Vickers из US-CERT; и Marcos Osorno из Лаборатории прикладной физики университета Джонса Хопкинса. Специальное признание адресуется Brent Logan из US-CERT за его графическую помощь. Авторы также хотели бы поблагодарить специалистов по безопасности Simon Burson, Anton Chuvakin (Gartner), Fred Cohen (Fred Cohen & Associates), Mariano M. del Rio (SIClabs), Jake Evans (Tripwire), Walter Houser (SRA), Panos Kampanakis (Cisco), Kathleen Moriarty (EMC), David Schwalenberg (National Security Agency), and Wes Young (Research and Education Networking Information Sharing and Analysis Center [REN-ISAC]), а также представителей Blue Glacier Management Group, Центров по контролю и профилактике заражений, Министерства энергетики, Госдепартамента и Федерального управления авиации за их особенно ценные комментарии и предложения.

Авторы также хотели бы выразить признательность людям, которые способствовали предыдущим версиям публикации. Особая благодарность адресуется Brian Kim из Booz Allen Hamilton, который создал в соавторстве исходную версию; Kelly Masone из Blue Glacier Management Group, которая создала в соавторстве первый пересмотр; а также Rick Ayers, Chad Bloomquist, Vincent Hu, Peter Mell, Scott Rose, Murugiah Souppaya, Gary Stoneburner, and John Wack из NIST; Don Benack and Mike Witt из US-CERT; и Debra Banning, Pete Coleman, Alexis Feringa, Tracee Glass, Kevin Kuhlkin, Bryan Laird, Chris Manteuffel, Ron Ritchey, and Marc Stevens из Booz Allen Hamilton для их острую и проницательную помощь в течение разработки документа, а также Ron Banerjee and Gene Schultz за их работу над предварительным проектом документа. Авторы также хотели бы выразить их благодарность специалистам по безопасности Tom Baxter (NASA), Mark Bruhn (Indiana University), Brian Carrier (CERIAS, Purdue University), Eoghan Casey, Johnny Davis, Jr. (Department of Veterans Affairs), Jim Duncan (BB&T), Dean Farrington (Wells Fargo Bank), John Hale (University of Tulsa), Georgia Killcrece (CERT®/CC), Barbara Laswell (CERT®/CC), Pascal Meunier (CERIAS, Purdue University), Jeff Murphy (University of Buffalo), Todd O'Boyle (MITRE), Marc Rogers (CERIAS, Purdue University), Steve Romig (Ohio State University), Robin Ruefle (CERT®/CC), Gene Schultz (Lawrence Berkeley National Laboratory), Michael Smith (US-CERT), Holt Sorenson, Eugene Spafford (CERIAS, Purdue University), Ken van Wyk, и Mark Zajicek (CERT®/CC), а также представителям Департамента Казначейства, за их особенно ценные комментарии и предложения.

Оглавление

Резюме..... 1

1. Введение 4

1.1 Полномочия..... 4
1.2 Назначение и область..... 4
1.3 Аудитория..... 4
1.4 Структура документа..... 4

2. Организация возможности реагирования на инциденты компьютерной безопасности..... 6

2.1 События и инциденты..... 6
2.2 Потребность в реагировании на инциденты..... 6
2.3 Создание политики, плана и процедур реагирования на инциденты..... 7
2.3.1 Элементы политики..... 7
2.3.2 Элементы плана..... 8
2.3.3 Элементы процедур..... 8
2.3.4 Обмен информацией с внешними сторонами..... 9
2.4 Структура команды реагирования на инциденты..... 13
2.4.1 Модели команды..... 13
2.4.2 Выбор модели команды..... 14
2.4.3 Персонал реагирования на инциденты..... 16
2.4.4 Зависимости в организациях..... 17
2.5 Услуги команды реагирования на инциденты..... 18
2.6 Рекомендации..... 19

3. Обработка инцидентов..... 21

3.1 Подготовка..... 21
3.1.1 Подготовка к обработке инцидентов..... 21
3.1.2 Предотвращение инцидентов..... 23
3.2 Обнаружение и анализ..... 25
3.2.1 Векторы атак..... 25
3.2.2 Признаки инцидента..... 26
3.2.3 Источники предшественников и индикаторов..... 27
3.2.4 Анализ инцидента..... 28
3.2.5 Документация инцидента..... 30
3.2.6 Назначение приоритетов инцидента..... 32
3.2.7 Уведомление об инциденте..... 33
3.3 Сдерживание, уничтожение и восстановление..... 35
3.3.1 Выбор стратегии сдерживания..... 35
3.3.2 Сбор свидетельства и обработка..... 36
3.3.3 Идентификация нападающих хозяев..... 37
3.3.4 Уничтожение и восстановление..... 37
3.4 Работа постинцидента..... 38
3.4.1 Извлечение уроков..... 38
3.4.2 Использование собранных данных об инциденте..... 39
3.4.3 Сохранение свидетельств..... 41
3.5 Контрольный список по обработке инцидента..... 42
3.6 Рекомендации..... 42

4. Координация и совместное пользование информацией..... 45

4.1 Координация..... 45
4.1.1 Отношения координации..... 46
4.1.2 Соглашения по обмену и требования к отчетности..... 47
4.2 Технологии совместного пользования информацией..... 48
4.2.1 Специальная..... 48
4.2.2 Частично автоматизированная..... 48
4.2.3 Рассмотрения безопасности..... 49
4.3 Разделённое совместное пользование информацией..... 49
4.3.1 Информация, влияющая на деятельность..... 49
4.3.2 Техническая информация..... 50
4.4 Рекомендации..... 51

Список приложений

Приложение A — Сценарии обработки инцидента..... 52
1 Вопросы по сценариям..... 52
2 Сценарии..... 53
Приложение B — Элементы данных, связанные с инцидентом..... 58
B.1 Элементы исходных данных..... 58
B.2 Элементы данных обработчика инцидента..... 59
Приложение C — Глоссарий..... 60
Приложение D — Акронимы..... 61
Приложение E — Ресурсы..... 63
Приложение F — Часто задаваемые вопросы..... 65
G приложения — Шаги кризисной обработки..... 68
Приложение H — Журнал изменений..... 69

Список иллюстраций

Рисунок 2-1. Связи с внешними сторонами.....
Рисунок 3-1. Жизненный цикл реагирования на инциденты.....
Рисунок 3-2. Жизненный цикл реагирования на инциденты (Обнаружение и анализ).....
Рисунок 3-3. Жизненный цикл реагирования на инциденты (Сдерживание, уничтожение и восстановление).....
Рисунок 3-4. Жизненный цикл реагирования на инциденты (Работа постинцидента).....
Рисунок 4-1. Координация реагирования на инциденты.....

Список таблиц

Таблица 3-1. Общие источники предшественников и индикаторов 27
Таблица 3-2. Функциональные категории воздействия 33
Таблица 3-3. Информационные категории воздействия 33
Таблица 3-4. Категории усилия по восстанавливаемости 33
Таблица 3-5. Контрольный список обработки инцидента 42
Таблица 4-1. Отношения координации 47

Резюме

Реагирование на инциденты компьютерной безопасности стало важным компонентом программ по информационным технологиям (IT). Атаки, связанные с кибербезопасностью, стали не только более многочисленными и разнообразными, но также и более разрушительными и подрывными. Часто появляются новые типы связанных с безопасностью инцидентов. Профилактические работы на основе результатов оценок степени риска могут понизить число инцидентов, но не все инциденты могут быть предотвращены. Поэтому необходима способность реагирования на инциденты для того, чтобы быстро обнаружить инциденты, минимизировать потери и разрушения, сократить те слабые места, которые использовались, и восстановить ИТ-услуги. С этой целью эта публикация предоставляет руководство по обработке инцидентов, особенно для анализа связанных с инцидентом данных и определения соответствующей реакции на каждый инцидент. Руководству можно следовать независимо от конкретных аппаратных платформ, операционных систем, протоколов или приложений.

Поскольку эффективное выполнение реагирования на инциденты является сложным мероприятием, обеспечение возможности успешного реагирования на инциденты требует существенного планирования и ресурсов. Важен постоянный мониторинг атак. Очень важно установление четких процедур для приоритизации обработки инцидентов, с целью реализации эффективных методов сбора, анализа и сообщения о данных. Также жизненно важно построить отношения и установить подходящие средства общения с другими внутренними группами (например, людскими ресурсами, юристами) и с внешними группами (например, другими командами реагирования на инциденты, правоохранительными органами).

Эта публикация помогает организациям в установлении возможностей по реагированию на инциденты компьютерной безопасности и обработке инцидентов эффективно и продуктивно. Этот пересмотр публикации, Пересмотр 2, обновляет материал всюду по публикации, чтобы отразить изменения в атаках и инцидентах. Понимание угроз и идентификация современных атак на их ранних стадиях является ключевым к предотвращению последующих компрометаций, а ранний обмен информацией между организациями относительно признаков этих атак является все более и более эффективным способом их определения.

Реализация следующих требований и рекомендаций должна облегчить эффективное и продуктивное реагирование на инциденты для Федеральных департаментов и агентств.

Организации должны создать, обеспечить и управлять формальной способностью реагирования на инциденты. Федеральный закон требует, чтобы Федеральные агентства сообщали об инцидентах Команде готовности к компьютерной чрезвычайной ситуации Соединенных Штатов (US-CERT), подразделению Министерства национальной безопасности (DHS).

Федеральный закон об управлении информационной безопасностью (FISMA) требует, чтобы Федеральные агентства установили способность реагирования на инциденты. Каждое федеральное гражданское агентство должно определить основную и вторичную точку контакта (POC) с US-CERT и сообщать обо всех инцидентах в соответствии с политикой реагирования на инциденты агентства. Каждое агентство ответственно за определение, как выполнить эти требования.

Установление способности реагирования на инциденты должно включать следующие действия:

- Создание политики и плана реагирования на инциденты
- Разработка способов для выполнения обработки инцидентов и представления отчётов
- Установление руководств для связи с внешними сторонами относительно инцидентов
- Выбор структуры команды и модели персонала
- Установление отношений и линий связи между командой реагирования на инциденты и другими группами, как внутренними (например, юридический департамент) так и внешними (например, правоохранительные органы)
- Определение, какие сервисы должна обеспечивать команда реагирования на инциденты
- Укомплектование персоналом и обучение команды реагирования на инциденты.

Организации должны уменьшить частоту инцидентов, эффективно обеспечив безопасность сетей, систем и приложений.

Предотвращение проблем часто менее дорогостояще и более эффективно, чем реагирование на них после того, как они произойдут. Таким образом предотвращение инцидентов - важное дополнение к способности реагирования на инциденты. Если меры безопасности недостаточны, могут произойти большие объемы инцидентов. Это может сокрушить ресурсы и возможность для реакции, что приведет к задержанному или неполному восстановлению и возможно более значительному ущербу и более длинным периодам отсутствия данных и сервисов. Обработка инцидентов может быть выполнена эффективнее, если организации дополняют свою способность реагирования на инциденты адекватными ресурсами, чтобы активно сопровождать безопасность сетей, систем и приложений. Это включает обучение персонала ИТ по исполнению стандартов обеспечения безопасности организации и формированию пользователей, знающих о политиках и процедурах относительно соответствующего использования сетей, систем и приложений.

Организации должны зарегистрировать свои руководства по взаимодействию с другими организациями относительно инцидентов.

Во время обработки инцидентов организация должна будет общаться с внешними сторонами, такими как другие команды реагирования на инциденты, правоохранительные органы, средства информации, продавцы и пострадавшие организации. Поскольку это взаимодействие часто должно происходить быстро, организации должны предопределить руководства по взаимодействию таким образом, чтобы делиться с другими сторонами только соответствующей информацией.

Организации должны быть обычно готовы обращаться с любым инцидентом, но должны сосредоточиться на том, чтобы быть готовым обращаться с инцидентами, которые используют общие векторы атаки.

Инциденты могут произойти бесчисленными способами, таким образом, невозможно разработать пошаговые инструкции для обработки каждого инцидента. Эта публикация определяет несколько типов инцидентов, на основе общих векторов атак; эти категории не предназначены, чтобы предоставить категорическую классификацию для инцидентов, а скорее должны использоваться в качестве основания для определения более конкретных процедур обработки. Различные типы инцидентов требуют различных стратегий ответа. Векторами атак являются:

Внешние/съемные носители: нападение, выполняемое со съемных носителей (например, флеш-накопитель, CD) или периферийных устройств.
Истощение: нападение, которое использует методы грубой силы, чтобы компрометировать, ухудшать или разрушать системы, сети или сервисы.
Web: нападение, выполняемое из вебсайта или веб-приложения.
Электронная почта: нападение, выполняемое с помощью электронного письма или приложения.
Несоответствующее использование: Любой инцидент, следующий из нарушения использования авторизованным пользователем приемлемых политик организации, исключая вышеупомянутые категории.
Потеря или кража оборудования: потеря или кража вычислительного устройства или носителя информации, используемого организацией, такого как ноутбук или смартфон.
Другое: Нападение, которое не вписывается ни в одну из этих категорий.

Организации должны подчеркивать важность обнаружения и анализа инцидентов всюду по организации.

В организации каждый день могут происходить миллионы возможных признаков инцидентов, регистрируемых, в основном, в журналах и программном обеспечении компьютерной безопасности. Автоматизация необходима, чтобы выполнить начальный анализ данных и выбор представляющих интерес мероприятий для рассмотрения людьми. Программное обеспечение корреляции событий может иметь большое значение в автоматизации аналитического процесса. Однако эффективность процесса зависит от качества данных, которые входят в него. Организации должны установить стандарты и процедуры регистрации, чтобы гарантировать, что журналами регистрации и защитным

программным обеспечением собирается достоверная информация и что данные регулярно пересматриваются.

Организации должны создать письменные руководства для приоритизации инцидентов.

Приоритизация обработки отдельных инцидентов является критическим моментом принятия решений в процессе реагирования на инциденты. Эффективное совместное пользование информации может помочь организации определять ситуации, которые имеют большую серьезность и требуют пристального внимания. Инциденты должны быть расположены по приоритетам на основе соответствующих факторов, таких как функциональное воздействие инцидента (например, текущее и вероятное будущее негативное воздействие на функции деятельности), информационное воздействие инцидента (например, воздействие на конфиденциальность, целостность и доступность информации организации), и восстанавливаемость от инцидента (например, время и типы ресурсов, которые должны быть потрачены на восстановление от инцидента).

Организации должны использовать процесс изучения уроков, чтобы получить значение от инцидентов.

После того, как серьёзный инцидент был обработан, организация должна провести изучение полученных уроков, чтобы рассмотреть эффективность обработки инцидента и определить необходимые улучшения существующих мер и методов безопасности. Изучение полученных уроков может также периодически проводиться для меньших инцидентов, если позволяют ресурсы и время. Информация, накопленная от изучения всех полученных уроков должны использоваться, чтобы определить и исправить слабые места систем и недостатки в политиках и процедурах. Последующие отчеты, генерируемые для каждого решённого инцидента, могут быть важны не только для их основного предназначения, но также и для использования при обработке будущих инцидентов и в обучении новых членов команды.

1. Введение

1.1. Полномочия

Национальный институт стандартов и технологий (NIST) разработал этот документ в содействии с его установленными законом обязанностями согласно Федеральному закону об управлении информационной безопасностью (FISMA) 2002, Общественный закон 107-347.

NIST ответственен за разработку стандартов и руководств, включая минимальные требования по обеспечению требуемой безопасности информации для деятельности и активов всех агентства, но такие стандарты и руководства не должны относиться к системам национальной безопасности. Это руководство непротиворечиво с требованиями Министерства управления и бюджета (OMB), Циркуляр A-130, Раздел 8b (3), “Обеспечение безопасности информационных систем Агентств”, как анализируется в A-130, Приложении IV: Анализ ключевых секций. Дополнительная информация предоставлена в A-130, Приложении III.

Это руководство было подготовлено к использованию Федеральными агентствами. Оно может быть используемо неправительственными организациями на добровольной основе и не охраняется законом об авторском праве, хотя ссылки на него желательны.

Ничто в этом документе не должно быть взято, чтобы противоречить стандартам и руководствам, сделанным обязательными и предназначенными для Федеральных агентств министром торговли в соответствии с его законными полномочиями, и при этом эти руководства не должны интерпретироваться как изменение или замена существующих полномочий министра торговли, директора OMB или любого другого Федерального должностного лица.

1.2. Назначение и область

Эта публикация стремится помочь организациям в снижении рисков от инцидентов компьютерной безопасности, предоставляя практические руководства по реагированию на инциденты эффективно и рационально. Она включает руководство по установлению эффективной программы реагирования на инциденты, но основное внимание документа - обнаружение, анализ, приоритизация и обработка инцидентов. Организации поощрены адаптировать рекомендуемые руководства и решения с учётом их конкретных требований к безопасности и предназначению.

1.3. Аудитория

Этот документ был создан для команд реагирования на инциденты компьютерной безопасности (CSIRTs), системных и сетевых администраторов, служб безопасности, персонала технической поддержки, директоров по ИТ-безопасности (CISOs), директоров по информации (CIOs), диспетчеров программ компьютерной безопасности и других, которые ответственны за подготовку к, или реагирование на, инциденты безопасности.

1.4. Структура документа

Остаток от этого документа организован в следующие разделы и приложения:

Раздел 2 обсуждает потребность в реагировании на инциденты, выделяет возможные структуры команды реагирования на инциденты и подчеркивает другие группы в организации, которые могут участвовать в обработке инцидентов.

Раздел 3 рассматривает основные шаги обработки инцидентов и предоставляет консультации для выполнения более эффективной обработки инцидентов, особенно обнаружения и анализа инцидентов.

Раздел 4 исследует потребность в координации реагирования на инциденты и совместном пользовании информацией.

Приложение A содержит сценарии реагирования на инциденты и вопросы для использования в настольных обсуждениях реагирования на инциденты.

Приложение B предоставляет списки предложенных полей данных, для сбора по каждому инциденту.

Приложения C и D содержат глоссарий и список акронимов, соответственно.

Приложение E определяет ресурсы, которые могут быть полезными в планировании и выполнении реагирования на инциденты.

Приложение F закрывает часто задаваемые вопросы по реагированию на инциденты.

Приложение G перечисляет главные шаги, которым нужно следовать при обработке критической ситуации компьютерной безопасности, связанной с инцидентом.

Приложение H содержит журнал изменений, перечисляющий существенные изменения, начиная с предыдущего пересмотра.

2. Организация способности реагирования на инциденты компьютерной безопасности

Организация эффективной способности реагирования на инциденты компьютерной безопасности (CSIRC) включает несколько важных решений и действий. Одним из первых рассмотрений должно быть формирование конкретного для организации определения термина «инцидент» таким образом, чтобы была ясна область термина. Организация должна решить, какие сервисы должна предоставить команда реагирования на инциденты, рассмотреть, какие структуры и модели команды могут предоставить эти сервисы, и выбрать и реализовать одну или несколько команд реагирования на инциденты. Создание плана, политики и процедур реагирования на инциденты - важная часть установления команды, так, чтобы реагирование на инциденты было выполнено эффективно, разумно и последовательно, и так, чтобы команда была уполномочена сделать то, что необходимо сделать. План, политики и процедуры должны отразить взаимодействия команды с другими командами в организации, а также с внешними сторонами, такими как правоохранительные органы, средства информации и другие организации реагирования на инциденты. Этот раздел предоставляет не только руководства, которые должны быть полезны организациям, которые устанавливают способности реагирования на инциденты, но также и советы относительно поддержания и усиления существующих способностей.

2.1. События и инциденты

Событие - любая существенная ситуация в системе или сети. События включают пользователя, соединяющегося с общим файлом, сервер, получающий запрос о веб-странице, пользователя, посылающего электронное письмо и межсетевой экран, блокирующий попытку подключения. *Неблагоприятные события* - события с негативным последствием, такие как крах системы, пакетный флуд, несанкционированное использование системных привилегий, несанкционированный доступ к чувствительным данным и выполнение вредоносного программного обеспечения, которое разрушает данные. Это руководство учитывает только неблагоприятные события, которые связаны с компьютерной безопасностью, а не вызванные стихийными бедствиями, перебоями в питании, и т.д.

Инцидент компьютерной безопасности - нарушение или непосредственная угроза нарушения[1] политик компьютерной безопасности, политик допустимого использования или методов стандартной защиты. Примеры инцидентов[2]:

- Нападавший даёт команду боту послать большие объемы запросов на взаимодействие к веб-серверу, заставляя его потерпеть крах.
- Пользователи обмануты при открытии «квартального отчета», посланного по электронной почте, который является на самом деле вредоносным программным обеспечением; запуск инструмента привёл к заражению их компьютеров и установлению связи с внешним хостом.
- Нападавший получает чувствительные данные и угрожает тем, что детали будут представлены публично, если организация не заплатит определяемую денежную сумму.
- Пользователь предоставляет или выставляет чувствительную информацию другим через одноранговые сервисы совместного доступа к файлам.

2.2. Потребность в реагировании на инциденты

Атаки часто ставят под угрозу персональные данные и бизнес-данные, и очень важно реагировать быстро и эффективно, когда происходят нарушения защиты. Концепция реагирования на инциденты компьютерной безопасности стала широко принятой и осуществляемой. Одно из преимуществ наличия способности реагирования на инциденты - то, что она поддерживает системное реагирование на инциденты (т.е., следование непротиворечивой методологии обработки инцидента) так, чтобы были

[1] “Непосредственная угроза нарушения” относится к ситуации, в которой у организации есть фактическое основание для уверенности в том, что конкретный инцидент должен произойти. Например, обновления антивирусного программного обеспечения могут содержать бюллетень от программного вендора, предупреждающий о новом вредоносном программном обеспечении, которое быстро распространяется через Интернет.

[2] Для остатка от этого документа термины «инцидент» и “инцидент компьютерной безопасности” взаимозаменяемы.

приняты соответствующие меры. Реагирование на инциденты помогает персоналу минимизировать потерю или кражу информации и разрушение сервисов, вызванные инцидентами. Другая выгода реагирования на инциденты - способность использовать информацию, полученную во время обработки инцидентов, чтобы лучше подготовиться к обработке будущих инцидентов и обеспечить более стойкую защиту для систем и данных. Способность реагирования на инциденты также помогает правильно обращаться с юридическими вопросами, которые могут возникнуть во время инцидентов.

Помимо коммерческих причин установить способность реагирования на инциденты, Федеральные департаменты и агентства должны выполнять законы, нормативные документы и политику, направляющие скоординированную, эффективную защиты против угроз информационной безопасности. Главные среди них - следующие:

- Циркуляр № A-130 OMB, Приложение III,[3] выпущенный в 2000г., который направляет Федеральные агентства на "гарантирование того, что имеется возможность предоставить помощь пользователям, когда инцидент безопасности происходит в системе, и поделиться информацией относительно общих уязвимостей и угроз. Эта способность должна обеспечивать обмен информацией с другими организациями … и должна помочь агентству в рассмотрении соответствующего судебного иска, непротиворечивого с руководством Министерства юстиции".
- FISMA (с 2002),[4] который требует, чтобы у агентств были "процедуры обнаружения, информирования и ответа на инциденты безопасности", и основывает централизованный Федеральный центр инцидентов информационной безопасности, в частности для:
  - "Предоставления своевременной технической помощи операторам информационных систем агентства … включая руководство по обнаружению и обработке инцидентов информационной безопасности …
  - Сбора и анализа информации об инцидентах, которые угрожают информационной безопасности
  - Сообщения операторам информационных систем агентства о текущих и потенциальных угрозах информационной безопасности и уязвимостях …".
- Стандарт обработки федеральной информации (FIPS) 200, *Минимальные требования безопасности для Федеральной информации и информационных систем*[5], март 2006, который определяет минимальные требования безопасности для Федеральной информации и информационных систем, включая реагирование на инциденты. Конкретные требования определены в NIST Специальная Публикация (SP) 800-53, *Рекомендуемые меры безопасности для Федеральных информационных систем и организаций*.
- Меморандум M-07-16 OMB, *Защита от и реагирование на нарушения персональной идентификационной информации*[6], май 2007, который дает представление о информировании об инцидентах безопасности, которые включают ПИИ.

2.3. Создание политики, плана и процедур реагирования на инциденты

Этот раздел обсуждает политики, планы и процедуры, связанные с реагированием на инциденты, с акцентом на взаимодействие с внешними сторонами.

2.3.1.1. Элементы политики

Политики управления реагированием на инциденты высоко индивидуализированы к организации. Однако большинство политик включает одни и те же основные элементы:

- Описание приверженности руководства
- Назначение и цели политики

[3] http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
[4] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
[5] http://csrc.nist.gov/publications/PubsFIPS.html
[6] http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

- Область политики (к кому и к чему она применяется и при каких обстоятельствах),
- Определение инцидентов компьютерной безопасности и связанных терминов
- Организационная структура и определение ролей, обязанностей и уровней полномочия; должна включать полномочия команды реагирования на инциденты по конфискации или отключению оборудования и по мониторингу подозрительной активности, требования по информированию об определенных типах инцидентов, требования и руководства по внешним связям и совместному пользованию информацией (например, что может быть разделено с кем, когда и по каким каналам), и указания по передаче и эскалации в процессе управления инцидентами
- Назначение приоритетов или рейтингов серьезности инцидентов
- Критерии качества работы (как обсуждено в Разделе 3.4.2)
- Формы отчётов и контактов.

2.3.2. Элементы плана

У организаций должны быть формализованный, сконцентрированный и согласованный подход к реагированию на инциденты, включая план реагирования на инциденты, который предоставляет путеводитель для реализации способности реагирования на инциденты. Каждой организации нужен план, который отвечает её уникальным требованиям, который касается предназначения, размера, структуры и функций организации. План должен предоставлять необходимые ресурсы и поддержку руководства. План реагирования на инциденты должен включать следующие элементы:

- Предназначение
- Стратегии и цели
- Санкционирование высшего руководства
- Подход организации к реагированию на инциденты
- Как команда реагирования на инциденты будет общаться с остальной частью организации и с другими организациями
- Метрики для измерения способности реагирования на инциденты и ее эффективности
- Путеводитель для наращивания способности реагирования на инциденты
- Как программа вписывается во всю организацию.

Предназначение, стратегии и цели организации по реагированию на инциденты должны помочь в определении структуры её способности реагирования на инциденты. Структура программы реагирования на инциденты должна также быть обсуждена в плане. Раздел 2.4.1 обсуждает типы структур.

Как только организация разрабатывает план и получает санкционирование руководства, организация должна реализовать план и пересматривать его, по крайней мере, ежегодно, чтобы гарантировать, что организация следует за путеводителем для наращивания способности и выполнения её целей по реагированию на инциденты.

2.3.3. Элементы процедур

Процедуры должны быть основаны на политике и плане реагирования на инциденты. Стандартные режимы работы (SOPs) являются представлением конкретных технических процессов, технологий, контрольных списков и форм, используемых командой реагирования на инциденты. SOPs должны быть довольно всесторонними и подробными, чтобы гарантировать, что приоритеты организации отражены в деятельности по реагированию. Кроме того, соответствующие стандартизированные реакции должны минимизировать ошибки, особенно те, которые могли бы быть вызваны напряженными ситуациями обработки инцидента. SOPs должны быть проверены, чтобы подтвердить

их точность и полноценность, затем распределены по всем членам команды. Пользователям SOP должно быть предоставлено обучение; документы SOP могут использоваться в качестве учебного инструмента. Предложенные элементы SOP представлены в Разделе 3.

2.3.4. Обмен информацией с внешними сторонами

Организации часто должны общаться с внешними сторонами относительно инцидентов, и они должны делать это когда соответствующе, например, контактирование с правоохранительными органами, удовлетворение запросов средств информации и поиск внешних экспертных знаний. Другим примером является обсуждение инцидентов с другими участвующими сторонами, такими как поставщики интернет-услуг (ISPs), продавцы уязвимого программного обеспечения или другие команды реагирования на инциденты. Организации могут также заранее делиться соответствующей индикаторной информацией инцидентов с коллегами, чтобы улучшить обнаружение и анализ инцидентов. Команда реагирования на инциденты должна обсудить совместное пользование информацией с подразделением организации по связям с общественностью, юридическим департаментом и руководством, прежде чем произойдет инцидент, чтобы установить политики и процедуры относительно совместного пользования информацией. Иначе чувствительная информация относительно инцидентов может быть предоставлена сторонам с отсутствующими полномочиями, потенциально ведя к дополнительным нарушениям и денежным убыткам. Команда должна регистрировать все контакты и связи с внешними сторонами с целью ответственности и доказательства.

Следующие разделы предоставляют руководства по взаимодействию с некоторыми типами внешних сторон, как изображено на рисунке 2-1. Двунаправленные стрелки указывают, что любая сторона может начать взаимодействие. Посмотрите Раздел 4 для получения дополнительной информации по связям с внешними сторонами и посмотрите Раздел 2.4 для обсуждения взаимодействия, включающего внешних специалистов по реагированию на инциденты.

Рисунок 2-1. Связи с внешними сторонами

2.3.4.1. Средства информации

Команда обработки инцидента должна установить процедуры взаимодействия со средствами информации, которые выполняют политики организации по взаимодействию со средствами информации и раскрытию информации.[7] Для обсуждения инцидентов со средствами информации организации часто считают выгодным, чтобы определить отдельную точку контакта (POC) и, по крайней мере, один резервный контакт. Следующие действия рекомендуются для подготовки этих выделенных контактов и также должны быть рассмотрены для подготовки других, кто может общаться со средствами информации:

- Проведите сеансы обучения по взаимодействию со средствами информации относительно инцидентов, которые должны включать важность не раскрытия чувствительной информации, такой как технические детали контрмер, которые могут помочь другим атакующим, и положительные аспекты сообщения важной информации обществу полностью и эффективно.
- Установите порядок информирования контактов со средствами информации о проблемах и чувствительности относительно конкретного инцидента прежде, чем обсуждать его со средствами информации.
- Сопроводите описание текущего статуса инцидента таким образом, чтобы взаимодействие со средствами информации было непротиворечивым и актуальным.

7 Например, организация может хотеть, чтобы члены ее офиса связей с общественностью и юридического департамента участвовали во всех обсуждениях инцидента со средствами информации.

- Напомните всему персоналу общие процедуры обработки запросов от средств информации.
- Проведите репетицию интервью и пресс-конференции во время упражнений по обработке инцидентов. Ниже приводятся примеры вопросов, задаваемых контакту со средствами информации:
  - Кто напал на Вас? Почему?
  - Когда это происходило? Как это происходило? Это происходило, потому что у Вас есть слабые методы безопасности?
  - Насколько широко распространился этот инцидент? Какие шаги Вы делаете, чтобы установить то, что произошло и предотвратить будущие случаи?
  - Каково воздействие этого инцидента? Была ли получена персональная идентификационная информация (PII)? Какова предполагаемая стоимость этого инцидента?

2.3.4.2. Правоохранительные органы

Одна из причин, что много связанных с безопасностью инцидентов не учитывается, состоит в том, что некоторые организации неправильно контактируют с правоохранительными органами. Доступно несколько уровней правоохранительных органов для исследования инцидентов: например, в Соединенных Штатах, федеральные исследовательские агентства (например, Федеральное бюро расследований [ФБР] и американская Секретная служба), офисы окружного прокурора, правоохранительные органы штатов и местные (например, графств) правоохранительные органы. Правоохранительные органы других стран также могут быть привлечены, если это касается атак, которые поступили от или направлены на объекты вне US. Кроме того, у агентств есть офис Генерального Инспектора (OIG) для расследования нарушений законов в каждом агентстве. Команда реагирования на инциденты должна познакомиться с представителями различных правоохранительных органов, прежде чем инцидент произойдет, чтобы обсудить условия, при которых нужно им сообщать об инцидентах, как сообщение должно быть выполнено, какие доказательства должны быть собраны, и как они должны быть собраны.

С правоохранительными органами нужно связаться через назначенных людей способом, непротиворечивым с требованиями закона и процедур организации. Многие организации предпочитают назначать одного члена команды реагирования на инциденты как основную POC с правоохранительными органами. Этот человек должен быть знаком с процедурами отчетности по всем соответствующим правоохранительным органам агентств и хорошо подготовленным, чтобы рекомендовать, с каким агентством, если таковые имеются, нужно связаться. Обратите внимание на то, что организация, как правило, не должна связываться со многими агентствами, потому что такие действия могли бы привести к ведомственным конфликтам. Команда реагирования на инциденты должна понимать, какие есть потенциальные ведомственные проблемы (например, физическое местоположение — организация, базирующаяся в одном штате имеет сервер находящийся в другом штате, который атакуют из системы в третьем штате, посредством удаленного доступа атакующими из четвертого штата).

2.3.4.3. Организации отчетности об инцидентах

FISMA требует, чтобы Федеральные агентства сообщали об инцидентах Команде готовности к компьютерным чрезвычайным ситуациям Соединенных Штатов (US-CERT),[8] которая является общеправительственной организацией реагирования на инциденты, которая помогает федеральным гражданским агентствам в их усилиях по обработке инцидентов. US-CERT не заменяет существующие команды реагирования агентств; скорее она увеличивает усилия федеральных гражданских агентств, служа точкой контакта по инцидентам. US-CERT анализирует предоставленную агентством информацию, чтобы определить тенденции и индикаторы атак; их легче различить, когда рассматриваются данные многих организаций, чем когда рассматриваются данные отдельной организации.

[8] http://www.us-cert.gov/

Каждое агентство должно назначить основную и вторичную POC с US-CERT и сообщать обо всех инцидентах, в соответствии с политикой реагирования на инциденты агентства. Организации должны создать политику, которая устанавливает, кто назначен, чтобы сообщать об инцидентах, и как нужно сообщать об инцидентах. Требования, категории и периоды времени для сообщения об инцидентах находятся на вебсайт US-CERT.[9] Все Федеральные агентства должны гарантировать, чтобы их процедуры реагирования на инциденты соответствуют требованиям US-CERT к отчетности и что процедуры выполняются правильно.

Все организации поощрены сообщать об инцидентах своему соответствующему CSIRTs. Если у организации нет своего собственного CSIRT для контактирования, она может сообщать об инцидентах другим организациям, включая Центры распространения и анализа информации (ISACs)**.** Одна из функций этих отраслевых групп частного сектора является распространение важной информации, связанной с компьютерной безопасностью, среди их участников. Несколько ISACs были сформированы для промышленных секторов, таких как Коммуникации, Электрический сектор, Финансовые услуги, Информационные технологии и Исследование и Образование.[10]

2.3.4.4. Другие внешние стороны

Организация может хотеть обсуждать инциденты с другими группами, включая упомянутые ниже. При обращении к этим третьим сторонам организация может хотеть работать через US-CERT или его ISAC как “доверенных проводников”, чтобы посредничать в отношениях. Вероятно, что другие испытывают подобные проблемы и доверенный проводник может гарантировать, что любые такие образцы определены и учтены.

- **ISP организации.** Организации, возможно, понадобится помощь со стороны её ISP в блокировании серьёзной сетевой атаки или отслеживании её происхождения.
- **Владельцы атакующих адресов.** Если нападения происходят из адресного IP пространства внешней организации, обработчики инцидента могут поговорить с установленными контактами по безопасности в организации, чтобы предупредить их о действиях или попросить, чтобы они собрали доказательства. Настоятельно рекомендуется координировать такие связи с US-CERT или ISAC.
- **Продавцы программ.** Обработчики инцидентов могут поговорить с продавцом программ о подозрительной активности. Этот контакт может включать вопросы о значении некоторых записей в журнале или известных ложных срабатываниях для некоторых обнаруженных сигнатур вторжения, когда возможно, должна быть показана минимальная информация относительно инцидента. В некоторых случаях, возможно, должно быть предоставлено больше информации — например, если кажется, что сервер ставился под угрозу через неизвестную программную уязвимость. Продавцы программ могут также предоставить информацию об известных угрозах (например, новые атаки), чтобы помочь организациям понять текущую окружающую среду угрозы.
- **Другие Команды реагирования на инциденты.** Организация может столкнуться с инцидентом, который подобен обработанному другими командами; предварительный обмен информацией может облегчить более эффективную и рациональную обработку инцидентов (например, предоставляя заблаговременное предупреждение, увеличивая подготовленность, разрабатывая ситуативное освоение). Группы, такие как Комиссия реагирования на инциденты и Команды безопасности (FIRST)[11], Правительственная Комиссия реагирования на инциденты и Команды безопасности (GFIRST) [12]и Рабочая группа антифишинга (APWG)[13], не являются командами реагирования на инциденты, но они помогают обмену информацией среди команд реагирования на инциденты.
- **Затронутые Третьи стороны.** Инцидент может затронуть третьи стороны непосредственно — например, внешняя организация может связаться с организацией и утверждать, что один из

[9] http://www.us-cert.gov/federal/reportingRequirements.html
[10] Посмотрите вебсайт Национального совета по ISACs http://www.isaccouncil.org/ для списка ISACs.
[11] http://www.first.org/
[12] GFIRST является специализированным для Федеральных департаментов и агентств. (http://www.us-cert.gov/federal/gfirst.html)
[13] http://www.antiphishing.org/

пользователей организации атакует её. Другим путём, которым третьи стороны могут быть затронуты, есть тот, когда нападавший получает доступ к их чувствительной информации, такой как информация о кредитной карте. В некоторой юрисдикции организации обязаны уведомлять все стороны, которые затронуты таким инцидентом. Независимо от обстоятельств, для организации предпочтительно уведомлять затронутые третьи стороны относительно инцидента до того, как средства информации или другие внешние организации сделают это. Обработчики должны стараться выделить только соответствующую информацию — затронутые стороны могут просить детали о внутренних расследованиях, которые не должны быть показаны публично.

Меморандум OMB M-07-16, *Защита против и реагирование на нарушение персональной идентификационной информации*, требует, чтобы Федеральные агентства разработали и проводили политику уведомления о нарушении персональной идентификационной информации (ПИИ).[14] Обработчики инцидентов должны понимать, как должны отличаться их действия по обработке инцидентов, когда есть подозрение, что произошло нарушение ПИИ, такие как уведомление дополнительных сторон или уведомление сторон в течение более короткого периода времени. Конкретные рекомендации для политик уведомления о нарушении ПИИ представлены в Меморандуме OMB M-07-16. Кроме того, у Национальной конференции Законодательных собраний есть список законов по уведомлению о нарушении государственной безопасности.[15]

2.4. Структура команды реагирования на инциденты

Команда реагирования на инциденты должна быть доступна для любого, кто обнаруживает или подозревает, что произошел инцидент, затрагивающий организацию. Один или более членов команды, в зависимости от величины инцидента и доступности персонала, должен затем обрабатывать инцидент. Обработчики инцидента анализируют данные об инциденте, определяют воздействие инцидента и соответственно действуют, чтобы ограничить ущерб и восстановить нормальные сервисы. Успех команды реагирования на инциденты зависит от участия и кооперации людей по всей организации. Этот раздел определяет таких людей, обсуждает модели команды реагирования на инциденты и предоставляет совет по выбору соответствующей модели.

2.4.1. Модели команды

Возможные структуры для команды реагирования на инциденты включают следующие:

- **Центральная Команда реагирования на инциденты.** Отдельная команда реагирования на инциденты обращается с инцидентами по всей по организации. Эта модель эффективна для небольших организаций и для организаций с минимальной географической распределённостью с точки зрения вычислительных ресурсов.
- **Распределенные Команды реагирования на инциденты.** У организации есть множество команд реагирования на инциденты, каждая ответственна за конкретный логический или физический сегмент организации. Эта модель эффективна для крупных организаций (например, одна команда на подразделение) и для организаций с важными вычислительными ресурсами в отдаленных местоположениях (например, одна команда за географический регион, одна команда за важную возможность). Однако команды должны быть частью одной координируемой сущности так, чтобы процесс реагирования на инциденты был непротиворечив по всей организации, и информация является общей для команд. Это особенно важно, потому что многие команды могут видеть компоненты того же самого инцидента или могут обращаться с подобными инцидентами.
- **Координируемые Команды.** Команда реагирования на инциденты предоставляет консультацию другим командам, не имея полномочий по тем командам — например, общая для департамента команда может помогать отдельным командам агентства. Эта модель может быть представлена

[14] http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

[15] http://www.ncsl.org/default.aspx?tabid=13489

как CSIRT для CSIRTs. Поскольку этот документ сосредоточен на центральных и распределенных CSIRTs, модель координируемых команд не учтена подробно в этом документе.[16]

Команды реагирования на инциденты могут также использовать любую из трех моделей укомплектования персоналом:

- **Сотрудники.** Организация выполняет всю её работу реагирования на инциденты с ограниченной технической и административной поддержкой от подрядчиков.
- **Частичный аутсорсинг.** Организация производит часть своей работы реагирования на инциденты на стороне. Раздел 2.4.2 обсуждает основные факторы, которые нужно рассмотреть при взаимодействии с соисполнителями. Хотя обязанности реагирования на инциденты могут быть разделены между организацией и одним или несколькими подрядчиками различными путями, наиболее распространенными стали несколько соглашений:
  - Самое распространенное соглашение для организации является производство мониторинга датчиков обнаружения вторжений, межсетевых экранов и других устройств безопасности внешним поставщиком услуг управления безопасностью (MSSP) 24 часа в день, 7 дней в неделю (24/7). MSSP определяет и анализирует подозрительную активность и сообщает о каждом обнаруженном инциденте команде реагирования на инциденты организации.
  - Некоторые организации выполняют основную внутреннюю работу реагирования на инциденты и обращаются к подрядчикам с просьбой помогать с обработкой инцидентов, особенно тех, которые более серьезны или широко распространены.
- **Полный аутсорсинг.** Организация полностью производит свою работу реагирования на инциденты на стороне, как правило, единым подрядчиком. Эта модель, скорее всего, будет использоваться, когда организация нуждается в постоянной единой команде реагирования на инциденты, но не имеет в наличии достаточно квалифицированных сотрудников. Предполагается, что у организации будут сотрудники, контролирующие и наблюдающие за работой подрядчика.

2.4.2. Выбор модели команды

Выбирая соответствующую структуру и модели комплектования для команды реагирования на инциденты, организации должны рассмотреть следующие факторы:

- **Потребность в доступности 24/7.** Большинству организаций нужен персонал реагирования на инциденты, чтобы был доступным 24/7. Это, как правило, означает, что с обработчиками инцидентов можно связаться по телефону, но это может также означать, что требуется локальное присутствие. Доступность в реальном времени является лучшей для реагирования на инциденты, потому что чем дольше инцидент длится, тем больше потенциал для ущерба и потерь. Часто необходим контакт в реальном времени при работе с другими организациями — например, прослеживание нападения до его источника.
- **Полностью занятые по сравнению с частично занятыми членами команды.** Организации с ограниченным финансированием, персоналом или потребностями по реагированию на инциденты, могут иметь только частично занятых членов команды реагирования на инциденты, представляющих услуги более виртуальной команды реагирования на инциденты. В этом случае команда реагирования на инциденты может считаться волонтерским отделом пожарной охраны. Когда чрезвычайная ситуация происходит, с членами команды быстро связываются, и те, кто может помочь, делают это. Существующая группа, такая как справочная служба ИТ, может действовать как первая POC для сообщения об инцидентах. Участники справочной службы могут быть обучены, чтобы выполнить первоначальное расследование и сбор данных и затем предупредить команду реагирования на инциденты, если окажется, что произошел серьезный инцидент.
- **Моральное состояние сотрудников.** Работа реагирования на инциденты очень напряжённая, поскольку является обязанностью по вызову для большинства членов команды. Эта комбинация делает её чрезмерно напряженной для членов команды реагирования на инциденты. Многие

[16] Информация о модели координируемых команд, а также обширная информация относительно других моделей команд, доступна в документе CERT®/CC называемом *Модели для Команд реагирования на инциденты компьютерной безопасности организаций (CSIRTs)* (http://www.cert.org/archive/pdf/03hb001.pdf).

организации будут также изо всех сил пытаться находить согласных, доступных, опытных и достаточно квалифицированных людей для участия, особенно в 24-часовой поддержке. Разделение ролей, особенно сокращение объема административной работы, за выполнение которой ответственны члены команды, может значительно повысить моральное состояние.

- **Затраты.** Затраты - основной фактор, особенно если сотрудники обязаны быть на месте 24/7. Организации могут быть не в состоянии включать в бюджеты затраты, связанные с реагированием на инциденты, такие как достаточное финансирование для обучения и поддержания квалификации. Поскольку команды реагирования на инциденты работают со многими аспектами ИТ, то их участникам нужны намного более широкие знания, чем большинству сотрудников ИТ. Они должны также понимать, как использовать инструменты реагирования на инциденты, такие как программное обеспечение электронных расследований. Другими затратами, которые могут игнорироваться, является физическая безопасность рабочих мест команды и коммуникационные механизмы.
- **Экспертные знания персонала.** Обработка инцидентов требует специализированных знаний и опыта в нескольких технических областях; широта и глубина требуемых знаний варьируются в зависимости от серьезности рисков организации. Подрядчики могут обладать более глубокими знаниями по обнаружению вторжений, расследований, уязвимостей, эксплоитов и других аспектов безопасности, чем сотрудники организации. Кроме того, MSSPs могут быть в состоянии коррелировать события среди клиентов так, чтобы они могли определить новые угрозы более быстро, чем мог бы какой-либо отдельный клиент. Однако у технических сотрудников в организации обычно есть намного более лучшее знание среды организации, чем у подрядчиков, которое может быть выгодным в идентификации ложных срабатываний, связанных с поведением конкретной организации и критичностью объектов. Раздел 2.4.3 содержит дополнительную информацию о рекомендуемых квалификациях членов команды.

Рассматривая взаимодействие с подрядчиками, организации должны иметь в виду эти проблемы:

- **Текущее и будущее качество работы.** Организации должны рассмотреть не только текущее качество (широта и глубина) работы подрядчика, но также и усилия, гарантирующие качество будущей работы — например, минимизация обращений и предоставление основательной программы обучения новым сотрудникам. Организации должны думать о том, как они могут объективно оценить качество работы подрядчика.
- **Ответственное подразделение.** Организации часто не желают давать подрядчикам полномочия по принятию эксплуатационных решений для среды (например, отсоединение веб-сервера). Важно задокументировать надлежащие меры для этих моментов принятия решения. Например, одна частично субподрядная модель решает эту проблему при наличии подрядчика, предоставлением данных об инциденте внутренней команде организации, наряду с рекомендациями по дальнейшей обработке инцидента. Внутренняя команда в конечном счете принимает эксплуатационные решения, а подрядчик продолжает оказывать поддержку по мере необходимости.
- **Чувствительная информация, показываемая подрядчику.** Деление обязанностей по реагированию на инциденты и ограничение доступа к чувствительной информации могут её лимитировать. Например, подрядчик может определить, какой идентификатор пользователя использовался в инциденте (например, ID 123456), но не знать, какой человек связан с идентификатором пользователя. Сотрудники могут тогда провести расследование. Соглашения о неразглашении (NDAs) являются одним возможным вариантом для защиты раскрытия чувствительной информации.
- **Отсутствие конкретных сведений по организации.** Точный анализ и назначение приоритетов инцидентов зависят от специальных знаний среды организации. Организация должна обеспечить подрядчика регулярно обновляемыми документами, которые определяют, каких инцидентов это касается, какие ресурсы очень важны и какой уровень реагирования должен быть при различном стечении обстоятельств. Организация должна также сообщать обо всех изменениях и обновлениях, сделанных в ее инфраструктуре ИТ, конфигурации сети и системах. Иначе, предположение подрядчика относительно того, как лучшее каждый инцидент должен быть обработан, неизбежно приводит в результате к инцидентам, с которыми не справляются, и к разочарованию с обеих сторон. Отсутствие специальных знаний по организации может также быть проблемой, даже когда реагирование на инциденты не производится на стороне, если недостаточно взаимодействие среди команд или если организация просто не собирает необходимую информацию.

- **Отсутствие корреляции.** Корреляция среди многих источников данных очень важна. Если система обнаружения вторжений делает запись предпринятой атаки на веб-сервер, но у подрядчика нет доступа к журналам регистрации сервера, он может быть неспособным определить, была ли атака успешной. Чтобы быть эффективным, подрядчик потребует административных привилегий к критическим системам и файлам регистрации устройств безопасности удаленно по безопасному каналу. Это увеличит затраты на администрирование, введет дополнительные точки входа доступа и увеличит риск несанкционированного раскрытия чувствительной информации.
- **Обработка инцидентов во многих местоположениях.** Эффективная работа реагирования на инциденты часто требует физического присутствия на объектах организации. Если подрядчик удален, рассмотрите, где подрядчик расположен, как быстро команда реагирования на инциденты может быть на любом объекте, и сколько это будет стоить. Рассмотрите локальные посещения; возможно, есть некоторые объекты или области, где подрядчику нельзя разрешить работать.
- **Поддержание внутренних возможностей реагирования на инциденты.** Организации, которые полностью осуществляют реагирование на инциденты используя подрядчика, должны стремиться поддерживать основные внутренние возможности реагирования на инциденты. Могут возникнуть ситуации, в которых подрядчик недоступен, поэтому, организация должна быть готова выполнить обработку инцидента сама. Технический персонал организации должен также быть в состоянии понимать значение, технические последствия и влияние рекомендаций подрядчика.

2.4.3. Персонал реагирования на инциденты

Отдельный сотрудник, с одной или более назначенными заменами, должен отвечать за реагирование на инциденты. В полностью субподрядной модели этот человек наблюдает и оценивает работу подрядчика. У всех других моделей обычно есть менеджер команды и один или несколько заместителей, которые принимают полномочия в отсутствие менеджера команды. Менеджеры обычно выполняют много задач, включая такие действия, как связь с верхним руководством и другими командами и организациями, разрешение кризисных ситуаций и гарантирование, что у команды есть необходимый персонал, ресурсы и знания. Менеджеры должны быть технически подготовлены и иметь отличные навыки общения, особенно способность общаться с большой аудиторией. Менеджеры в итоге ответственны за обеспечение того, что работы реагирования на инциденты выполняются правильно.

В дополнение к менеджеру и заместителю команды, у некоторых команд есть также технический руководитель — человек с сильными техническими навыками и опытом реагирования на инциденты, который осуществляет надзор и несёт конечную ответственность за качество технической работы команды. Должность технического руководителя не следует путать с позицией ведущего по инциденту. Более многочисленные команды часто назначают ведущего по инциденту в качестве основной POC для обработки конкретного инцидента; ведущий по инциденту закрепляется ответственным за обработку инцидента. В зависимости от размера команды реагирования на инциденты и величины инцидента, ведущий по инциденту может не выполнять фактическую обработку инцидента, а скорее координировать работу обработчиков, собирать от них информацию, предоставлять новую информацию по инциденту другим группам и гарантировать, что потребности команды удовлетворены.

У членов команды реагирования на инциденты должна быть превосходная техническая подготовка в таких областях, как системное администрирование, администрирование сети, программирование, техническая поддержка или обнаружение вторжений. У каждого члена команды должны быть хорошие навыки по решению проблем и способности к критическому мышлению. Не обязательно для каждого члена команды быть техническим экспертом — в значительной степени, практические и финансовые рассмотрения продиктуют это — но наличие по крайней мере одного очень опытного человека в каждой основной области технологии (например, обычно подвергаются нападению операционные системы и приложения) является необходимостью. Может также быть полезно иметь некоторых членов команды, специализирующихся в особых технических областях, таких как обнаружение сетевого вторжения, анализ вредоносного кода или юридические действия. Также часто полезно временно вводить технических специалистов, которые обычно не являются частью команды.

Важно противодействовать перегоранию персонала, предоставляя возможности для повышения квалификации и роста. Предложения для повышения и поддержки подготовки следующие:

- Достаточный бюджет финансирования, чтобы поддерживать, увеличивать и расширять мастерство в технических областях и дисциплинах безопасности, а также в менее технических темах, таких как законодательные аспекты реагирования на инциденты. Это должно включать отправку персонала на конференции и поощрение или иное стимулирование участия в конференциях, обеспечение доступности технических справочников, которые способствуют более глубокому техническому пониманию и иногда привлечение внешних экспертов (например, подрядчиков) с глубокими техническими знаниями в необходимых областях, если позволяет финансирование.
- Дайте возможность членам команды выполнять другие задачи, такие как создание обучающих материалов, проведение семинаров по освоению мер безопасности и выполнение исследований.
- Рассмотрите ротацию сотрудников в и из команды реагирования на инциденты и участвуйте в обменах, в которых члены команды временно меняются местами с другими (например, сетевыми администраторами), чтобы получить новые технические знания.
- Поддерживайте достаточное укомплектование персоналом так, чтобы у членов команды могло бы быть продолжительное свободное время (например, отпуска).
- Создайте программу наставничества, чтобы дать возможность основному техническому персоналу помогать менее опытному персоналу изучать обработку инцидентов.
- Разработайте сценарии обработки инцидентов и сделайте так, чтобы члены команды обсудили, как бы они обрабатывали их. Приложение А содержит ряд сценариев и список вопросов, которые могут использоваться во время обсуждений сценария.

У членов команды реагирования на инциденты должны быть другие квалификации в дополнение к техническим знаниям. Способности работы в команде имеют фундаментальное значение, потому что кооперация и координация необходимы для успешного реагирования на инциденты. У каждого члена команды должны также быть хорошие навыки общения. Разговорные навыки важны, потому что команда будет взаимодействовать с большим разнообразием людей, а навыки письма важны, когда члены команды готовят оповещения и процедуры. Хотя не у всех в команде должны быть сильное письмо и разговорные навыки, но, по крайней мере, несколько человек в каждой команде должны обладать ими так, чтобы команда могла представлять себя хорошо перед другими.

2.4.4. Зависимости в организациях

Важно определить другие группы в организации, которые, возможно, должны участвовать в обработке инцидентов так, чтобы их кооперация могла бы быть установлена, прежде чем это будет необходимо. Каждая команда реагирования на инциденты полагается на экспертные знания, суждение и способности других, включая:

- **Руководство.** Руководство устанавливает политику реагирования на инциденты, бюджет и укомплектование персоналом. В конечном счете руководство является ответственным за координацию реагирования на инциденты среди различных заинтересованных сторон, уменьшение ущерба и сообщение в Конгресс, OMB, Главное бюджетно-контрольное управление (GAO) и другие стороны.
- **Информационное доверие.** Сотрудники информационной безопасности, могут быть необходимы во время некоторых стадий обработки инцидентов (предотвращение, сдерживание, уничтожение и восстановление) — например, чтобы изменить меры обеспечения сетевой безопасности (например, настройка правил межсетевого экрана).
- **Поддержка ИТ.** У технических ИТ экспертов (например, системных и сетевых администраторов) есть не только необходимая подготовка чтобы помогать, но также обычно есть и лучшее понимание технологий, которыми что они управляют ежедневно. Это понимание может гарантировать, что приняты соответствующие меры для затронутой системы, такие как, отсоединение системы, подвергнувшейся нападению.
- **Юридический департамент.** Юристы должны рассмотреть планы, политики и процедуры реагирования на инциденты, чтобы гарантировать их соответствие законам и федеральным руководствам, включая право на приватность. Кроме того, главным юрисконсультом или

юридическим департаментом должно быть предоставлено руководство, если есть причина полагать, что у инцидента могут быть юридические последствия, включая сбор свидетельств, судебное преследование подозреваемого, или судебный иск, или если может быть потребность в меморандуме о взаимопонимании (MOU) или других обязывающих соглашениях, включающих ограничение ответственности для совместного пользования информацией.

- **Связи с общественностью и связи со средствами информации.** В зависимости от сущности и воздействия инцидента, может существовать потребность в информировании средств информации и, более широко, общественности.
- **Человеческие ресурсы.** Если сотрудник подозревается в порождении инцидента, может быть подключен департамент человеческих ресурсов— например, в помощь по дисциплинарным разбирательствам.
- **Планирование бесперебойной деятельности.** Организации должны гарантировать, что политики и процедуры реагирования на инциденты и процессы бесперебойной деятельности находятся в синхронизации. Инциденты компьютерной безопасности подрывают устойчивость деятельности организации. Профессионалы планирования бесперебойной деятельности должны быть проинформированы об инцидентах и их воздействиях, таким образом, они смогут уточнить оценки влияния на бизнес, оценки степени риска и планы непрерывности деятельности. Далее, потому что у планировщиков бесперебойной деятельности есть большой опыт в уменьшении нарушения эксплуатации во время сложных обстоятельств, они могут быть полезными в планировании реагирования на определенные ситуации, такие как условия отказа в обслуживании (DoS).
- **Физическая безопасность и управление оборудованием.** Некоторые инциденты компьютерной безопасности происходят посредством нарушения физической безопасности или включают координируемые логические и физические нападения. Команде реагирования на инциденты также, возможно, понадобится доступ к средствам во время обработки инцидента — например, чтобы получить поставившую под угрозу рабочую станцию из запертого офиса.

2.5. Услуги команды реагирования на инциденты

Основной задачей команды реагирования на инциденты является выполнение реагирования на инциденты, но довольно редко команда выполняет только реагирование на инциденты. Ниже приводятся примеры других услуг, которые могла бы предложить команда:

- **Обнаружение вторжений.** Первый уровень команды реагирования на инциденты часто принимает на себя ответственность за обнаружение вторжений.[17] Команда обычно извлекает в этом выгоду, поскольку это должно помогать проанализировать инциденты более быстро и точно, на основе знаний, которые получены о технологиях обнаружения вторжений.
- **Распространение оповещений.** Команда может выпускать в организации извещения по новым уязвимостям и угрозам.[18] Если возможно, должны использоваться автоматизированные методы доведения информации; например, National Vulnerability Database (NVD) предоставляет информацию через XML и каналы RSS, когда в неё добавлены новые уязвимости.[19] Оповещения часто нужны, когда появляются новые угрозы, такие как резонансное социальное или политическое событие (например, свадьба знаменитости), которое атакующие, вероятно, используют в их социальной технике. Только одна группа в организации должна распространять оповещения по компьютерной безопасности, чтобы избежать дублирования усилий и противоречия информации.

[17] Для получения дополнительной информации о технологиях IDPS посмотрите NIST SP 800-94, *Руководство по Системам обнаружения и предотвращения вторжений (IDPS)*. Это доступно по http://csrc.nist.gov/publications/PubsSPs.html#800-94.

[18] Команды должны формулировать оповещения так, чтобы они не обвиняли человека или организацию по аспектам безопасности. Команды должны встретиться с консультантами по правовым вопросам, чтобы обсудить возможную потребность в правовой оговорке в оповещениях, заявив, что у команды и организации нет ответственности в отношении точности оповещения. Это является самым подходящим, когда оповещения может быть послали подрядчикам, продавцам и другим не сотрудникам, которые являются пользователями вычислительных ресурсов организации.

[19] http://nvd.nist.gov/.

- **Образование и освоение.** Образование и освоение являются умножителями ресурсов — чем больше пользователи и технический персонал знают об обнаружении, сообщении и ответе на инциденты, тем меньше усилий должно быть у команды реагирования на инциденты. Эта информация может быть сообщена через многие средства: семинары, вебсайты, информационные бюллетени, плакаты и даже этикетки на мониторах и ноутбуках.
- **Распространение информации.** Команды реагирования на инциденты часто участвуют в группах распространения информации, таких как ISACs или региональные партнерства. Соответственно, команды реагирования на инциденты часто управляют усилиями по распространению информации об инцидентах в организации, такими как агрегирование информации, связанной с инцидентами и эффективный обмен этой информацией с другими организациями, а также гарантирование, что соответствующая информация распространяется на предприятии.

2.6. Рекомендации

Ключевые рекомендации, представленные в этом разделе по организации способности обработки инцидентов компьютерной безопасности, сведены ниже.

- **Установите формальную способность реагирования на инциденты.** Организации должны быть готовы ответить быстро и эффективно, когда компьютерная безопасности нарушена. FISMA требует, чтобы Федеральные агентства обеспечили способность реагирования на инциденты.
- **Создайте политику реагирования на инциденты.** Политика реагирования на инциденты - основа программы реагирования на инциденты. Она определяет, какие события считают инцидентами, устанавливает организационную структуру для реагирования на инциденты, определяет роли и обязанности и формирует требования для сообщения об инцидентах, среди других элементов.
- **Разработайте план реагирования на инциденты на основе политики реагирования на инциденты.** План реагирования на инциденты является путеводителем по реализации программы реагирования на инциденты на основе политики организации. План определяет и ближние - и долгосрочные цели для программы, включая метрики для оценки программы. План реагирования на инциденты должен также указывать, как часто обработчики инцидентов должны обучаться и требования для обработчиков инцидентов.
- **Разработайте способы реагирования на инциденты.** Процедуры реагирования на инциденты предоставляют подробные шаги для реагирования на инциденты. Процедуры должны закрывать все фазы процесса реагирования на инциденты. Процедуры должны быть основаны на политике и плане реагирования на инциденты.
- **Установите политики и процедуры относительно распространения информации, связанной с инцидентом.** Организация должна сообщать соответствующие детали инцидента внешним сторонам, таким как средства массовой информации, правоохранительные органы и организации отчетности об инцидентах. Команда реагирования на инциденты должна обсудить это с офисом связей с общественностью организации, юридическим департаментом и руководством, чтобы установить политики и процедуры относительно распространения информации. Команда должна выполнять существующую политику организации по взаимодействию со средствами массовой информации и другими внешними сторонами.
- **Предоставьте уместную информацию об инцидентах в соответствующую организацию.** Федеральные гражданские агентства обязаны сообщать об инцидентах в US-CERT; другие организации могут связаться с US-CERT и/или их ISAC. Сообщение является полезным, потому что US-CERT и ISACs используют данные, о которых сообщают, чтобы предоставить информацию сторонам сообщения относительно новых угроз и тенденций инцидентов.
- **Рассмотрите соответствующие факторы, выбирая модель команды реагирования на инциденты.** Организации должны тщательно взвесить преимущества и недостатки каждой возможной модели структуры команды и модели укомплектования персоналом в контексте потребностей организации и имеющихся ресурсов.

- **Выберите людей с соответствующими знаниями для команды реагирования на инциденты.** Доверие и мастерство команды зависят в большой степени от технической подготовки и способностей к критическому мышлению её участников. Критические технические знания включают системное администрирование, администрирование сети, программирование, техническую поддержку и обнаружение вторжений. Работа в команде и коммуникационные навыки также необходимый для эффективной обработки инцидентов. Необходимое обучение должно быть предоставлено всем членам команды.
- **Определите другие группы в организации, которые, возможно, должны участвовать в обработке инцидентов.** Каждая команда реагирования на инциденты полагается на экспертные знания, суждение и возможности других команд, включая руководство, информационного доверия, поддержки ИТ, юристов, связей с общественностью и управления оборудованием.
- **Определите, какие услуги команда должна предложить.** Хотя главное назначение команды - реагирование на инциденты, большинство команд выполняет дополнительные функции. Примеры включают мониторинг сенсоров обнаружения вторжений, доведение оповещений по безопасности и разъяснение пользователям по безопасности.

3. Обработка инцидентов

У процесса реагирования на инциденты есть несколько фаз. Начальная фаза включает назначение и обучение команды реагирования на инциденты и приобретение необходимых инструментов и ресурсов. Во время подготовки организация также пытается ограничить число инцидентов, которые произойдут, выбирая и реализуя ряд мер безопасности на основе результатов оценок степени риска. Однако остаточный риск неизбежно сохранится после того, как меры безопасности реализованы. Обнаружение нарушений защиты является, таким образом, необходимым, чтобы предупредить организацию каждый раз, когда инциденты происходят. В соответствии с серьезностью инцидента, организация может смягчить воздействие инцидента, ограничивая его и, в итоге, восстанавливаясь от него. Во время этой фазы, действия часто возвращаются назад к обнаружению и анализу — например, чтобы видеть, не заражены ли дополнительные хосты вредоносным программным обеспечением после ликвидации вредоносного инцидент. После того, как инцидент соответственно обработан, организация выпускает отчет, который детализирует причину и стоимость инцидента и шаги, которые организация должна сделать, чтобы предотвратить будущие инциденты. Этот раздел подробно описывает основные фазы процесса реагирования на инциденты — подготовку, обнаружение и анализ, сдерживание, уничтожение и восстановление, и работы постинцидента. Рисунок 3-1 иллюстрирует жизненный цикл реагирования на инциденты.

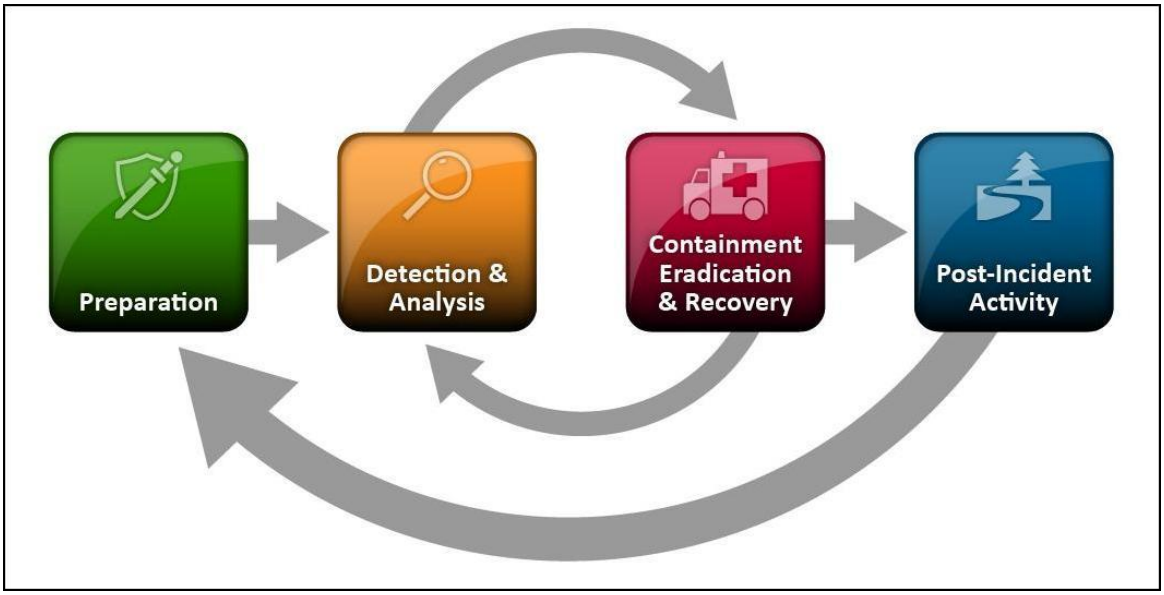

Рисунок 3-1. Жизненный цикл реагирования на инциденты

3.1. Подготовка

Методологии реагирования на инциденты, как правило, подчеркивают подготовку — не только установление способности реагирования на инциденты так, чтобы организация была готова ответить на инциденты, но также и предотвращение инцидентов, гарантируя, что системы, сети и приложения достаточно безопасны. Хотя команда реагирования на инциденты, как правило, не ответственна за предотвращение инцидентов, это фундаментально для успеха программ реагирования на инциденты. Этот раздел предоставляет основные советы при подготовке к обработке инцидентов и по предотвращению инцидентов.

3.1.1. Подготовка к обработке инцидентов

Перечни ниже предоставляют примеры доступных инструментов и ресурсов, которые могут иметь значение во время обработки инцидентов. Эти перечни предназначены, чтобы быть отправной точкой для обсуждений того, какие инструментах и ресурсы необходимы для обработчиков инцидентов организации. Например, смартфоны - один из способов иметь устойчивый механизм коммуникации и координации в чрезвычайной ситуации. Организация должна иметь много

(отдельных и различных) механизмов коммуникации и координации в случае отказа одного механизма.

Средства коммуникации и оборудование обработчика инцидентов:

- **Контактная информация** для членов команды и других в и за пределами организации (основные и резервные контакты), такие как правоохранительные органы и другие команды реагирования на инциденты; информация может включать номера телефонов, адреса электронной почты, общие ключи шифрования (в соответствии с программным обеспечением шифрования, описанным ниже), и инструкции для подтверждения идентичности контакта
- **Информация по вызову** других команд в организации, включая информацию эскалации
- **Механизмы отчетности об инцидентах,** такие как номера телефона, адреса электронной почты, формы онлайн и безопасные системы мгновенного обмена сообщениями, которые пользователи могут использовать, чтобы сообщать о подозреваемых инцидентах; по крайней мере один механизм должен позволять людям сообщать об инцидентах анонимно
- **Система отслеживания задач** для прослеживания информации об инцидентах, статуса, и т.д.
- **Смартфоны**, которые будут носить члены команды для внеурочной поддержки и локальных коммуникаций
- **Программное обеспечение шифрования**, которое будет использоваться для коммуникации среди членов команды в организации и с третьими сторонами; для Федеральных агентств программное обеспечение должно использовать FIPS-утвержденный алгоритм шифрования[20]
- **Оперативное помещение** для централизованной коммуникации и координации; если постоянное оперативное помещение не требуется или не практично, команда должна создать процедуру обеспечения временным оперативным помещением при необходимости
- **Средство безопасного хранения** для обеспечения безопасности свидетельств и других чувствительных материалов

Аналитическое аппаратное и программное обеспечение инцидента:

- **Цифровые рабочие станции для расследования[21] и/или устройства резервного копирования**, чтобы создавать образы дисков, хранить файлы журнала и хранить другие соответствующие данные об инциденте
- **Ноутбуки** для работ, таких как анализ данных, сниффинг пакетов и написание отчетов
- **Запасные рабочие станции, серверы и сетевое оборудование или виртуализированные эквиваленты**, которые могут быть использованы для различного назначения, такого как восстановление резервных копий и анализ вредоносного программного обеспечения
- **Чистые съемные носители**
- **Портативный принтер**, чтобы печатать копии файлов журнала и других свидетельства от несетевых систем
- **Снифферы пакетов и анализаторы протоколов**, для перехвата и анализа сетевого трафика
- **Цифровое программное обеспечение для расследований**, чтобы анализировать образы дисков
- **Съемные носители** с доверенными версиями программ, которые будут использоваться, чтобы собирать свидетельства от систем
- **Аксессуары для сбора свидетельства**, включая защищенные ноутбуки, цифровые фотоаппараты, магнитофоны, набор форм заключений, сумки и бирки для хранения свидетельств, и ленту для свидетельств, чтобы сохранять свидетельства для возможных юридических действий

[20] FIPS 140-2, *Требования безопасности для криптографических модулей*, http://csrc.nist.gov/publications/PubsFIPS.html

[21] Цифровая рабочая станция для расследований специально проектируется, чтобы помочь обработчикам инцидентов в получении и анализе данных. Эти рабочие станции, как правило, содержат ряд съемных жестких дисков, которые могут использоваться для хранения свидетельств.

Аналитические ресурсы инцидента:

- **Списки портов,** включая обычно используемые порты и порты троянского коня
- **Документация** по OSs, приложениям, протоколам и продуктам обнаружения вторжений и антивирусным продуктам
- **Сетевые схемы и списки критических активов**, таких как серверы баз данных
- **Текущие графики** активности анализируемых сетей, систем и приложений
- **Криптографические хэши** критических файлов[22], для ускорения анализа, проверки и ликвидации инцидентов

Программное обеспечение смягчения инцидентов:

- **Доступ к образам** чистой ОС и инсталляторам приложений для целей восстановления и исправления

Многие команды реагирования на инциденты создают *дежурный набор*, который является портативным набором, содержащим материалы, которые могут быть необходимы во время расследования. Дежурный набор должен быть готов к использованию в любом случае. Дежурные наборы содержат многие из тех элементов, которые перечислены в перечнях выше. Например, каждый дежурный набор, как правило, включает ноутбук, загруженный соответствующим программным обеспечением (например, снифферы пакетов, цифровые средства расследований). Другие важные материалы включают устройства резервного копирования, чистые носители информации и основное сетевое оборудование и кабели. Поскольку назначение дежурного набора состоит в том, чтобы облегчить более быстрое реагирование, команда должна избегать брать элементы из дежурного набора.

У каждого обработчика инцидентов должен быть доступ по крайней мере к двум вычислительным устройствам (например, ноутбуки). Один, такой же как в дежурном наборе, должен использоваться, чтобы выполнять сниффинг пакетов, анализ вредоносного кода и все другие действия, которые связаны с риском заразить ноутбук, на котором они выполняются. Этот ноутбук должен быть вычищен и все программное обеспечение повторно установлено, прежде чем он будет использоваться для другого инцидента. Обратите внимание на то, что, потому что этот ноутбук - особого назначения, он, вероятно, будет использовать программное обеспечение иное, чем для стандартных инструментов и конфигураций предприятия, и когда это возможно, обработчику инцидентов должно быть позволено определять основные технические требования для этих следственных ноутбуков специального назначения. В дополнение к следственному ноутбуку у каждого обработчика инцидентов должны быть также стандартный ноутбук, смартфон или другое вычислительное устройство для того, чтобы писать отчеты, читать электронную почту и выполнять другие обязанности, не связанные с практическим анализом инцидентов.

Упражнения, включающие моделируемые инциденты, также могут быть очень полезны для подготовки персонала обработки инцидентов; посмотрите NIST SP 800-84 для получения дополнительной информации об упражнениях[23] и Приложение A для типовых сценариев тренировок.

3.1.2. Предотвращение инцидентов

Удержание количества инцидентов на низком уровне очень важно для защиты процессов деятельности организации. Если меры безопасности недостаточны, могут произойти объемы инцидентов, превышающие возможности команды реагирования на инциденты. Это может вести к замедленным и неполным реакциям, которые приведут к большему отрицательному влиянию на бизнес (например, более значительному ущербу, более длинным периодам обслуживания и отсутствия данных).

За рамки этого документа выходит предоставление конкретных рекомендаций по обеспечению безопасности сетей, систем и приложений. Хотя команды реагирования на инциденты обычно не ответственны за обеспечение безопасности ресурсов, они могут рекомендовать проверенные методы безопасности. Команда реагирования на инциденты может быть в состоянии определить

[22] Проект National Software Reference Library (NSRL) поддерживает записи кэшей различных файлов, включая операционную систему, приложение и файлы графических изображения. Кэши могут быть загружены с http://www.nsrl.nist.gov/.

[23] *Руководство по проверке, обучению и программам подготовки планов ИТ и возможностей,* http://csrc.nist.gov/publications/PubsSPs.html#800-84

проблемы, о которых иначе не знает организация; команда может играть ключевую роль в оценке степени риска и обучении, определяя недостатки. Другие документы уже предоставляют советы по общим концепциям безопасности и руководства по операционным системам и специализированным приложениям.[24] Следующий текст, однако, предоставляет краткий обзор некоторых основных рекомендуемых методов для обеспечения безопасности сетей, систем и приложений:

- **Оценки степени риска.** Периодические оценки степени риска систем и приложений должны определять, какие риски представляются комбинациями угроз и уязвимостей.[25] Это должно включать понимание применимых угроз, включая конкретные угрозы для организации. Каждый риск должен быть расположен по приоритету, и риски могут быть снижены, переданы или приняты пока не будет достигнут обоснованный общий уровень риска. Другая выгода от регулярного проведения оценок степени риска в том, что определяются критические ресурсы, позволяя персоналу выделить работы по мониторингу и реагированию для этих ресурсов.[26]
- **Безопасность хоста.** Все хосты должны быть укреплены, используя соответствующие стандартные конфигурации. В дополнение к соблюдению для каждого хоста правильного обновления, хосты должны конфигурироваться по принципу наименьшего количества привилегий — предоставление пользователям только тех привилегий, которые необходимы для выполнения их санкционированных задач. Хосты должны допускать ревизию и должны регистрировать значительные события, связанные с безопасностью. Безопасность хостов и их конфигураций должна непрерывно контролироваться.[27] Многие организации используют Security Content Automation Protocol (SCAP)[28] представляющий контрольные списки конфигурации для операционных систем и приложений, чтобы помочь в обеспечении безопасности хостов последовательно и эффективно.[29]
- **Сетевая безопасность.** Сетевой периметр должен формироваться, чтобы запрещать любую активность, которая явно не разрешена. Это включает обеспечение безопасности всех точек контакта, путём виртуальных частных сетей (VPNs) и выделенных связей с другими организациями.
- **Предотвращение вредоносного кода.** Программное обеспечение по обнаружению и остановке вредоносного программного обеспечения должно быть развернуто во всей организации. Защита от вредоносного кода должна быть развернута на уровне хоста (например, операционных систем сервера и рабочей станции), уровне сервера приложений (например, почтового сервера, веб-прокси) и уровне клиента приложения (например, почтового клиента, клиента обмена мгновенными сообщениями).[30]
- **Обучение и подготовка пользователей.** Пользователи должны быть обучены политикам и процедурам по соответствующему использованию сетей, систем и приложений. Применимые уроки, извлеченные из предыдущих инцидентов, также должны быть доведены пользователям, чтобы они видели, как их действия могут затронуть организацию. Улучшение обучения пользователей относительно инцидентов должно уменьшить частоту инцидентов. Персонал ИТ должен быть обучен так, чтобы они могли сопровождать свои сети, системы и приложения в соответствии со стандартами обеспечения безопасности организации.

---

[n] http://csrc.nist.gov/publications/PubsSPs.html предоставляет ссылки на Специальные публикации NIST по компьютерной безопасности, которые включают документы по базовой защите операционных систем и безопасности приложений.

[25] Руководства по оценке степени риска доступны в NIST SP 800-30, *Руководство по проведению оценок степени риска*, в http://csrc.nist.gov/publications/PubsSPs.html#800-30-Rev1.

[26] Информация относительно идентификации критических ресурсов представлена в FIPS 199, *Стандарты по классификации безопасности федеральной информации и информационных систем*, в http://csrc.nist.gov/publications/PubsFIPS.html.

[27] Для получения дополнительной информации о непрерывном мониторинге смотрите NIST SP 800-137, *Непрерывный мониторинг информационной безопасности для федеральных информационных систем и организаций* (http://csrc.nist.gov/publications/PubsSPs.html#800-137).

[28] Больше информации о SCAP доступно в NIST SP 800-117 пересмотр 1, Руководство по адаптации и использованию Security Content Automation Protocol (SCAP) Version 1.2 (http://csrc.nist.gov/publications/PubsSPs.html#800-117).

[29] Хост NIST по хранению контрольных списков безопасности в http://checklists.nist.gov/.

[30] Больше информации относительно предотвращения вредоносного кода доступно в NIST SP 800-83, *Руководство по предотвращению обработке инцидентов с вредоносным кодом* (http://csrc.nist.gov/publications/PubsSPs.html#800-83).

3.2. Обнаружение и анализ

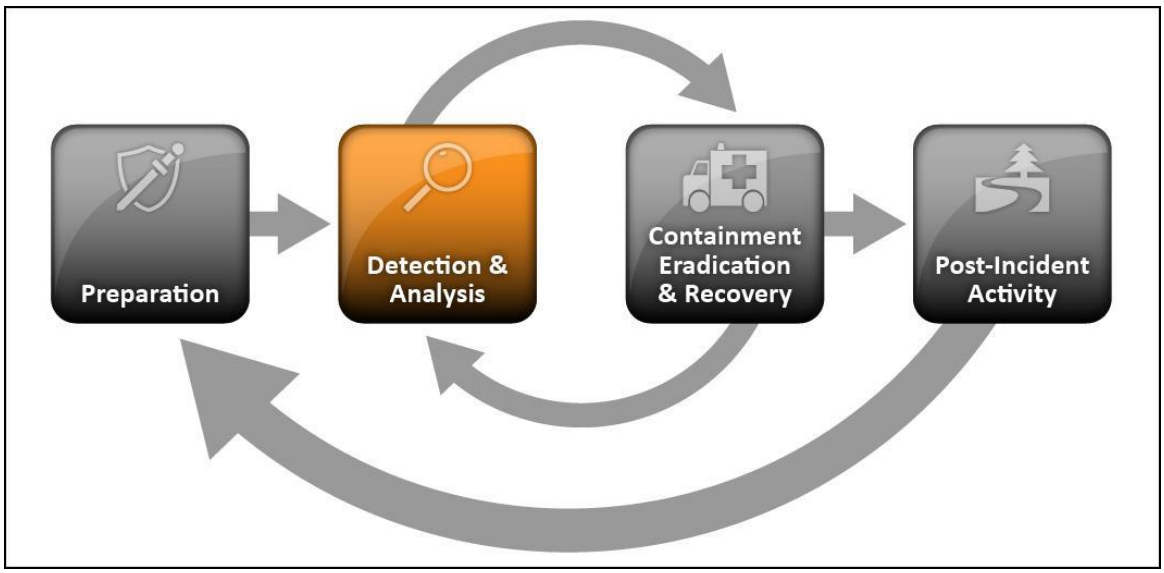

Рисунок 3-2. Жизненный цикл реагирования на инциденты (Обнаружение и анализ)

3.2.1. Векторы атаки

Инциденты могут произойти бесчисленными способами, таким образом, невозможно разработать пошаговые инструкции для обработки каждого инцидента. Организации должны быть готовы обращаться с любым инцидентом, но должны сосредоточиться на том, чтобы быть готовыми обращаться с инцидентами, которые используют общие векторы атаки. Различные типы инцидентов заслуживают различных стратегий реагирования. Упомянутые ниже векторы атак не предназначены, чтобы предоставить полную классификацию для инцидентов; скорее они просто перечисляют общепринятые методики нападения, которые могут использоваться в качестве основания для определения более конкретных процедур обработки.

- **Внешние съемные носители:** нападение, выполняемое со съемных носителей или периферийных устройств — например, вредоносный код, распространяющийся в систему из зараженной карты флэш-памяти с интерфейсом USB.
- **Истощение:** нападение, которое использует методы грубой силы для компрометации, ухудшения или разрушения систем, сетей или сервисов (например, DDoS предназначена для ослабления или лишения доступа к сервису или приложению; атака грубой силой против механизма аутентификации, такого как пароли, CAPTCHAS или цифровые подписи).
- **Web:** нападение, выполняемое от вебсайта или веб-приложения — например, атака с использованием кросс-сайтовых сценариев используется для кражи учётных данных или перенаправления к сайту, который эксплуатирует уязвимости браузера и устанавливает вредоносное программное обеспечение.
- **Электронная почта:** нападение, выполняемое с помощью электронного письма или приложения — например, эксплоитный код, замаскированный как приложенный документ или ссылка на злонамеренный вебсайт в теле электронного письма.
- **Олицетворение**: атака, включающая замену чего-то полезного чем-то злонамеренным — например, имитация, атака посредника, обманные точки доступа сети и атаки с инъекцией кода SQL, все включают олицетворение.
- **Неподходящее использование:** Любой инцидент, следующий из нарушения приемлемых политик использования организации авторизованным пользователем, исключая вышеупомянутые категории; например, пользователь устанавливает программное обеспечение совместного доступа к файлам, ведя к потере чувствительных данных; или пользователь выполняет незаконную деятельность в системе.

- **Потеря или кража оборудования:** потеря или кража вычислительного устройства или носителя информации, используемого организацией, такого как ноутбук, смартфон или аутентификационный маркер.
- **Другое:** Нападение, которое не вписывается ни в одну из других категорий.

Этот раздел сосредотачивается на рекомендуемых методах обработки любого типа инцидента. За рамки этой публикации выходит предоставление конкретных советов на основе векторов атак; такие руководства предоставляются в отдельных публикациях, учитывающих другие темы обработки инцидентов, таких как NIST SP 800-83 по предотвращении и обработке инцидентов с вредоносным кодом.

3.2.2. Признаки инцидента

Для многих организаций самая сложная часть процесса реагирования на инциденты это точное обнаружение и оценка возможных инцидентов — определение, произошел ли инцидент и, если да, то типа, степени и величины проблемы. Сложность этого определяется комбинацией трех факторов:

- Инциденты могут быть обнаружены через многие различные средства, с различными уровнями детализации и точности. Автоматизированные средства обнаружения включают сетевой и хостовый IDPSs, антивирусное программное обеспечение и анализаторы логов. Инциденты могут быть также обнаружены ручными средствами, такими как сообщения пользователей о проблемах. У некоторых инцидентов есть явные признаки, которые могут быть легко обнаружены, тогда как другие почти невозможно обнаружить.
- Объем потенциальных признаков инцидентов, как правило, высок — например, это не редко для организации получать тысячи или даже миллионы оповещений по датчику обнаружения вторжений в день. (См. Раздел 3.2.4 для получения информации относительно анализа таких тревог.)
- Глубокие, специализированные технические знания и обширный опыт необходимы для надлежащего и эффективного анализа связанных с инцидентом данных.

Признаки инцидента попадают в одну из двух категорий: предшественники и индикаторы. *Предшественник* – признак того, что инцидент может произойти в будущем. *Индикатор* – признак того, что инцидент, возможно, произошел или возможно происходит сейчас.

У большинства атак нет соответствующих или обнаружимых предшественников с точки зрения объекта. Если предшественники обнаружены, у организации имеется возможность предотвратить инцидент, изменяя её состояние безопасности, чтобы защитить объект от атаки. Как минимум организация может мониторить активность, затрагивающую объект более тесно. Примеры предшественников:

- Записи в журнале веб-сервера, которые показывают использование сканера уязвимости
- Сообщение о новом эксплоите, который предназначается для уязвимости почтового сервера организации
- Угроза от группы, заявляющей, что группа будет атаковать организацию.

В то время как предшественники относительно редки, индикаторы слишком общие. Существует слишком много типов индикаторов, чтобы исчерпывающе перечислить их, но некоторые примеры упомянуты ниже:

- Сетевой датчик обнаружения проникновения сообщает, когда происходит попытка переполнения буфера сервера базы данных.
- Антивирусное программное обеспечение сообщает, когда оно обнаруживает, что хост заражен вредоносным программным обеспечением.
- Системный администратор видит имя файла с необычными характеристиками.
- Записи хоста по контролю конфигурации изменяются в его журнале регистрации.

- Приложения регистрирует множественные неудавшиеся попытки доступа от незнакомой удаленной системы.
- Почтовый администратор видит большое количество отклонённых электронных писем с подозрительным содержанием.
- Сетевой администратор замечает необычное отклонение от типичных потоков сетевого трафика.

3.2.3. Источники предшественников и индикаторов

Предшественники и индикаторы идентифицируются с использованием различных других источников, наиболее общими для безопасности компьютерного программного обеспечения являются предупреждения, журналы регистрации, общедоступная информация и люди. Таблица 3-2 содержит перечень общих источников предшественников и индикаторов для каждой категории.

Таблица 3-1. Общие источники предшественников и индикаторов

Источник	Описание
	Предупреждения
IDPSs	Продукты IDPS определяют подозрительные события и делают запись подходящих данных относительно них, включая дату и время обнаружения атаки, тип нападения, источник и расположение IP адреса и имя пользователя (если применимо и известно). Большинство продуктов IDPS использует сигнатуры атак, чтобы определить злонамеренную активность; сигнатуры должны быть представлены так, чтобы могли быть обнаружены новейшие атаки. Программное обеспечение IDPS часто выдают *ложные предупреждения* — сообщают, что происходит злонамеренная активность, когда на самом деле ничего не происходит. Аналитики должны вручную проверять сообщения IDPS или тщательно пересматривая сопровождающие запись материалы или получая связанные данные из других источников.[31]
SIEMs	Продукты управления информацией и событиями безопасности (SIEM) подобны продуктам IDPS, но они генерируют тревоги на основе анализа данных журналов(см. ниже).
Антивирусы и программное обеспечение против спама	Антивирусное программное обеспечение обнаруживает различные формы вредоносного программного обеспечения, генерирует предупреждения и предотвращает инфицирование хостов вредоносным программным обеспечением. Существующие антивирусные продукты эффективны при предотвращении многих видов вредоносного программного обеспечения, если их сигнатуры актуальны. Программное обеспечение против спама используется, чтобы обнаружить спам и препятствовать тому, чтобы он достиг почтовых ящиков пользователей. Спам может содержать вредоносное программное обеспечение, фишинговые атаки и другое злонамеренное содержание, таким образом, предупреждения от программного обеспечения против спама могут указывать на попытки нападения.
Программное обеспечение проверки целостности файлов	Программное обеспечение проверки целостности файлов может обнаружить изменения, внесенные в важные файлы во время инцидентов. Оно использует алгоритм хеширования, чтобы получить криптографическую контрольную сумму для каждого определяемого файла. Если файл изменен и контрольная сумма повторно вычислена, существует чрезвычайно высокая вероятность, что новая контрольная сумма не будет соответствовать старой контрольной сумме. Регулярно повторно вычисляя контрольные суммы и сравнивая их с предыдущими значениями, можно обнаруживать изменения файлов.
Сервисы мониторинга третьих лиц	Третьи лица предлагают много основанных на подписке и свободных услуг мониторинга. Примером являются сервисы обнаружения мошенничества, которые уведомляют организацию, если ее IP адреса, доменные имена, и т.п. связаны с текущей инцидентной активностью, включающей другие организации. Имеются также свободные черные списки в реальном времени с подобной информацией. Другой пример стороннего сервиса мониторинга - список уведомления CSIRC; эти списки часто доступны только другим командам реагирования на инциденты.
	Журналы регистрации
Журналы регистрации операционных систем, сервисов и приложений	Журналы регистрации операционных систем, сервисов и приложений (особенно данные связанные с аудитом) часто имеют большое значение, когда происходит инцидент, как например, к каким учетным записям был получен доступ и какие действия были выполнены. Организации должны требовать базового уровня журналирования для всех систем и более высокого уровень для критических систем. Журналы регистрации могут использоваться для анализа, коррелируя информацию о событии. В зависимости от информации о событии тревога может быть сгенерирована, чтобы указать на инцидент. Раздел 3.2.4 обсуждает ценность централизованной регистрации.
Журналы регистрации сетевых устройств	Журналы регистрации сетевых устройств, таких как межсетевые экраны и маршрутизаторы, не являются, как правило, основным источником предшественников или индикаторов. Хотя эти устройства обычно конфигурируются так, чтобы регистрировать заблокированные попытки подключения, они предоставляют мало информации о сущности активности. Однако, они могут быть ценны в идентификации сетевых тенденций и в корреляции событий, обнаруженных другими устройствами.

[31] Посмотрите NIST SP 800-94, *Руководство по системам обнаружения и предотвращения вторжений,* для получения дополнительной информации о продуктах IDPS. Это доступно по http://csrc.nist.gov/publications/PubsSPs.html#800-94.

Источник	Описание
Сетевые потоки	Сетевой поток - конкретный сеанс связи, происходящий между хостами. Маршрутизаторы и другие сетевые устройства могут предоставить информацию сетевого потока, которая может использоваться, чтобы найти аномальную сетевую активность, вызванную вредоносным программным обеспечением, экс-фильтрацией данных и другими злонамеренными действиями. Есть много стандартов для форматов данных потока, включая NetFlow, sFlow, и IPFIX.
	Общедоступная информация
Информация относительно новых уязвимостей и эксплоитов	Нахождение в курсе новых уязвимостей и эксплоитов может препятствовать тому, чтобы произошли некоторые инциденты и помогать в обнаружении и анализе новых атак. National Vulnerability Database (NVD) содержит информацию относительно уязвимостей.[32] Организации, такие как US-CERT[33] и CERT®/CC периодически предоставляют информацию о новых угрозах через брифинги, веб-регистрации и списки рассылки.
	Люди
Люди от в организация	Пользователи, системные администраторы, сетевые администраторы, служба безопасности и другие в организации могут сообщать о признаках инцидентов. Важно проверять все такие сообщения. Один из подходов состоит в том, чтобы спросить людей, которые предоставляют такую информацию, насколько уверенны они в точности информации. Фиксация этой оценки наряду с предоставленной информацией может значительно помочь во время анализа инцидента, особенно когда обнаружены противоречивые данные.
Люди из других организаций	К отчетам по инцидентам, которые происходят во вне, нужно отнестись серьезно. Например, с организацией может связаться сторона, утверждающая, что система в организации нападает на её системы. Внешние пользователи могут также сообщить о других индикаторах, таких как стертая веб-страница или недоступный сервис. Другие команды реагирования на инциденты также могут сообщать об инцидентах. Важно иметь в распоряжении механизмы для третьих сторон, чтобы фиксировать индикаторы и для обучения персонала тщательно контролировать эти механизмы; это может быть просто подготовка номера телефона и адреса электронной почты, сконфигурированных так, чтобы отправить сообщения справочной службе.

3.2.4. Анализ инцидентов

Обнаружение и анализ инцидентов были бы легки, если бы каждый предшественник или индикатор были бы гарантированно точны; к сожалению, дело обстоит не так. Например, предоставляемые пользователями индикаторы, такие как жалобы на сервер, являющийся недоступным, часто неправильные. Системы обнаружения вторжений могут выдать ложные предупреждения — неправильные индикаторы. Эти примеры демонстрируют то, что делает обнаружение и анализ инцидентов настолько трудными: каждый индикатор в идеале должен быть оценен, чтобы определить, истин ли он. В довершение всего, общее количество индикаторов может быть тысячи или миллионы в день. Нахождение реальных инцидентов безопасности, которые произошли из всех индикаторов, может быть грандиозной задачей.

Даже если индикатор точен, это не обязательно означает, что инцидент произошел. Некоторые индикаторы, такие как отказ сервера или модификация критических файлов, могли произойти по нескольким причинам кроме инцидента безопасности, включая человеческую ошибку. Однако, учитывая появление индикаторов, обоснованно подозревать, что инцидент мог бы происходить и действовать соответственно. Определение, является ли конкретное событие на самом деле инцидентом, иногда является вопросом суждения. Чтобы принять решение, возможно необходимо сотрудничать с другим техническим персоналом и персоналом информационной безопасности. Во многих случаях ситуация должна быть обработана тем же самым способом независимо от того, является ли она связанной с безопасностью. Например, если организация теряет интернет-соединение каждые 12 часов, и никто не знает причины, персонал должен решать проблему столь же быстро и будет использовать те же самые ресурсы, чтобы диагностировать проблему, независимо от ее причины.

Некоторые инциденты легко обнаружить, такие как, явно стертая веб-страница. Однако, много инцидентов не связаны с такими ясными признаками. Небольшие признаки, такие как одно изменение в одном конфигурационном файле системы, могут быть единственными индикаторами того, что инцидент произошел. В обработке инцидентов, обнаружение может быть наиболее трудная задача. Обработчики инцидентов ответственны за анализ неоднозначных, противоречивых и неполных признаков, чтобы определить то, что произошло. Хотя существуют технические решения которые могут сделать обнаружение легче, лучшим средством является формирование команды высококвалифицированных и опытных сотрудников, которые могут проанализировать предшественники и индикаторы эффективно и разумно и принять соответствующие меры. Без

[32] http://nvd.nist.gov/

[33] http://www.us-cert.gov/cas/signup.html

хорошо обученного и способного персонала, обнаружение и анализ инцидентов будут проведены неэффективно и будут сделаны дорогостоящие ошибки.

Команда реагирования на инциденты должна работать быстро, чтобы анализировать и проверять каждый инцидент, следуя предопределенному процессу и документируя каждый сделанный шаг. Когда команда полагает, что инцидент произошел, команда должна быстро выполнить начальный анализ, чтобы определить область инцидента, такой как, какие сети, системы или приложения затронуты; кто или что породило инцидент; и как инцидент происходит (например, какие инструменты или методы атаки используются, какие уязвимости эксплуатируются). Начальный анализ должен предоставить достаточно информации для команды, чтобы расположить по приоритетам последующие работы, такие как сдерживание инцидента и более глубокий анализ результатов инцидента.

Выполнение начального анализа и проверки является сложным. Следующее - рекомендации для того, чтобы сделать анализ инцидентов более легким и эффективным:

- **Профиль сетей и систем.** *Профилирование* измеряет характеристики ожидаемой активности так, чтобы изменения к ней могли быть более легко определены. Примерами профилирования является запуск программного обеспечением проверки целостности файлов на хостах, чтобы получить контрольные суммы для критических файлов и мониторинг пропускной способности сети, используемый, чтобы определить, какие средние и пиковые уровни использования находятся в различные дни и время. На практике трудно обнаружить инциденты, точно используя большинство профильных технологий; организации должны использовать профилирование в качестве одной из нескольких технологий обнаружения и анализа.
- **Понимание нормального поведения.** Члены команды реагирования на инциденты должны изучить сети, системы и приложения, чтобы понять, в чём состоит их нормальное поведение так, чтобы неправильное поведение могло бы быть определено более легко. Обработчики инцидентов не могут иметь всестороннего знания всего поведения во всём окружении, но обработчики должны знать, какие эксперты могли заполнить пробелы. Один из способов - получить эти знания посредством рассмотрения записей в журналах и предупреждений системы безопасности. Это может быть утомительным, если не используется фильтрация, чтобы уплотнить журналы регистрации до разумного размера. По мере того, как обработчики становятся более знакомыми с журналами регистрации и предупреждениями, они должны быть в состоянии сосредоточиться на необъясненных записях, которые обычно более важны, чтобы заняться расследованиями. Проведение частых пересмотров журналов должно поддерживать свежие знания, и аналитик должен быть в состоянии заметить тенденции и изменения со временем. Пересмотры также дают аналитику индикатор надежности каждого источника.
- **Создайте политику хранения журналов.** Информация относительно инцидентов, может быть записана в нескольких местах, таких как межсетевой экран, IDPS и журналы приложений. Создание и реализация политики хранения журналов, которая определяет, сколько времени данные журналов должны поддерживаться может быть чрезвычайно полезным в анализе, потому что более старые записи в журнале могут показать разведывательную активность или предыдущие случаи подобных нападений. Другая причина хранения журналов регистрации состоит в том, что инциденты могут быть не обнаружены спустя дни, недели или даже несколько месяцев. Отрезок времени по поддержке данных журналов зависит от нескольких факторов, включая политику организации по хранению данных и объема данных. Посмотрите NIST SP 800-92, *Руководство* по *управлению журналами регистрации компьютерной безопасности* для дополнительных рекомендаций, связанных с регистрацией.[34]
- **Выполните корреляцию событий.** Свидетельство инцидента может охватить несколько журналов регистрации, при этом каждый содержит различные типы данных — у журнала регистрации межсетевого экрана может быть источник IP адреса который использовался, тогда как журнал приложения может содержать имя пользователя. Сетевой IDPS может обнаружить что атака была направлена против конкретного хоста, но он может не знать, было ли нападение успешно. Аналитик, возможно, должен исследовать журналы регистрации хоста, чтобы определить эту информацию. Корреляция событий среди множественных источников индикаторов может быть неоценимой в утверждении, произошел ли конкретный инцидент.

[34] http://csrc.nist.gov/publications/PubsSPs.html#800-9

- **Сохраняйте все часы хостов синхронизированными.** Протоколы, такие как Network Time Protocol (NTP) синхронизируют часы среди хостов.[35] Корреляция событий будет более сложной, если у устройств, сообщающих о событиях, будут несогласованные установки часов. С очевидной точки зрения предпочтительно иметь непротиворечивые метки времени в журналах регистрации — например, иметь три журнала регистрации, которые показывают, что атака произошла в 0:07:01, а не журналы, которые указывают атаку как произошедшую в 12:07:01, 12:10:35 и 11:07:06.
- **Поддерживайте и используйте базу знаний по информации.** База знаний должна включать информацию, которая обработчикам нужна для оперативных справок во время анализа инцидента. Хотя можно построить базу знаний со сложной структурой, простой подход тоже может быть эффективным. Текстовые документы, электронные таблицы и относительно простые базы данных предоставляют эффективные, гибкие и доступные для поиска механизмы для разделения данных среди членов команды. База знаний должна содержать разнообразную информацию, включая объяснения значения и соответствия предшественников и индикаторов, такую как предупреждения IDPS, записи в журнале операционной системы и коды ошибок приложений.
- **Используйте поисковые системы интернета для исследования. П**оисковые системы интернета могут помочь аналитикам находить информацию по необычной активности. Например, аналитик может видеть некоторые необычные попытки подключения, нацеленные на порт TCP 22912. Выполняя поиск по терминам «TCP», «порт» и «22912» можно получить некоторые запросы, которые содержат журналы регистрации подобной активности или даже объяснения значения номера порта. Обратите внимание на то, что для исследования должны использоваться отдельные рабочие станции, чтобы минимизировать риск организации от проведения этих поисков.
- **Запуск анализаторов пакетов для сбора дополнительных данных.** Иногда индикаторы не содержат достаточного количества деталей, чтобы дать возможность обработчику понять то, что происходит. Если инцидент происходит в сети, самым быстрым способом собрать необходимые данные может быть наличие анализатора пакетов для перехвата сетевого трафика. Конфигурация анализатора пакетов для записи трафика, которая соответствует указанным критериям, должна поддерживать управляемый объем данных и минимизировать непреднамеренный захват другой информации. Из-за интересов приватности некоторые организации могут требовать, чтобы обработчики инцидентов запрашивали и получали разрешение перед использованием анализаторов пакетов.
- **Фильтрация данных.** Имеется просто недостаточно времени, чтобы рассмотреть и проанализировать все индикаторы; по минимуму должна быть исследована самая подозрительная активность. Одна эффективная стратегия состоит в том, чтобы отфильтровывать категории индикаторов, которые имеют тенденцию быть незначительными. Другая стратегия фильтрации состоит в том, чтобы показывать только категории индикаторов, которые имеют самое высокое значение; однако, этот подход несет существенный риск, потому что новая злонамеренная активность может не попасть в одну из выбранных категорий индикаторов.
- **Ищите помощь от других.** Иногда команда будет неспособна определить точную причину и сущность инцидента. Если у команды отсутствует достаточная информация, чтобы сдержать и уничтожить инцидент, то она должна консультироваться с внутренними ресурсами (например, персоналом информационной безопасности) и внешними ресурсами (например, US-CERT, другой CSIRTs, подрядчики с экспертными знаниями по реагированию на инциденты). Важно точно определить причину каждого инцидента так, чтобы он мог быть полностью заглушен, а эксплуатируемые уязвимости могли быть сокращены, чтобы препятствовать тому, чтобы произошли подобные инциденты.

3.2.5. Документация инцидента

Команда реагирования на инциденты, которая подозревает, что инцидент произошел, должна немедленно начать делать запись всех фактов относительно инцидента.[36] Вахтенный журнал - эффективная и простая среда для этого,[37] но ноутбуки, магнитофоны и цифровые фотоаппараты

[35] Больше информации относительно NTP доступно по http://www.ntp.org/.

[36] Обработчики инцидентов должны регистрировать только факты по инциденту, а не личные мнения или заключения. Субъективный материал должен быть представлен в сообщениях о происшествии, не фиксируемых как свидетельство.

[37] Если используется вахтенный журнал, то предпочтительно, чтобы вахтенный журнал бал перевязан, и чтобы обработчики инцидентов нумеровали страницы, писали чернилами и не повреждали вахтенный журнал (т.е., не вырывали страницы).

также могут служить этому назначению.[38] Документирование системных событий, разговоров и наблюдаемых изменений в файлах может привести к более эффективной, более систематизированной и менее подверженной ошибкам обработке проблемы. Каждый шаг, сделанный от времени, когда инцидент был обнаружен, до его окончательного разрешения, должен быть зарегистрирован и добавлена метка времени. На каждом документе относительно инцидента необходимо проставить дату и подписать обработчика инцидента. Информация такого характера может использоваться также в качестве свидетельства в суде, действующем по нормам общего права, если производится законное судебное расследование. Каждый раз, когда возможно, обработчики должны работать в командах по крайней мере вдвоём: один человек может делать записи и регистрировать события, в то время как другой человек выполнять технические задачи. Раздел 3.3.2 представляет больше информации о свидетельствах.[39]

Команда реагирования на инциденты должна поддерживать записи о статусе инцидентов, наряду с другой уместной информацией.[40] Использование приложения или базы данных, таких как система отслеживания задач, помогает гарантировать, что инциденты обрабатываются и разрешаются своевременно. Система отслеживания задач должна содержать информацию относительно следующего:

- Текущий статус инцидента (новый, происходящий, отправленный для расследования, решенный, и т.д.)
- Резюме инцидента
- Индикаторы, относящиеся к инциденту
- Другие инциденты, имеющие отношение к этому инциденту
- Меры, принятые всеми обработчиками инцидента по этому инциденту
- Последовательность заключений, если возможно
- Оценки воздействий, имеющие отношение к инциденту
- Контактная информация других участвующих сторон (например, владельцев системы, системных администраторов)
- Список свидетельств, собранных во время расследования инцидента
- Комментарии от обработчиков инцидента
- Следующие шаги, которые будут сделаны (например, восстановление хоста, модернизация приложения).[41]

Команда реагирования на инциденты должна хранить данные об инциденте и ограничить доступ к ним, потому что они часто содержат чувствительную информацию — например, данные по эксплуатируемым уязвимостям, недавним нарушениям защиты и пользователям, которые, возможно, выполнили несоответствующие действия. Например, только у санкционированного персонала должен быть доступ к базе данных инцидента. Сообщения по инциденту (например, электронные письма) и документы должны быть зашифрованы или иначе защищены так, чтобы прочитать их мог только санкционированный персонал.

---

[38] Рассмотрите допустимость свидетельств, собираемых с помощью устройства, перед их использованием. Например, любые устройства, которые являются потенциальными источниками свидетельств, не должны сами использоваться для того, чтобы записывать другие свидетельства.

[39] NIST SP 800-86, *Руководство по интеграции технологий расследования в реагирование на инциденты,* предоставляет подробную информацию об установлении возможностей по расследованию, включая разработку политик и процедур.

[40] Приложение B содержит предлагаемый список элементов данных, для сбора при сообщении об инцидентах. Кроме того, документ CERT®/CC *Состояние практик команд реагирования на инциденты компьютерной безопасности (CSIRTs)* содержит несколько типовых форм отчетности об инцидентах. Документ доступен в http://www.cert.org/archive/pdf/03tr001.pdf.

[41] Трансъевропейская Ассоциация исследований и образования по сетям (TERENA) разработала RFC 3067, *Требования TERENA по описанию объекта и формату обмена по инцидентам* (http://www.ietf.org/rfc/rfc3067.txt). Документ предоставляет рекомендации по тому, какая информация должна быть собрана для каждого инцидента. Рабочая группа IETF по расширенной обработке инцидентов (inch) (http://www.cert.org/ietf/inch/inch.html), разработала RFC, который подробно останавливается на работе TERENA — RFC 5070, *Формат обмена описаниями объекта инцидента* (http://www.ietf.org/rfc/rfc5070.txt).

3.2.6. Назначение приоритетов инцидентов

Приоритизация обработки инцидентов является, возможно, самым критическим моментом принятия решений в процессе обработки инцидентов. Исходя из ограниченности ресурсов, инциденты не должны обрабатываться по принципу «первым прибыл, первым обслужен». Вместо этого обработка должна быть распределена по приоритетам на основе соответствующих факторов, таких как:

- **Функциональное воздействие инцидента.** Инциденты, предназначающиеся для ИТ-систем влияют, как правило, на деловую функциональность, которую эти системы предоставляют, проявляясь в некотором типе негативного воздействия на пользователей этих систем. Обработчики инцидентов должны рассмотреть, как инцидент повлияет на существующую функциональность затронутых систем. Обработчики инцидента должны рассмотреть не только текущее функциональное воздействие инцидента, но также и вероятное будущее функциональное воздействие инцидента, если это немедленно не определяется.
- **Информационное воздействие инцидента.** Инциденты могут затронуть конфиденциальность, целостность и доступность информации организации. Например, злонамеренный источник может экс-фильтровать чувствительную информацию. Обработчики инцидента должны рассмотреть, как эта экс-фильтрация информации повлияет на полное предназначение организации. Инцидент, который приводит к экс-фильтрации чувствительной информации, может также затронуть другие организации, если какие-либо из данных принадлежали партнерской организации.
- **Восстанавливаемость от инцидента.** Размер инцидента и тип ресурсов, которые он затрагивает, определяют количество времени и ресурсы, которые должны быть потрачены на восстановление от инцидента. В некоторых случаях невозможно восстановиться после инцидента (например, если скомпрометирована конфиденциальность чувствительной информации), и нет смысла тратить ограниченные ресурсы на длинный цикл обработки инцидента, если это усилие не направлено на обеспечение того, чтобы подобный инцидент не произошел в будущем. В других случаях инцидент может потребовать для обработки гораздо больше ресурсов, чем те, что имеет в наличии организация. Обработчики инцидента должны определять усилия, которые необходимы, чтобы восстановиться после инцидента и тщательно взвешивать их против стоимости, которую потребуют усилия по восстановлению и любых требований, связанных с обработкой инцидента.

Объединение функционального воздействия на системы организации и воздействия на информацию организации определяет влияние инцидента на деятельность— например, распределенная атака «отказ в обслуживании» на публичный сервер может временно уменьшить функциональность для пользователей, пытающихся получить доступ к серверу, тогда как несанкционированный доступ корневого уровня к публичному серверу может привести к экс-фильтрации персональной идентификационной информации (PII), которая может оказать длительное влияние на репутацию организации.

Восстанавливаемость от инцидента определяет возможные реакции, которые команда может принять, обрабатывая инцидент. Инцидент с высоким функциональным воздействием и низким усилием по восстановлению является идеальным кандидатом на незамедлительное принятие мер от команды. Однако некоторые инциденты могут не иметь лёгких путей восстановления и, возможно, должны находиться в очереди для реакции более стратегического уровня — например, для инцидента, который приводит к экс-фильтрации и публичному распространению по почте атакующим гигабайтов чувствительных данных, нет легкого пути восстановления, так как данные уже раскрыты; в этом случае команда может передать часть ответственности за обработку инцидента экс-фильтрации данных команде более стратегического уровня, которая разрабатывает стратегию для предотвращения нарушений в будущем и создает план поддержки приведения в готовность тех людей или организаций, данные которых экс-фильтровались. Команда должна расположить по приоритетам реакцию на каждый инцидент на основе оценки влияния на деятельность, вызванного инцидентом, и предполагаемые усилия, требуемые для восстанавления после инцидента.

Организация может лучше определить эффект своих собственных инцидентов из-за их ситуативного освоения. Таблица 3-2 предоставляет примеры функциональных категорий воздействия, которые организация могла бы использовать для рейтинга ее собственных инцидентов. Рейтинг инцидентов может быть полезным в приоритизации ограниченных ресурсов.

Таблица 3-2. Категории функционального воздействия

Категория	Определение
Нет	Нет влияния на способность организации предоставить все услуги всем пользователям
Низкое	Минимальный эффект; организация может продолжать предоставлять все критические услуги всем пользователям, но с низкой эффективностью
Среднее	Организация потеряла способность предоставлять критическую услугу подмножеству пользователей системы
Высокое	Организация больше не в состоянии предоставлять некоторые критические услуги любым пользователям

Таблица 3-3 предоставляет примеры возможных категорий информационного воздействия, которые описывают степень информационной компрометации, произошедшей во время инцидента. В этой таблице, за исключением оценки «Нет», категории не взаимоисключающие и организация может выбрать более чем одну.

Таблица 3-3. Категории информационного воздействия

Категория	Определение
Нет	Нет информации, которая бы экс-фильтровалась, изменялась, удалялась, или иначе ставилась под грозу
Нарушение приватности	Произведен доступ к или экс-фильтрация чувствительной персональной идентификационной информации (PII) налогоплательщиков, сотрудников, владельцев и т.д.
Нарушение конфиденциальности	Произведен доступ к или экс-фильтрация несекретной конфиденциальной информации, такой как защищаемая информация важной инфраструктуры (PCII)
Потеря целостности	Чувствительная или конфиденциальная информация была изменена или удалена

Таблица 3-4 показывает примеры категорий усилий по восстановлению, которые отражают уровень и тип ресурсов, требуемых для восстановления после инцидента.

Таблица 3-4. Категории усилий по восстановлению

Категория	Определение
Регулярные	Время по восстановлению предсказуемо при существующих ресурсах
Дополнительные	Время по восстановлению предсказуемо с дополнительными ресурсами
Расширенные	Время по восстановлению непредсказуемо; необходимы дополнительные ресурсы и помощь извне
Восстановление невозможно	Восстановление после инцидента невозможно (например, чувствительные данные экс-фильтрованы и представлены публично); необходимо осуществлять расследование

Организации должны также установить процесс эскалации для тех случаев, когда команда не реагирует на инцидент в течение определяемого времени. Это может произойти по многим причинам: например, сотовые телефоны могут быть недоступны, или у людей могут быть личные чрезвычайные ситуации. Процесс эскалации должен указывать, сколько времени человек должен ждать реакции и что делать, если реакция не происходит. Обычно на первом шаге должен дублироваться начальный контакт. После ожидания в течение короткого времени — возможно, 15 минут — сообщающий должен передать инцидент к следующему уровню, такому как менеджер команды реагирования на инциденты. Если этот человек не отвечает в течение некоторого времени, то инцидент должен быть снова передан к следующему уровню управления. Этот процесс должен быть повторен до тех пор, пока кто-то не ответит.

3.2.7. Уведомление об инциденте

Когда инцидент проанализирован и ему определён приоритет, команда реагирования на инциденты должна уведомить соответствующих людей так, чтобы все, кто должен быть включен, выполняли их роли. Политики реагирования на инциденты должны включать положения относительно отчетности об инцидентах — как минимум, о чем нужно сообщить, кому и в какое время (например, начальное

уведомление, регулярные обновления статуса). Точные требования к отчетности варьируются среди организаций, но стороны, которые, как правило, уведомляются, включают:

- Директор по информации
- Руководитель информационной безопасности
- Местный директор по информационной безопасности
- Другие команды реагирования на инциденты в организации
- Внешние команды реагирования на инциденты (если соответствующе)
- Владелец системы
- Кадровый орган (для случаев, включающих сотрудников, таких как домогательство по электронной почте)
- Орган по связям с общественностью (для инцидентов, которые могут генерировать публичную информацию),
- Юридический департамент (для инцидентов с потенциальными юридическими ответвлениями)
- US-CERT (требованное для Федеральных агентств и систем, работающих от имени Федерального правительства; смотрите Раздел 2.3.4.3),
- Правоохранительные органы (если соответствующе)

Во время обработки инцидента команда, возможно, должна предоставлять обновления статуса некоторым сторонам, даже в некоторых случаях всей организации. Команда должна спланировать и подготовить несколько методов взаимодействия, включая неэлектронные методы (например, лично, на бумаге), и выбрать методы, которые подходят для конкретного инцидента. Возможные методы взаимодействия включают:

- Электронная почта
- Вебсайт (внутренний, внешний или портал)
- Телефонные звонки
- Лично (например, ежедневные брифинги)
- Голосовое сообщение почтового ящика (например, настройка отдельного голосового почтового ящика для обновлений инцидента и обновление голосового сообщения для отражения текущего статуса инцидента; использование сообщения голосовой почты справочной службы),
- Бумага (например, почтовые уведомления на досках объявлений и дверях, раздача уведомлений во всех точках входа).

3.3. Сдерживание, уничтожение и восстановление

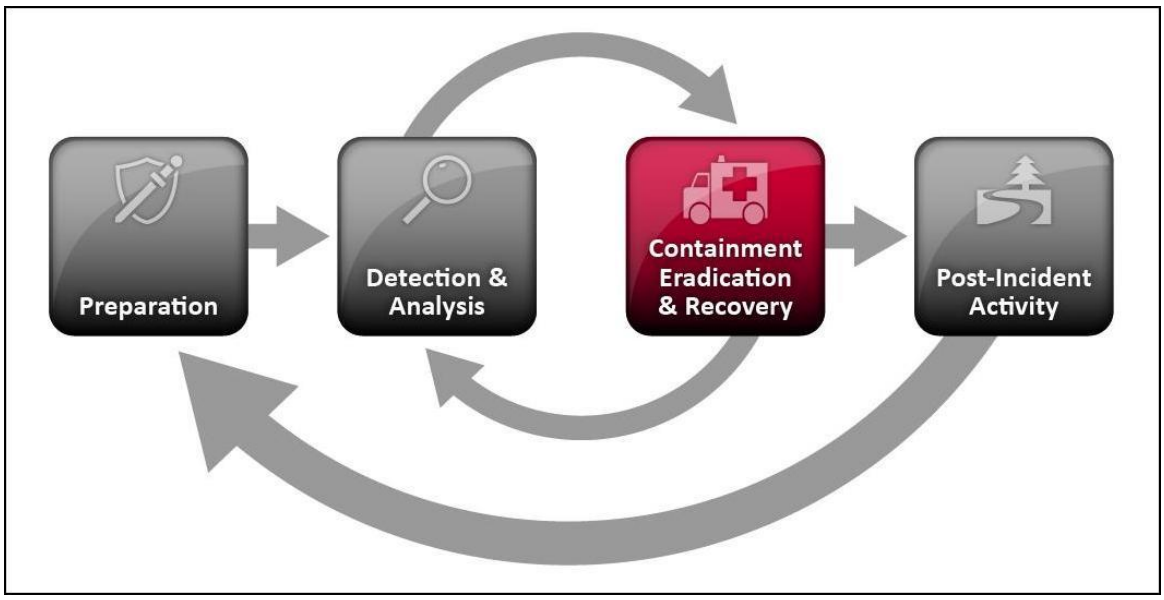

Рисунок 3-3. Жизненный цикл реагирования на инциденты (сдерживание, уничтожение и восстановление)

3.3.1. Выбор стратегии сдерживания

Сдерживание важно, прежде чем инцидент переполнит ресурсы или превысит ущерб. Большинство инцидентов требует сдерживания, так, чтобы важное рассмотрение было как можно раньше в ходе обработки каждого инцидента. Сдерживание предоставляет время для разработки адаптированной стратегии устранения. Основная часть сдерживания - принятие решения (например, выключить систему, разъединить ее от сети, отключить некоторые функции). Такие решения намного легче принять, если есть предопределенные стратегии и процедуры сдерживания инцидента. Организации должны определить приемлемые риски при обращении с инцидентами и разработать соответствующие стратегии.

Стратегии сдерживания варьируются на основе типа инцидента. Например, стратегия сдерживания вредоносной инфекции, перенесенной электронной почтой, очень отличается от сетевой DDos-атаки. Организации должны создать отдельные стратегии сдерживания для каждого основного типа инцидента с ясно определёнными критериями, чтобы облегчить принятие решения. Критерии определения правильной стратегии включают:

- Потенциальный ущерб ресурсам и хищение ресурсов
- Потребность в сохранении свидетельств
- Доступность сервиса (например, сетевое соединение, услуги, предоставленные третьим сторонам)
- Время и ресурсы, необходимые для реализации стратегии
- Эффективность стратегии (например, частичное сдерживание, полное сдерживание)
- Длительность решения (например, чрезвычайная работа, которая будет завершена через четыре часа, временная работа, которая будет завершена через две недели, постоянное решение).

В определенных случаях некоторые организации перенаправляют атакующего к песочнице (форма сдерживания) так, чтобы они могли контролировать работу атакующего, обычно чтобы собрать дополнительные свидетельства. Команда реагирования на инциденты должна обсудить эту стратегию со своим юридическим департаментом, чтобы определить, выполнимо ли это. Способы контролировать работу атакующего кроме игры в песочнице не должны использоваться; если организация знает, что система была скомпрометирована и позволяет компрометации продолжаться, она может быть ответственной за то, что атакующий использует скомпрометированную систему, чтобы

атаковать другие системы. Отложенная стратегия сдерживания опасна, потому что атакующий может нарастить несанкционированный доступ или поставить под угрозу другие системы.

Другая потенциальная проблема относительно сдерживания - то, что некоторые нападения могут нанести дополнительный ущерб, когда они сдерживаются. Например, скомпрометированный хост может запустить злонамеренный процесс, который будет периодически запрашивать другой хост. Когда обработчик инцидента попытается сдержать инцидент, разъединяя скомпрометированный хост от сети, последующие запросы будут терпеть неудачу. В результате отказа злонамеренный процесс может переписать или зашифровать все данные на жестком диске хоста. Обработчики не должны предполагать, что просто потому, что хост был разъединен от сети, дальнейший вред хосту будет предотвращен.

3.3.2. Сбор и обработка свидетельств

Хотя основная причина сбора свидетельств во время инцидента состоит в том, чтобы разрешить инцидент, это может также быть необходимо для процессуальных действий.[42] В таких случаях важно для полноты документа, чтобы все свидетельства, включая по скомпрометированным системам, были сохранены.[43] Доказательства должны быть собраны согласно процедурам, учитывающим все действующие законы и нормативные документы, которые были разработаны по предыдущим обсуждениям с юридическим персоналом и соответствующими правоохранительными органами таким образом, чтобы любое свидетельство могло бы быть принято в суде.[44] Кроме того, свидетельство должно составляться в любом случае; каждый раз, когда свидетельство передаётся от человека к человеку, цепочка форм заключений должна детализировать передачу и включать подпись каждой стороны. Подробный журнал регистрации должен хранить всё о свидетельствах, включая следующее:

- Идентификационную информацию (например, местоположение, серийный номер, номер модели, имя хоста, адреса контроля доступа к носителю информации (MAC) и IP адреса компьютеров)
- Имя, название и номер телефона каждого человека, который собрал или обрабатывал свидетельства во время расследования
- Время и дата (включая часовой пояс) каждого случая обработки свидетельств
- Местоположение, где свидетельства были сохранены.

Сбор свидетельств с вычислительных ресурсов представляет некоторые проблемы. Вообще желательно получать свидетельство об интересуемой системы, как только есть подозрение, что инцидент, возможно, произошел. Много инцидентов порождают динамическую цепь событий; начальный образ состояния системы может быть более полезным в идентификации проблемы и ее источника, чем большинство других мер, которые могут быть приняты на данном этапе. С очевидной точки зрения, намного лучше получить моментальный образ системы вместо того, чтобы делать это после того, как обработчики инцидента, системные администраторы и другие непреднамеренно изменили состояние машины во время расследования. Пользователи и системные администраторы должны быть осведомлены о шагах, которые они должны сделать, чтобы сохранить свидетельства. Посмотрите NIST SP 800-86, *Руководство по интеграции технологий расследования в реагирование на инциденты*, для получения дополнительной информации о сохранении свидетельств.

---

[42] NIST SP 800-86, *Руководство по интеграции технологий расследования в реагирование на инциденты,* предоставляет подробную информацию об установлении возможности расследования. Оно сосредотачивается на технологиях расследования для PC, но большая часть материала применима и к другим системам. Документ может быть найден по http://csrc.nist.gov/publications/PubsSPs.html#800-86.

[43] Сбор и обработка свидетельств, как правило, не выполняются для каждого инцидента, который происходит — например, большинство вредоносных инцидентов не заслуживают получения свидетельств. Во многих организациях цифровые действия по расследованию не являются необходимыми для большинства инцидентов.

[44] *Поиск и захват компьютеров и получение электронного свидетельства в уголовных расследованиях*, от Секции компьютерных преступления и интеллектуальной собственности (CCIPS) Министерства юстиции, предоставляет законное руководство по сбору свидетельств. Документ доступен по http://www.cybercrime.gov/ssmanual/index.html.

3.3.3. Определение атакующих хостов

Во время обработки инцидента владельцы систем и другие иногда хотят или должны опознать атакующий хост или хосты. Хотя эта информация может быть важной, обработчики инцидента должны обычно оставаться нацеленными на сдерживание, уничтожение и восстановление. Определение атакующего хоста может отнимать много времени и быть бесполезным процессом, который может мешать тому, чтобы команда достигла своей основной цели — уменьшение влияния на деятельность. Следующие элементы описывают обычно выполняемые работы по определению атакующего хоста:

- **Определение IP адреса атакующего хоста.** Новые обработчики инцидентов часто сосредотачиваются на IP адресе атакующего хоста. Обработчик может попытаться определить, что адрес не был сымитирован, проверив возможность соединения к нему; однако, это просто указывает, что хост по тому адресу отвечает или не отвечает на запросы. Отказ ответить не означает, что адрес не реален — например, хост, может быть сконфигурирован так, чтобы игнорировать запросы и traceroutes. Кроме того, нападавший, возможно, получил динамический адрес, который был уже повторно назначен на кого-то еще.
- **Исследование атакующего хоста через поисковые системы.** Интернет-поиск с использованием IP адреса очевидного источника нападения может привести к большей информации относительно нападения — например, списку рассылки сообщений относительно подобного нападения.
- **Использование баз данных инцидентов.** Несколько групп собирают и объединяют данные об инцидентах различных организаций в базы данных инцидентов. Это совместное пользование информацией может происходить в различных формах, таких как черные списки следящих систем и реального времени. Организация может также проверить свою собственную базу знаний или систему отслеживания задач для соответствующих действий.
- **Мониторинг возможных каналов связи атакующего.** Обработчики инцидента могут контролировать каналы связи, которые могут быть использованы атакующим хостом. Например, много ботов используют IRC в качестве своих основных средств сообщения. Кроме того, атакующие могут собираться на некоторых IRC каналах, чтобы хвастать об их компрометациях и делиться информацией. Однако обработчики инцидентов должны рассматривать любую такую информацию, которую они получают, только как потенциальную версию, а не как факт.

3.3.4. Уничтожение и восстановление

После того, как инцидент сдержан, может быть необходимо уничтожение по устранению компонент инцидента, такое как удаление вредоносного программного обеспечения и аннулирование нарушенных учетных записей пользователей, а также идентификация и смягчение всех уязвимостей, которые использовались. Во время уничтожения важно опознать все затронутые хосты в организации так, чтобы они могли быть повторно установлены. Для некоторых инцидентов уничтожение или не требуется, или выполняется во время восстановления.

При восстановлении администраторы возвращают системы к нормальному функционированию, подтверждают, что системы функционируют обычно, и (если применимо) исправляют уязвимости, чтобы предотвратить подобные инциденты. Восстановление может включать такие действия как восстановление систем из чистых резервных копий, восстановление систем с нуля, замена скомпрометированных файлов чистыми версиями, установка патчей, изменение паролей и усиление безопасности сетевого периметра (например, набора правил межсетевого экрана, списков управления доступом пограничного маршрутизатора). Верхние уровни системной регистрации или сетевого мониторинга часто являются частью процесса восстановления. Как только ресурс успешно атакован, он часто подвергается атаке снова, или другие ресурсы в организации подвергаются атаке подобным образом.

Уничтожение и восстановление должны быть сделаны поэтапно так, чтобы шаги устранения были расположены по приоритетам. Для крупномасштабных инцидентов восстановление может занять месяцы; намерение ранних фаз должно состоять в том, чтобы увеличить полную безопасность путём относительно быстрых (дни, недели) высоко значимых изменений, чтобы предотвратить будущие инциденты. Более поздние фазы должны быть нацелены на долгосрочные изменения (например, изменения инфраструктуры) и постоянную работу, чтобы сохранить предприятие максимально безопасным.

Поскольку действия по уничтожению и восстановлению, как правило, специфичны для ОС и приложений, подробные рекомендации и советы относительно них выходят за рамки этого документа.

3.4. Действия постинцидента

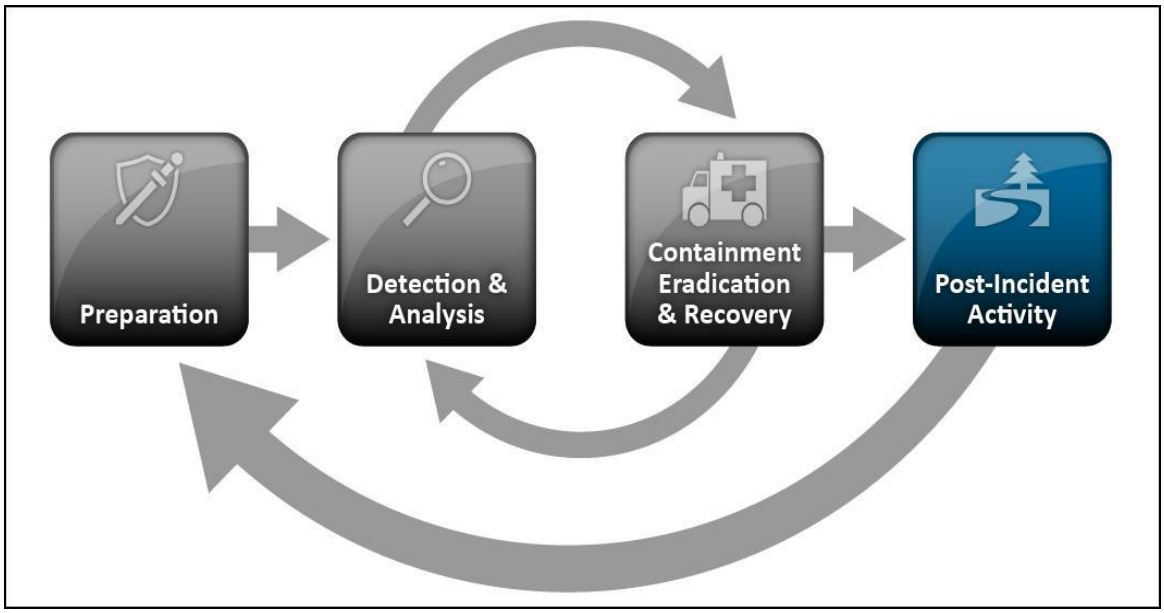

Рисунок 3-4. Жизненный цикл реагирования на инциденты (действия постинцидента)

3.4.1. Изучение уроков

Одна из самых важных частей реагирования на инциденты является также чаще всего опущенной: изучение и улучшение. Каждая команда реагирования на инциденты должна развиваться, чтобы отражать новые угрозы, улучшать технологию и извлекать уроки. “Изучение уроков” при встрече со всеми участвующими сторонами после основного инцидента, и периодически после меньших инцидентов, когда позволяют ресурсы, может быть чрезвычайно полезным в мерах по повышению безопасности и в самом процессе обработки инцидентов. Многие инциденты могут быть закрыты просто изучением уроков на встречах. Эта встреча предоставляет шанс достигнуть закрытия в отношении инцидента, пересматривая то, что произошло, что было сделано по вмешательству, и как хорошо вмешательство сработало. Встреча должна быть проведена в течение нескольких дней после конца инцидента. Вопросы, на которые нужно ответить при встрече, включают:

- Что точно произошло, и в какое время?
- Как хорошо действовал персонал и руководство имея дело с инцидентом? Были ли выполнены задокументированные процедуры? Действительно ли они были адекватны?
- Какая информация была необходима раньше?
- Были ли предприняты какие-либо шаги или действия, которые, возможно, затруднили восстановление?
- Что персонал и руководство сделали бы по-другому в следующий раз, когда бы подобный инцидент произошёл? Как может быть улучшен обмен информацией с другими организациями?
- Какие корректирующие действия могут предотвратить подобные инциденты в будущем?
- За какими предшественниками или индикаторами нужно наблюдать в будущем, чтобы обнаружить подобные инциденты?
- Какие дополнительные инструменты или ресурсы необходимы, чтобы обнаружить, проанализировать и смягчить будущие инциденты?

Для маленьких инцидентов нужен ограниченный постинцидентный анализ, за исключением инцидентов, выполненных посредством новых методов атаки, которые представляют большую озабоченность и интерес. После того, как серьезные атаки произошли, обычно стоит провести постфактум встречи, которые выходят за рамки команды и организации, чтобы предоставить механизм для совместного пользования информацией. Основное внимание при проведении таких встреч должно быть направлено на то, чтобы были включены нужные люди. Мало того, что важно пригласить людей, которые были вовлечены в инцидент, который анализируется, но также важно рассмотреть, кто должен быть приглашен в целях облегчения будущей кооперации.

Успех таких встреч также зависит от повестки дня. Сбор запросов об ожиданиях и потребностях (включая предложенные темы для рассмотрения) от участников перед встречами увеличивает вероятность того, что потребности участников будут удовлетворены. Кроме того, установление правил в начале или во время начала встречи может минимизировать путаницу и разногласие. Наличие одного или нескольких модераторов, которые квалифицированы в групповых действиях, может привести к высокой отдаче. Наконец, также важно задокументировать важные пункты соглашения и практические меры и сообщить их сторонам, которые не могли посетить встречу.

Встречи по изучению уроков предоставляют и другие преимущества. Отчеты об этих встречах - хороший материал для обучения новых членов команды, показывая им, как более опытные члены команды реагируют на инциденты. Обновление политик реагирования на инциденты и процедур является другой важной частью процесса изучения уроков. Анализ постфактум способа, которым был обработан инцидент, будет часто показывать недостающие шаги или погрешность в процедуре, предоставляя стимул для изменений. Из-за изменяющейся сущности информационных технологий и изменений в персонале, команда реагирования на инциденты должна рассмотреть всю связанную документацию и процедуры обработки инцидентов в определяемых интервалах.

Другой важной работой постинцидента является создание заключительного отчет для каждого инцидента, который может быть довольно ценным для будущего использования. Отчет предоставляет справку, которая может использоваться, чтобы помочь в обработке подобных инцидентов. Создание формальной хронологии событий (включая информацию с меткой времени, такую как логи данных от систем) важно по юридическим причинам, также как финансовая оценка суммы ущерба, вызванного инцидентом. Эта оценка может стать основанием для последующих действий судебного расследования такими сущностями, как офис Главного федерального прокурора США. Последующие отчеты должны быть сохранены на период времени, который определен в политиках хранения отчётов.[45]

3.4.2. Использование собранных данных об инциденте

Действия по изучению уроков должны произвести ряд объективных и субъективных данных относительно каждого инцидента. Со временем собранные данные об инциденте должны быть полезными в нескольких направлениях. Данные, особенно полное время участия и стоимость, могут быть используемы, чтобы оправдать дополнительное финансирование команды реагирования на инциденты. Исследование особенностей инцидента может указать на слабые места системы безопасности и угрозы, а также изменения в тенденциях инцидента. Эти данные могут быть положены в процесс оценки степени риска, в конечном счете ведя к выбору и реализации дополнительных мер обеспечения безопасности. Другим хорошим использованием данных является измерение успешности команды реагирования на инциденты. Если данные об инциденте собраны и сохранены правильно, они могут предоставить несколько оценок успеха (или по крайней мере работы) команды реагирования на инциденты. Данные об инциденте могут также быть собраны, чтобы определить, вызывает ли изменение в возможности реагирования на инциденты соответствующее изменение в деятельности команды (например, улучшения действенности, сокращения стоимости). Кроме того, организации, которые обязаны сообщать информацию об инциденте, должны будут собирать

[45] General Records Schedule (GRS) 24, *Отчёты по эксплуатации и управлению информационными технологиями*, определяет что “отчёты и последующие записи по обработке инцидентов по компьютерной безопасности,” должны быть ликвидированы через “3 года после того, как все необходимые дополнительные меры были завершены”. GRS 24 доступен из Национального управления архивов и документации по http://www.archives.gov/records-mgmt/grs/grs24.html.

необходимые данные, чтобы удовлетворить требованиям. Посмотрите Раздел 4 для получения дополнительной информации об обмене данными об инциденте с другими организациями.

Организации должны сосредоточиться на сборе данных, которые являются применимыми, вместо того, чтобы собирать данные просто потому, что они доступны. Например, подсчёт числа предшествующих сканирований портов, которые происходят каждую неделю и формирование в конце года диаграммы, которая показывает, что сканирование портов увеличилось на восемь процентов, не очень полезно и может быть просто потерей времени. Абсолютные числа не информативны — имеет значение понимание того, какие они представляют угрозы процессам деятельности организации. Организации должны решить, какие данные об инциденте собирать на основе требований к отчетности и на основе ожидаемого дохода от инвестиций в данные (например, определение новой угрозы и сокращение соответствующих уязвимостей, прежде чем они смогут использоваться.) Возможные метрики для данных, связанных с инцидентом, включают:

- **Число обработанных инцидентов.**[46] Обработка большего количества инцидентов не обязательно лучше — например, число обработанных инцидентов может уменьшиться из-за лучших мер обеспечения сетевой и хостовой безопасности, а не из-за небрежности команды реагирования на инциденты. Число обработанных инцидентов лучше всего взять в качестве меры относительного объема работы, которую команда реагирования на инциденты должна была выполнить, а не как мера качества команды, если это не рассматривать в контексте других мер, которые совместно дают признак качества работы. Более эффективно произвести отдельный подсчёт инцидентов для каждой категории инцидентов. Подкатегории также могут использоваться, чтобы предоставить больше информации. Например, возросшее число инцидентов, выполненных инсайдерами, может вызвать более строгие положения политики относительно фоновых расследований для персонала и неправильного употребления вычислительных ресурсов и более строгие меры безопасности для внутренних сетей (например, развертывание программного обеспечения обнаружения вторжений для более внутренних сетей и хостов).
- **Время на инцидент.** Для каждого инцидента время может быть измерено несколькими способами:
  - Общая сумма труда, потраченного работающими по инциденту
  - Время, прошедшее с начала инцидента до обнаружения инцидента, до начальной оценки воздействия, и до каждой стадии процесса обработки инцидента (например, сдерживания, восстановления)
  - Сколько времени заняло у команды реагирования на инциденты, чтобы ответить на первоначальное сообщение об инциденте
  - Сколько времени заняло, чтобы сообщить об инциденте руководству и, при необходимости, соответствующим внешним сущностям (например, US-CERT).
- **Объективная оценка каждого инцидента.** Реакция на инцидент, который был решен, может быть проанализирована, чтобы определить, насколько она была эффективна. Ниже приводятся примеры выполнения объективной оценки инцидента:
  - Рассмотрение журналов регистрации, форм, отчетов и другой документации инцидента для приверженности установленным политикам и процедурам реагирования на инциденты
  - Определение, какие предшественники и индикаторы инцидента были зарегистрированы, чтобы определить, как эффективно инцидент был зафиксирован и определён
  - Определение, нанес ли инцидент ущерб, прежде чем он был обнаружен

[46] Метрики, такие как число обработанных инцидентов, обычно не имеют значения в сравнении различных организаций, потому что каждая организация, вероятно, определяет ключевые термины по-разному. Например, большинство организаций определяет «инцидент» с точки зрения своих собственных политик и методов, и то что одна организация рассматривает как отдельный инцидент, может быть рассмотрено другими как множественные инциденты. Более конкретные метрики, такие как число сканирований портов, имеют также мало значения в сравнениях организаций. Например, очень маловероятно, что различные системы безопасности, такие как сетевые датчики обнаружения вторжений, все будут использовать те же самые критерии в маркировке такой активности, как сканирование портов.

  - Определение, была ли определена фактическая причина инцидента, и определение вектора атаки, используемых уязвимостей, и характеристик целевых или пострадавших систем, сетей и приложений
  - Определение, является ли инцидент повторением предыдущего инцидента
  - Вычисление предполагаемого денежного ущерба от инцидента (например, информации и критических бизнес-процессов, негативно затронутых инцидентом)
  - Измерение различия между начальной оценкой воздействия и заключительной оценкой воздействия (см. Раздел 3.2.6),
  - Идентификация, какие меры, если таковые имеются, возможно, предотвратили инцидент.
- **Субъективная оценка каждого инцидента.** Члены команды реагирования на инциденты могут быть опрошены по оценке своей собственной работы, а также других членов команды и всей команды. Другой ценный источник данных - владелец ресурса, который подвергся нападению, чтобы определить, думает ли владелец, что инцидент был обработан эффективно, и является ли результат удовлетворительным.

Помимо использования этих метрик, чтобы измерить успех команды, организации могут также счесть полезным периодически пересматривать их программы реагирования на инциденты. Аудиты определят проблемы и недостатки, которые могут быть исправлены. Как минимум аудит реагирования на инциденты должен оценить следующие элементы в отношении применимого регулирования, политик и общепринятых методов:

- Политики, планы и процедуры реагирования на инциденты
- Инструменты и ресурсы
- Модель и структура команды
- Обучение и тренированность обработчиков инцидента
- Документация и отчеты по инцидентам
- Меры успеха, обсужденные ранее в этом разделе.

3.4.3. Хранение свидетельств

Организации должны установить политику, как долго должны храниться свидетельства по инциденту. Большинство организаций принимает решение хранить все свидетельства в течение месяцев или спустя годы после того, как инцидент завершился. Следующие факторы нужно рассмотреть во время создания политики:

- **Расследование.** Если возможно, что атакующий будет преследоваться по суду, свидетельства, возможно, должны быть сохранены, пока все судебные иски не будут завершены. В некоторых случаях это может занять несколько лет. Кроме того, свидетельства, которые кажутся незначительными теперь, могут стать более важными в будущем. Например, если атакующий в состоянии использовать знания, собранные в одной атаке, чтобы выполнить более сложную атаку позже, свидетельства от первого нападения могут быть ключом к объяснению того, как вторая атака было выполнена.
- **Хранение данных.** У большинства организаций есть политики хранения данных, которые определяют, сколько времени определенные типы данных должны храниться. Например, организация может определить, что электронные письма должны храниться в течение только 180 дней. Если образ диска содержит тысячи электронных писем, организация может хотеть, чтобы образ хранился не более, чем 180 дней, если это не абсолютно необходимо. Как обсуждено в Разделе 3.4.2, General Records Schedule (GRS) 24 определяет, что записи по обработке инцидента нужно хранить три года.
- **Стоимость.** Оригинальные аппаратные средства (например, жесткие диски скомпрометированной системы), которые сохранены как свидетельства, а также жесткие диски и съемные носители, которые используются, чтобы хранить образы дисков, обычно индивидуально

недороги. Однако, если организация хранит много таких компонентов в течение многих лет, стоимость может быть существенной. Организация также должна сохранить функциональные компьютеры, которые могут использовать хранимые аппаратные средства и носители информации.

3.5. Контрольный список обработки инцидента

Контрольный список в Таблице 3-6 представляет основные шаги, которые должны быть выполнены при обработке инцидента. Обратите внимание на то, что фактические выполняемые шаги могут измениться на основе типа инцидента и сущности отдельных инцидентов. Например, если обработчик точно знает, что произошло на основе анализа индикаторов (Шаг 1.1), то может быть не требуется выполнять Шаги 1.2 или 1.3 в дальнейшей работе по исследованию. Контрольный список предоставляет руководство обработчикам по основным шагам, которые должны быть выполнены; но он не диктует точную последовательность шагов, которые должны всегда выполняться.

Таблица 3-5. Контрольный список обработки инцидента

	Действие	Выполнение
	Обнаружение и анализ	
1.	Определите, произошел ли инцидент	
1.1	Проанализируйте предшественники и индикаторы	
1.2	Ищите корреляцию информации	
1.3	Выполните исследование (например, поисковые системы, база знаний)	
1.4	Как только обработчик полагает, что инцидент произошел, начните документировать расследование и собирать свидетельства	
2.	Определите приоритет обработки инцидента на основе соответствующих факторов (функциональное воздействие, информация воздействие, усилие по восстанавливаемости, и т.д.)	
3.	Сообщите об инциденте соответствующему внутреннему персоналу и внешним организациям	
	Сдерживание, уничтожение и восстановление	
4.	Получите, сохраните, обеспечьте безопасность и задокументируйте свидетельства	
5.	Обеспечьте сдерживание инцидента	
6.	Уничтожьте инцидент	
6.1	Определите и сократите все уязвимости, которые использовались	
6.2	Удалите вредоносное программное обеспечение, несоответствующие материалы и другие компоненты	
6.3	Если обнаружены другие затронутые хосты (например, новые вредоносные инфекции), повторите шаги Обнаружения и Анализа (1.1, 1.2), чтобы опознать все другие затронутые хосты, затем обеспечьте сдерживание (5) и уничтожьте (6) инцидент для них	
7.	Оправьтесь от инцидента	
7.1	Возвратите затронутые системы к состоянию оперативной готовности	
7.2	Подтвердите, что затронутые системы функционируют обычно	
7.3	Если необходимо, реализуйте дополнительный мониторинг, чтобы определить связанную работу будущего	
	Работа постинцидента	
8.	Создайте завершающий отчет	
9.	Проведите встречу по изучению уроков (обязательный для серьёзных инцидентов, опционально для остальных)	

3.6. Рекомендации

Ключевые рекомендации, представленные в этом разделе по обработке инцидентов, просуммированы ниже.

- **Приобретите инструменты и ресурсы, которые могут иметь значение во время обработки инцидента.** Команда будет более эффективна при обработке инцидентов, если ей будут доступны различные инструменты и ресурсы. Примеры включают списки контактов, программное обеспечение шифрования, сетевые графики, устройства резервного копирования, программное обеспечение для электронного расследования и списки портов.
- **Препятствуйте тому, чтобы инциденты произошли, гарантировав, что сети, системы и приложения достаточно безопасны.** Предотвращение инцидентов выгодно для организации, а также уменьшает рабочую нагрузку команды реагирования на инциденты. Выполнение периодических оценок степени риска и снижение определенного риска до допустимого уровня эффективны в сокращении количества инцидентов. Также очень важно освоение политики и процедур безопасности пользователями, персоналом ИТ и руководством.
- **Определяйте предшественники и индикаторы посредством сигналов, генерируемых несколькими типами программного обеспечения безопасности.** Системы обнаружения и предотвращения вторжений, антивирусное программное обеспечение и программное обеспечение проверки целостности файлов ценны для обнаружения признаков инцидентов. Каждый тип программного обеспечения может обнаружить инциденты, которые не могут другие типы программного обеспечения, таким образом, настоятельно рекомендуется использование нескольких типов программного обеспечения компьютерной безопасности. Также могут быть полезными сторонние сервисы мониторинга.
- **Установите механизмы для сообщения об инцидентах внешним сторонам.** Внешние стороны могут хотеть сообщать организации об инцидентах— например, они могут полагать, что один из пользователей организации атакует их. Организации должны опубликовать номер телефона и адрес электронной почты, которые внешние стороны могут использовать, чтобы сообщать о таких инцидентах.
- **Потребуйте базового уровня регистрации и аудита для всех систем и более высокого уровня для всех критических системах.** Журналы регистрации операционных систем, сервисов и приложений часто имеют значение во время анализа инцидента, особенно если был установлен аудит. Журналы регистрации могут предоставить информацию к каким учетным записям получили доступ и какие действия были выполнены.
- **Профилируйте сети и системы.** Профилирование измеряет особенности ожидаемых уровней активности так, чтобы изменения в текущих образцах могли быть более легко определены. Если процесс профилирования автоматизирован, отклонения от ожидаемых уровней активности можно обнаружить и сообщить администраторам быстрее, что приводит к более быстрому обнаружению инцидентов и эксплуатационных проблем.
- **Поймите нормальные поведения сетей, систем и приложений.** Члены команды, которые понимают нормальное поведение, должны быть в состоянии более легко определить неправильное поведение. Это знание лучше всего может быть получено, пересматривая записи и предупреждения системы безопасности в журнале; обработчики должны познакомиться с типичными данными и могут исследовать необычные записи, чтобы получить больше знаний.
- **Создайте политику хранения журналов.** Информация относительно инцидента может записываться в нескольких местах. Создание и проведение политики хранения журналов, которая определяет, сколько времени регистрируемые данные должны храниться, может быть чрезвычайно полезным для анализа, потому что более старые записи в журнале могут показать работу разведки или предыдущие случаи подобных нападений.
- **Выполните корреляцию событий.** Свидетельства инцидента могут храниться в нескольких журналах регистрации. Корреляция событий среди различных источников может быть неоценимой в сборе всей доступной информации для инцидента и утверждения, произошел ли инцидент.
- **Сохраняйте все часы хостов синхронизированными.** Если у устройств, сообщающих о событиях будут несоответствующие установки часов, корреляция событий будет более сложной. Несоответствия часов могут также вызвать проблемы с точки зрения доказательств.

- **Поддерживайте и используйте базу знаний информации.** Обработчикам при анализе инцидента срочно необходима справочная информация; центральная база знаний предоставляет непротиворечивый, поддерживаемый источник информации. База знаний должна включать общую информацию, такую как данные по предшественникам и индикаторам предыдущих инцидентов.
- **Начните записывать всю информацию, как только команда подозревает, что инцидент произошел.** Каждый шаг, от времени, обнаружения инцидента до его окончательного разрешения, должен быть задокументирован с добавлением метки времени. Эта информация может служить свидетельством в суде, действующем по нормам общего права, если предусмотрено законное судебное преследование. Запись выполненных шагов может также привести к более эффективной, систематизированной и меньше подверженной ошибкам обработке проблемы.
- **Защитите данные об инциденте.** Они часто содержат чувствительную информацию относительно таких вещей как уязвимости, нарушения защиты и пользователи, которые, возможно, выполняли несоответствующие действия. Команда должна гарантировать, что доступ к данным об инциденте правильно ограничен и логически и физически.
- **Расположите по приоритетам обработку инцидентов на основе соответствующих факторов.** Из-за ограничений ресурсов инциденты не должны обрабатываться по принципу «первым прибыл, первым обслужен». Вместо этого организации должны установить письменные руководства, которые определяют, как быстро команда должна ответить на инцидент и какие действия должны быть выполнены, на основе соответствующих факторов, таких как функциональное и информационное воздействие инцидента и вероятность восстановления от инцидента. Это экономит время для обработчиков инцидента и предоставляет обоснование руководству и владельцам систем для их действий. Организации должны также установить процесс эскалации для тех случаев, когда команда не отвечает на инцидент в течение определяемого времени.
- **Включите положения относительно отчетности об инцидентах в политику реагирования на инциденты организации.** Организации должны определить, о каких инцидентах нужно сообщать, когда о них нужно сообщать и кому. Стороны обычно включаемые: директор по информации, руководитель информационной безопасности, местный сотрудник по информационной безопасности, другие команды реагирования на инциденты в организации и владельцы систем.
- **Установите стратегии и процедуры сдерживания инцидентов.** Важно сдерживать инциденты быстро и эффективно, чтобы ограничить их влияние на деятельность. Организации должны определить приемлемые риски в сдерживании инцидентов и разработать соответствующие стратегии и процедуры. Стратегии сдерживания должны различаться на основе типа инцидента.
- **Выполните установленные процедуры для сбора и обработки свидетельств.** Команда должна точно задокументировать, как все свидетельства были сохранены. Свидетельства должны составляться в любом случае. Команда должна встретиться с юридическим персоналом и правоохранительными органами, чтобы обсудить обработку свидетельств, и затем разработать способы на основе этих обсуждений.
- **Соберите изменённые данные от систем как свидетельства.** Это включает списки сетевых соединений, процессов, сессий входа, открытых файлов, конфигураций сетевых интерфейсов и содержания памяти. Запуском тщательно выбранных команд из доверенного носителя информации можно собрать необходимую информацию, не повреждая свидетельства системы.
- **Получите образы систем на образы дисков для расследования, а не резервные копии файловой системы.** Образы дисков должны быть сделаны на очищенных, защищенных от записи или неперезаписываемых носителях информации. Этот процесс превосходит резервную копию файловой системы для назначения исследований и получения свидетельств. Образ также ценен в том, что намного более безопасно проанализировать образ, чем выполнить этот анализ на оригинальной системе, потому что анализ может непреднамеренно изменить оригинал.
- **Проведите встречи по изучению уроков после важных инцидентов.** Встречи по изучению уроков чрезвычайно полезны в мерах по повышению безопасности и самом процессе обработки инцидентов.

4. Координация и совместное пользование информацией

Сущность современных угроз и нападений делает для организаций более важным чем когда-либо сотрудничество во время реагирования на инциденты. Организации должны гарантировать, что они эффективно скоординировали свои части действий по реагированию на инциденты с соответствующими партнерами. Самый важный аспект координации реагирования на инциденты - совместное пользование информацией, когда различные организации обмениваются информацией по угрозам, атакам и уязвимостям друг с другом так, чтобы знание каждой организации принесло пользу другим. Совместное пользование информацией об инцидентах часто взаимовыгодно, потому что те же самые угрозы и атаки часто затрагивают одновременно многие организации.

Как упомянуто в Разделе 2, координирование и обмен информацией с партнерскими организациями могут усилить способность организации эффективно отвечать на ИТ инциденты. Например, если организация определяет некоторое поведение в своей сети, которое кажется подозрительным и посылает информацию о событии ряду доверенных партнеров, кто-то еще, возможно, уже видел в этой сети подобное поведение и будет в состоянии ответить дополнительными деталями о подозрительной активности, включая сигнатуры, другие индикаторы для поиска, или предложит восстановительные мероприятия. Сотрудничество с доверенным партнером может дать возможность организации ответить на инцидент более быстро и эффективно, чем когда организация действует в изоляции.

Это увеличение действенности стандартных технологий реагирования на инциденты не единственный стимул для координации между организациями и совместного пользования информацией. Другой стимул для совместного пользования информацией - возможность ответить на инциденты, используя технологии, которые могут быть не доступны отдельной организации, особенно если эта организация - малого и среднего размера. Например, у небольшой организации, которая определяет особенно сложный случай вредоносного программного обеспечения в её сети, может не быть внутренних ресурсов, чтобы полностью проанализировать вредоносное программное обеспечение и определить его воздействие на систему. В этом случае, организация в состоянии эффективно использовать доверенную сеть совместного пользования информацией, чтобы эффективно произвести анализ на стороне этого вредоносного программного обеспечения используя ресурсы третьей стороны, у которой есть адекватные технические возможности выполнить анализ вредоносности.

Эта часть документа обращает внимание на координацию и совместное пользование информацией. Раздел 4.1 представляет обзор координации при реагировании на инциденты и фокусируется на потребности в координации между организациями, чтобы подкрепить процессы реагирования на инциденты организации. Раздел 4.2 обсуждает технологии для совместного пользования информацией между организациями, и Раздел 4.3 исследует, как ограничить, какой информацией делиться или не делиться с другими организациями.

4.1. Координация

Как обсуждено в Разделе 2.3.4, организация, возможно, должна взаимодействовать с несколькими типами внешних организаций в ходе проведения работ реагирования на инциденты. Примеры этих организаций включают другие команды реагирования на инциденты, правоохранительные органы, поставщиков интернет-услуг и партнеров и клиентов. Команда реагирования на инциденты организации должна планировать свою координацию по инцидентам с этими сторонами, прежде чем инциденты произойдут, чтобы гарантировать, что все стороны знают свои роли и что установлены эффективные линии связи. Рисунок 4-1 даёт пример представления в организации выполнения координации в каждой фазе жизненного цикла реагирования на инциденты, подчеркивающий, что координация ценна всюду по жизненному циклу.

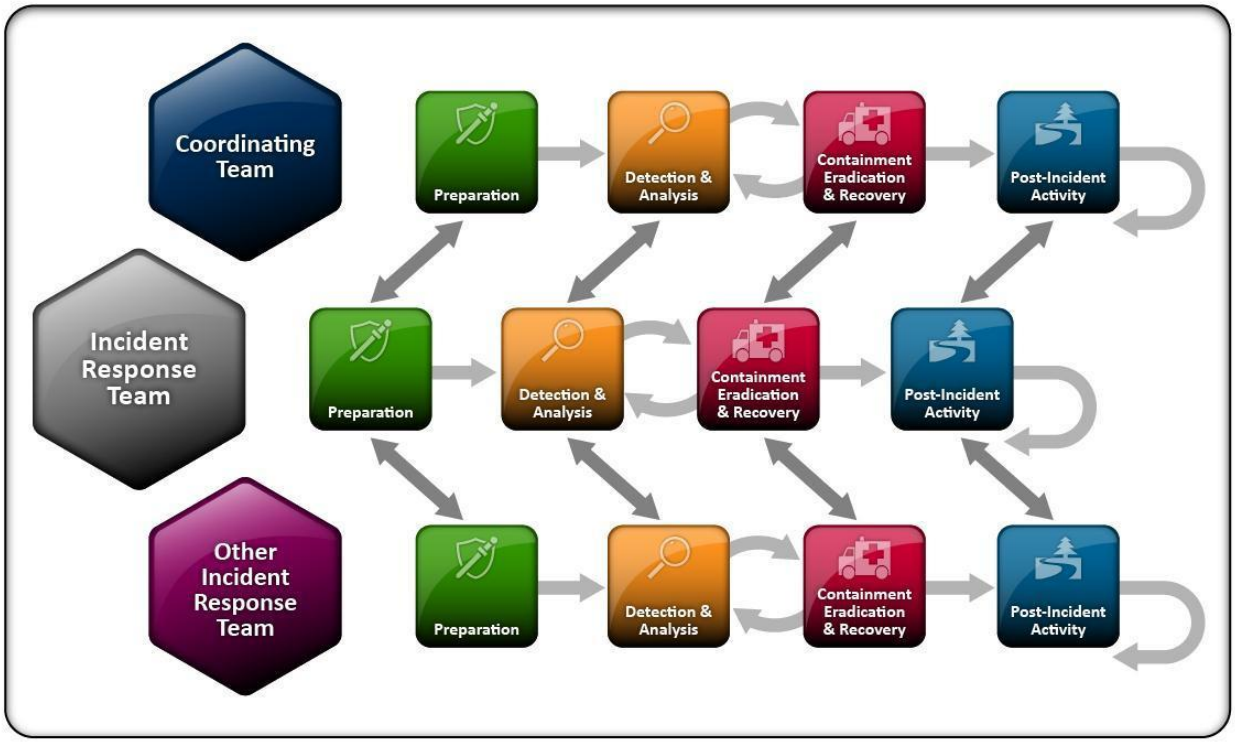

Рисунок 4-1. Координация реагирования на инциденты

4.1.1. Отношения координации

Команда реагирования на инциденты в организации может участвовать в различных типах соглашений координации, в зависимости от типа организации, с которой она координирует. Например, члены команды, ответственные за технические детали реагирования на инциденты, могут координировать с эксплуатационными коллегами в партнерских организациях, чтобы разделить стратегии смягчения атак, охватывающих различные организации. Альтернативно, во время того же самого инцидента, менеджер команды реагирования на инциденты может координировать с ISACs, чтобы удовлетворить необходимые требования к отчетности и обратиться за советом и дополнительными ресурсами для того, чтобы успешно ответить на инцидент. Таблица 4-1 предоставляет некоторые примеры отношений координации, которые могут существовать, при сотрудничестве с внешними организациями.

Таблица 4-1. Отношения координации

Категория	Определение	Общая информация
«Команда к» команде	Отношения от команды к команде существуют каждый раз, когда технические респонденты инцидента в различных организациях сотрудничают с их коллегами во время любой фазы жизненного цикла обработки инцидента. Организации, участвующие в этом типе отношений, обычно являются коллегами без любых полномочий друг к другу и принимают решение поделиться информацией, пулом ресурсов и знанием повторного использования, чтобы решить проблемы, общие для обеих команд.	Информация, наиболее часто передаваемая в отношении «команда к команде», тактическая и техническая (например, технические индикаторы компрометации, предлагаемые восстановительные мероприятия), но может также включать другие типы информации (планы, процедуры, извлеченные уроки), если проведена как часть фазы Подготовки.
«Команда к» координирующей команде	Отношения команда к координирующей команде существуют между командой реагирования на инциденты организации и отдельной организацией, которая действует как центральная точка для координируемого реагирования на инциденты и управления, такой как US - CERT или ISAC. Этот тип отношений может включать определенную степень требуемой отчётности от членских организаций координационному органу, а также ожидание, что команда координирования распространит своевременную и полезную информацию к участвующим членским организациям.	Команды и координирующие команды часто делятся тактической, технической информацией, а также информацией относительно угроз, уязвимостей и рисков с сообществом, объединяемом командой координирования. Координирующей команде, возможно, также понадобится конкретная информация о воздействии инцидентов, чтобы помочь принимать решения о том, где сосредоточить ее ресурсы и внимание.
Координирующая команда к координирующей команде	Отношения между различными координирующими командами, такими как US-CERT и ISACs существуют, чтобы делиться информацией, касающейся сквозных инцидентов, которые могут затронуть различные сообщества. Координирующие команды действуют от имени своих соответствующих организаций - членов сообщества, чтобы делиться информацией по характеру и области сквозных инцидентов и повторяемыми стратегиями смягчения чтобы помочь в общей реакции сообществ.	Тип информации, обмениваемой координирующими командами с их коллегами, обычно состоит из периодических резюме во время деятельности в «устойчивом состоянии», дополненных обменом тактическими, техническими деталями, планами реагирования и информацией по оценке воздействия или степени риска во время координируемых действий реагирования на инциденты.

Организации могут искать стимулы, чтобы строить отношения, необходимые для координации. Хорошие области, чтобы начать строить сообщество, включают промышленный сектор, к которому организация принадлежит, и географический регион, где организация действует. Команда реагирования на инциденты организации может попытаться сформировать отношения с другими командами (на уровне от команды к команде) в его собственном промышленном секторе и регионе, или присоединиться к устоявшимся органам в промышленном секторе, которые уже способствуют совместному пользованию информацией. Другое рассмотрение для построения отношений состоит в том, что некоторые отношения обязательные, а другие добровольные; например, отношения команды к координирующей команде часто обязательны, в то время как отношения от команды к команде обычно добровольны. Организации рассматривают добровольные отношения потому, что они удовлетворяют взаимные личные интересы. Обязательные отношения обычно определяются регулятивным органом в промышленности или другой сущностью.

4.1.2 Соглашения по обмену и требования к отчетности

Организации, пытающиеся поделиться информацией с внешними организациями, должны консультироваться с их юридическим департаментом прежде, чем предпринять любые усилия по координации. Могут существовать контракты или другие соглашения, которые должны быть учтены, прежде чем произойдут обсуждения. Пример - соглашение о неразглашении (NDA), чтобы защитить конфиденциальность наиболее чувствительной информации организации. Организации должны также рассмотреть любые существующие требования по отчётности, такие как обмен информацией об инцидентах с ISAC или информирование об инцидентах высокоуровневого CIRT.

4.2. Технологии совместного пользования информацией

Совместное пользование информацией - основной элемент предоставления координации между организациями. Даже самые маленькие организации должны быть в состоянии поделиться информацией об инцидентах с коллегами и партнерами, чтобы эффективно иметь дело со многими инцидентами. Организации должны осуществлять такое совместное пользование информацией всюду по жизненному циклу реагирования на инциденты и не ждать, пока инцидент не будет полностью решен прежде, чем поделиться его деталями с другими. Раздел 4.3 обсуждает типы информации об инцидентах, которыми организации могут хотеть или не хотеть делиться с другими.

Этот раздел сосредотачивается на технологиях по совместному пользованию информацией. Раздел 4.2.1 рассматривает оперативные методы, в то время как Раздел 4.2.2 исследует частично автоматизированные методы. Наконец, Раздел 4.2.3 обсуждает рассмотрения безопасности, связанные с совместным пользованием информацией.

4.2.1. Оперативные методы

Большая часть совместного пользования информацией об инцидентах традиционно происходит посредством оперативных методов, таких как электронная почта, клиенты мгновенного обмена сообщениями и телефон. Оперативные механизмы совместного пользования информацией обычно полагаются на связи отдельного сотрудника с сотрудниками в командах реагирования на инциденты партнерских организаций.

Сотрудник использует эти связи, чтобы вручную поделиться информацией с коллегами и координироваться с ними, чтобы строить стратегии ответа на инцидент. В зависимости от размера организации, эти оперативные технологии могут быть самым рентабельным способом поделиться информацией с партнерскими организациями. Однако, вследствие неформализованной сущности оперативного совместного пользования информацией, невозможно гарантировать, что процессы совместного пользования информацией будут всегда работать. Например, если особенно хорошо связанный сотрудник уходит из команды реагирования на инциденты, то команда может временно потерять большинство каналов совместного пользования информацией, на которые она полагается, чтобы эффективно координировать с внешними организациями.

Оперативные методы совместного пользования информацией также в основном не стандартизированы с точки зрения того, какая информация сообщается и как это взаимодействие происходит. Из-за отсутствия стандартизации они имеют тенденцию требовать ручного вмешательства и являются более ресурсоемкими для обработки, чем альтернативные, частично автоматизированные методы. Каждый раз, когда возможно, организация должна пытаться формализовать свои стратегии совместного пользования информацией через формальные соглашения с партнерскими организациями и технические механизмы, которые помогут частично автоматизировать обмен информацией.

4.2.2. Частично автоматизированные методы

Организации должны попытаться автоматизировать как можно больше процессов совместного пользования информацией, чтобы сделать координацию между организациями рациональной и экономически эффективной. В действительности будет невозможно полностью автоматизировать обмен всей информацией об инциденте, и при этом это не желательно вследствие безопасности и доверительного рассмотрения. Организации должны пытаться достигнуть баланса в объединении автоматизации совместного пользования информацией с процессами ориентированными на человека для управления информационными потоками.

Когда проектируются решения по автоматизации совместного пользования информацией, организации должны сначала рассмотреть, какими типами информации они будут обмениваться с партнерами. Организация может хотеть строить формальный словарь данных, перечисляющий все сущности и отношения между сущностями, которыми они хотят обмениваться. Как только организации поймут типы информации, которой они будут делится, необходимо построить формальные, машинно-обрабатываемые модели, чтобы охватить эту информацию. Везде, где возможно, организация должна использовать существующие стандарты обмена данными для

представления информации, которой необходимо обмениваться.[47] Выбирая модели обмена данными, организация должна работать со своими партнерскими организациями, чтобы гарантировать, что выбранные стандарты совместимы с системами реагирования на инциденты партнерской организации. Выбирая существующие модели обмена данными, организации могут предпочесть выбирать многоуровневые модели, которые моделируют различные аспекты области реагирования на инциденты и затем усиливать эти модели модульным способом, передавая только информацию, необходимую в конкретном моменте принятия решения в жизненном цикле. Приложение E предоставляет неисчерпывающий список существующих стандартов, определяющих модели обмена данными, которые применимы к области реагирования на инциденты.

В дополнение к выбору моделей обмена данными для обмена информацией об инцидентах, организация должна также работать со своими партнерскими организациями, чтобы договориться о технических транспортных механизмах для того, чтобы давать возможность обмену информацией произойти автоматизированным способом. Эти транспортные механизмы включают, как минимум, транспортный протокол для обмена информацией, архитектурную модель для связи с информационным ресурсом, и применимые порты и доменные имена для доступа к информационному ресурсу в конкретной организации. Например, группа партнерских организаций может решить обмениваться информацией об инцидентах с использованием Representational State Transfer (REST) архитектуры, чтобы обмениваться IODEF/Real-Time Inter-Network Defense (RID) данными по Hypertext Transfer Protocol Secure (HTTPS) по порту 4590 из конкретного доменного имени в демилитаризованной зоне каждой организации.

4.2.3. Рассмотрения безопасности

Есть несколько рассмотрений безопасности, которые команды реагирования на инциденты должны рассмотреть, планируя их совместное пользование информацией. Одним является возможность определить, кто может видеть какую часть информации об инциденте (например, защита чувствительной информации). Может также быть необходимо выполнить очистку данных, чтобы удалить чувствительные части данных из информации об инциденте, не нарушая информацию относительно предшественников, индикаторов и другой технической информации. Посмотрите Раздел 4.3 для получения дополнительной информации о разделении совместного пользования информацией. Команда реагирования на инциденты должна также гарантировать, что приняты необходимые меры, чтобы защитить информацию, передаваемую командам других организаций.

Есть также много юридических вопросов, которые нужно рассмотреть относительно совместного использования данными. Посмотрите Раздел 4.1.2 для получения дополнительной информации.

4.3. Разделённое совместное пользование информацией

Организации должны уравновесить пользу от совместного пользования информацией с недостатками предоставления чувствительной информации, идеально делиться с соответствующими сторонами необходимой и только необходимой информацией. Организации могут думать о своей информации об инцидентах как о состоящей из двух типов: влияющей на деятельность и технической. Информацией, влияющей на деятельность, часто делятся в контексте отношений «команды к координирующей команде», как определено в Разделе 4.1.1, в то время как технической информацией часто делятся во всех трех типах отношений координации. Этот раздел обсуждает оба типа информации и предоставляет рекомендации для выполнения разделённого совместного пользования информацией.

4.3.1. Информация, влияющая на деятельность

Информация, влияющая на деятельность, включает информацию о том, как инцидент затрагивает организацию с точки зрения воздействия на предназначение, финансы и т.п. Такая информация, по крайней мере на итоговом уровне, часто сообщается высокоуровневым координирующим командам

[47] Согласно Национальному закону о Передаче и продвижении технологий (NTTAA), “все Федеральные агентства и департаменты должны использовать технические стандарты, которые разработаны или приняты добровольными организациями по стандартизации”. Дополнительную информацию см. в http://standards.gov/nttaa.cfm.

реагирования на инциденты, чтобы сообщить оценку ущерба, нанесенного инцидентом. Координирующим командам, возможно, понадобится эта информация о воздействии, чтобы принять решения относительно степени помощи, предоставляемой сообщившей организации. Координирующая команда может также использовать эту информацию, чтобы принять решения относительно того, как конкретный инцидент затронет другие организации в сообществе, которое она представляет.

Координирующая команда может потребовать, чтобы членские организации сообщали относительно информации влияния на бизнес определенного уровня. Например, координирующая команда может потребовать, чтобы членская организация сообщала информацию о воздействии с использованием категорий, определенных в Разделе 3.2.6. В этом случае для гипотетического инцидента организация сообщала бы, что оказывается *среднее* функциональное воздействие, *нет* информационного воздействия, и потребуется *расширенное* время восстановления. Эта информация высокого уровня предупредила бы координирующую команду, что членской организации требуется некоторый уровень дополнительных ресурсов для восстановления после инцидента. Координирующая команда могла бы тогда дополнительно связаться с членской организацией, чтобы определить, сколько требуется ресурсов, а также тип ресурсов на основе технической информации, предоставленной об инциденте.

Информация влияния на деятельность полезна для сообщения только для организаций, у которых есть некоторый интерес в гарантировании предназначения организации, испытывающей инцидент. В большинстве случаев команды реагирования на инциденты должны избегать делиться информацией влияния на деятельность с внешними организациями, если нет ясного ценностного предложения или формальных требований к отчетности. Делясь информацией с коллегами и партнерскими организациями, команды реагирования на инциденты должны сосредоточиться на обмене технической информацией, как определено в Разделе 4.3.2.

4.3.2. Техническая информация

Есть много различных типов технических индикаторов, показывающих возникновение инцидента в организации. Эти индикаторы происходят из разнообразия технической информации, связанной с инцидентами, такой как имена хоста и IP адреса атакующего хоста, образцы вредоносного программного обеспечения, предшественников и индикаторов подобных инцидентов и типов уязвимостей, используемых в инциденте. Раздел 3.2.2 предоставляет обзор того, как организации должны собирать и использовать эти индикаторы, чтобы помочь определить инцидент, который происходит. Кроме того, Раздел 3.2.3 предоставляет список общих источников данных об индикаторах инцидента.

В то время как организации получают пользу от сбора их внутренних индикаторов, они могут получить дополнительную пользу от анализа индикаторов, полученных от партнерских организаций и выдачи внутренних индикаторов для внешнего анализа и использования. Если организация получает внешние данные об индикаторах, относящихся к инциденту, которые они не видели, они могут использовать эти данные об индикаторах, чтобы определить инцидент, когда он начнет происходить. Точно так же организация может использовать внешние данные об индикаторах, чтобы обнаружить происходящий инцидент, о котором она не знала вследствие отсутствия внутренних ресурсов, чтобы собрать конкретные данные об индикаторах. Организации могут также извлечь выгоду из обмена их внутренними данными об индикаторах с внешними организациями. Например, если они делятся технической информацией, относящейся к испытываемому им инциденту, партнерская организация может ответить предложением стратегии устранения обрабатываемого инцидента.

Организации должны делиться как можно большим количеством этой информации; однако, могут быть резоны безопасности и ответственности, почему организация не хотела бы показывать детали используемых уязвимостей. Внешними индикаторами, такими как общие характеристики атак и идентификаторы атакующих хостов, обычно безопасно делить с другими. Организации должны рассмотреть, какими типами технической информации нужно или не нужно делиться с различными сторонами, и затем пытаться делиться как можно большим количеством соответствующей информации с другими организациями.

Технические данные об индикаторах полезны, когда они позволяют организации определять фактический инцидент. Однако не все данные об индикаторах, полученные от внешних источников, будут относиться к организации, получающей их. В некоторых случаях, эти внешние данные генерируют ложные срабатывания в сети получающей организации и могут заставить потратить ресурсы на несуществующие проблемы.

У организаций, участвующих в совместном пользовании информацией об инцидентах, должен быть персонал, квалифицированный в получении технической информации об индикаторах от сообществ по обмену информацией и распространения этой информации всюду по предприятию, предпочтительно автоматизированным способом. Организации должны также попытаться гарантировать, чтобы они обмениваются только индикаторами, по которым у них есть относительно высокий уровень доверия, что они показывают актуальный инцидент.

4.4. Рекомендации

Ключевые рекомендации, представленные в этом разделе для обработки инцидентов, получены в итоге ниже.

- **Планируйте координацию по инцидентам с третьими сторонами до того, как инциденты произойдут.** Примеры третьих сторон включают другие команды реагирования на инциденты, правоохранительные органы, поставщиков интернет-услуг и коллег и клиентов. Это планирование помогает гарантировать, что все стороны знают свои роли и что установлены эффективные линии взаимодействия.
- **Консультируйтесь с юридическим департаментом прежде, чем предпринять любые усилия по координации.** Могут иметься другие контракты или соглашения, которые должны быть учтены, прежде чем произойдёт обсуждение.
- **Выполняйте совместное пользование информацией об инцидентах всюду по жизненному циклу реагирования на инциденты.** Совместное пользование информацией - основной элемент предоставления координации между организациями. Организации не должны ждать, пока инцидент будет полностью разрешен прежде, чем поделиться его деталями с другими.
- **Пытайтесь автоматизировать как можно большую часть процесса совместного пользования информацией.** Это делает координацию между организациями рациональной и экономически эффективной. Организации должны пытаться достигнуть баланса автоматизации совместного пользования информацией с ориентированными на человека процессами управления информационными потоками.
- **Уравновесьте пользу от совместного пользования информацией с недостатками от обмена чувствительной информацией.** Идеально организации должны делиться необходимой и только необходимой информацией с соответствующими сторонами. Информацией влияния на деятельность часто делятся в отношениях «команды к координирующей команде», в то время как технической информацией часто делятся во всех типах отношений координации. Делясь информацией с партнёрами и партнерскими организациями, команды реагирования на инциденты должны сосредоточиться на обмене технической информацией.
- **Используйте совместно как можно больше соответствующей информации об инцидентах с другими организациями.** Организации должны рассмотреть, какими типами технической информации нужно или не нужно делиться с различными сторонами. Например, внешними индикаторами, такими как общие характеристики атак и идентификаторы атакующих хостов, обычно безопасно делиться с другими, но могут быть и причины безопасности и ответственности, почему организация не хотела бы показывать детали используемых уязвимостей.

Приложение A — сценарии обработки инцидентов

Сценарии обработки инцидентов предоставляют недорогой и эффективный способ получить навыки реагирования на инциденты и отождествить потенциальные проблемы с процессами реагирования на инциденты. Команде реагирования на инциденты или членам команды дают сценарий и список связанных вопросов. Команда обсуждает каждый вопрос и определяет наиболее вероятный ответ. Цель состоит в том, чтобы определить то, что команда действительно сделала бы и сравнить это с политиками, процедурами и обычно рекомендуемыми методами, чтобы определить несоответствия или недостатки. Например, ответ на один вопрос может указать, что реакция была бы замедленна, потому что команда испытывает недостаток в части программного обеспечения или потому что другая команда не оказывает поддержку вне рабочего времени.

Упомянутые ниже вопросы применимы почти к любому сценарию. Каждый вопрос сопровожден указанием на соответствующий раздел (разделы) документа. После вопросов находятся сценарии, каждый из которых сопровожден дополнительными конкретными вопросами об инцидентах. Организации очень поощрены приспособить эти вопросы и сценарии для использования в их собственных упражнениях по реагированию на инциденты.[48]

A1 Вопросы сценария

Подготовка:

1. Организация полагала бы, что эта активность является инцидентом? Если так, какую из политик организации нарушает эта активность? *(Раздел 2.1)*
2. Какие меры существуют, чтобы попытаться препятствовать тому, чтобы этот тип инцидента произошел или ограничить его воздействие? *(Раздел 3.1.2)*

Обнаружение и анализ:

1. Какие предшественники инцидента, если таковые имеются, организация могла бы обнаружить? Какие предшественники заставили бы организацию принимать меры, прежде чем инцидент произойдёт? *(Разделы 3.2.2, 3.2.3)*
2. Какие индикаторы инцидента организация могла бы обнаружить? Какие индикаторы заставили бы кого-то думать, что инцидент, возможно, произошел? *(Разделы 3.2.2, 3.2.3)*
3. Какие дополнительные инструменты могли бы быть необходимы, чтобы обнаружить этот конкретный инцидент? *(Раздел 3.2.3)*
4. Как команда реагирования на инциденты проанализировала бы и определила бы этот инцидент? Какой персонал был бы включен в процесс анализа и проверки? *(Раздел 3.2.4)*
5. Каким людям и группам в организации команда сообщила бы об инциденте? *(Раздел 3.2.7)*
6. Как команда расположила бы по приоритетам обработку этого инцидента? *(Раздел 3.2.6)*

Сдерживание, уничтожение и восстановление:

1. Какую стратегию организация должна взять, чтобы сдержать инцидент? Почему эта стратегия предпочтительнее других? *(Раздел 3.3.1)*
2. Что могло произойти, если бы инцидент не был сдержан? *(Раздел 3.3.1)*
3. Какие дополнительные инструменты могли бы быть необходимы, чтобы ответить на этот конкретный инцидент? *(Разделы 3.3.1, 3.3.4)*
4. Какой персонал был бы включен в процессы сдерживания, уничтожения и/или восстановления? *(Разделы 3.3.1, 3.3.4)*
5. Какие источники свидетельств, если таковые имеются, организация должна получить? Как свидетельства были бы получены? Где они были бы сохранены? Сколько времени они должны храниться? *(Разделы 3.2.5, 3.3.2, 3.4.3)*

[48] Для получения дополнительной информации об упражнениях посмотрите NIST SP 800-84, *Руководство по проверке, подготовке и обучению по Программе по планированию и возможностям ИТ*, которая доступна по http://csrc.nist.gov/publications/PubsSPs.html#800-84.

Работа постинцидента:

6. Кто присутствовал бы на встрече по изучению уроков относительно этого инцидента? *(Раздел 3.4.1)*
7. Что могло бы быть сделано, чтобы препятствовать тому, чтобы подобные инциденты произошли в будущем? *(Раздел 3.1.2)*
8. Что могло бы быть сделано, чтобы улучшить обнаружение подобных инцидентов? *(Раздел 3.1.2)*

Общие вопросы:

1. Сколько членов команды реагирования на инциденты участвовало бы в обработке этого инцидента? *(Раздел 2.4.3)*
2. Помимо команды реагирования на инциденты, какие группы в организации были бы включены в обработку этого инцидента? *(Раздел 2.4.4)*
3. Каким третьим сторонам команда сообщила бы об инциденте? Когда должно происходить каждое сообщение? Как должно быть сделано каждое сообщение? Какую информацию Вы сообщили бы или не сообщили бы и почему?
4. Какие другие связи с третьими сторонами могут производиться? *(Раздел 2.3.2)*
5. Какие инструменты и ресурсы команда использовала бы в обработке этого инцидента? *(Раздел 3.1.1)*
6. Какие аспекты обработки были бы другими, если бы инцидент произошел в другой день и время (в рабочее и в не рабочее время)? *(Раздел 2.4.2)*
7. Какие аспекты обработки были бы различны, если бы инцидент произошел в различном физическом местоположении (внутри или во вне)? *(Раздел 2.4.2)*

A2 Сценарии

Сценарий 1: Отказ в обслуживании (DoS) сервера системы доменных имен (DNS)

В субботу днем внешние пользователи начинают иметь проблемы получения доступа к общим вебсайтам организации. За следующий час проблема ухудшается до состояния, когда почти каждая попытка доступа терпит неудачу. Между тем член сетевого персонала организации реагирует на тревоги от граничного интернет-маршрутизатора и решает, что пропускная способность интернета организации потребляется необычно большим объемом пакетов User Datagram Protocol (UDP) к и от обоих общих серверов DNS организации. Анализ трафика показывает, что серверы DNS получают большие объемы запросов от одного внешнего IP адреса. Кроме того, все запросы DNS от этого адреса исходят из того же самого исходного порта.

Следующее - дополнительные вопросы для этого сценария:

1. С кем организация должна связаться относительно внешнего рассматриваемого IP адреса?
2. Предположим, что после того, как начальные меры по сдерживанию были применены, сетевые администраторы обнаружили, что девять внутренних хостов также делали попытку тех же самых необычных запросов к серверу DNS. Как это затронуло бы обработку этого инцидента?
3. Предположим, что были опознаны два из девяти внутренних хостов, разъединенных от сети прежде чем их системные владельцы были определены. Как должны быть опознаны их системные владельцы?

Сценарий 2: Заражение червём и агентом Distributed Denial of Service (DDoS)

Во вторник утром выпущен новый червь; он распространяется через съемные носители и он может скопировать себя, чтобы открыть совместное использование Windows. Когда червь заражает хост, он устанавливает агента DDoS.

Организация уже подверглась широко распространенным инфекциям, прежде чем антивирусные сигнатуры стали доступными спустя несколько часов после того, как червь начал распространяться.

Следующее - дополнительные вопросы для этого сценария:

1. Как команда реагирования на инциденты опознала бы все зараженные хосты?
2. Как организация попыталась бы препятствовать тому, чтобы червь проник в организацию, прежде чем антивирусные сигнатуры были бы выпущены?
3. Как организация попыталась бы препятствовать тому, чтобы червь был распространен зараженными хостами, прежде чем антивирусные сигнатуры были бы выпущены?
4. Организация попыталась бы исправить все уязвимые машины? Если так, как это было бы сделано?
5. Как бы изменилась обработка этого инцидента, если бы зараженные хосты, которые приняли агента DDoS, были бы сконфигурированы, чтобы атаковать вебсайт другой организации следующим утром?
6. Как бы изменилась обработка этого инцидента, если бы один или несколько зараженных хостов содержали чувствительную персональную идентификационную информацию относительно сотрудников организации?
7. Как команда реагирования на инциденты информировала бы пользователей организации о статусе инцидента?
8. Какие дополнительные меры команда приняла бы для хостов, которые в настоящее время не связаны с сетью (например, сотрудники в отпуске, удаленные сотрудники, которые иногда соединяются)?

Сценарий 3: Украденные документы

В понедельник утром юридический департамент организации получает звонок из федерального Бюро расследований (ФБР) относительно некоторой подозрительной активности, включающей системы организации. Позже в тот же день агент ФБР встречается с членами руководства и юридического департамента, чтобы обсудить активность. ФБР исследовало активность, включающую публикацию чувствительных правительственных документов, и некоторые документы по сообщениям принадлежат организации. Источник просит помощи организации, и руководство просит помощи команды реагирования на инциденты в получении необходимых свидетельств чтобы определить, являются ли эти документы легальными или нет и как они, возможно, утекли.

Следующее - дополнительные вопросы для этого сценария:

1. Из каких источников команда реагирования на инциденты могли бы собрать свидетельства?
2. Что команда сделала бы, чтобы сохранить расследование конфиденциальным?
3. Как бы изменилась обработка этого инцидента, если бы команда опознала внутренний хост, ответственный за утечку?
4. Как бы изменилась обработка этого инцидента, если бы команда сочла что руткит установлен на внутреннем хосте, ответственном за утечку?

Сценарий 4: Скомпрометированный сервер базы данных

Во вторник ночью администратор базы данных выполняет во вне рабочее время некоторую поддержку на нескольких производственных серверах баз данных. Администратор замечает некоторые незнакомые и необычные имена каталогов на одном из серверов. После рассмотрения списков директорий и просмотра некоторых файлов, администратор приходит к заключению, что сервер подвергся нападению и вызывает команду реагирования на инциденты для помощи. Расследование команды определяет, что атакующий успешно получил корневой доступ к серверу шесть недель назад.

Следующее - дополнительные вопросы для этого сценария:

1. Какие источники команда могла бы использовать, чтобы определить, когда компрометация произошла?

2. Как бы изменилась обработка этого инцидента, если бы команда нашла, что на сервере базы данных был запущен анализатор пакетов и перехвачены пароли из сети?
3. Как бы изменилась обработка этого инцидента, если бы команда нашла, что на сервере был запущен процесс, который копирует базу данных, содержащую чувствительную информацию потребителей (включая персональную идентификационную информацию) каждую ночь, и передаёт её внешнему адресу?
4. Как бы изменилась обработка этого инцидента, если бы команда обнаружила руткит на сервере?

Сценарий 5: Неизвестная экс-фильтрация

В воскресенье ночью один из сетевых датчиков обнаружения вторжений организации сигнализирует об аномальной внешней сетевой активности, включающей передачу больших файлов. Аналитик вторжений рассматривает сигналы; кажется, что тысячи .RAR файлов копируются из внутреннего хоста к внешнему хосту, и внешний хост расположен в другой стране. Аналитик связывается с командой реагирования на инциденты для того, чтобы она могла исследовать активность далее. Команда неспособна видеть то, что содержат .RAR файлы, потому что их содержание зашифровано. Анализ внутреннего хоста, содержащего .RAR файлы, показывает признаки установки бота.

Следующее - дополнительные вопросы для этого сценария:

1. Как бы команда определила то, что, скорее всего, находится внутри .RAR файлов? Какие другие команды могли бы помочь команде реагирования на инциденты?
2. Если команда реагирования на инциденты определила, что начальная компрометация была выполнена через карту беспроводной сети во внутреннем хосте, как команда далее исследует эту активность?
3. Если команда реагирования на инциденты определила, что для того, чтобы получить чувствительные файлы из других хостов в предприятии, использовался внутренний хост, как команда далее исследует эту активность?

Сценарий 6: Несанкционированный доступ к записям платежной ведомости

В среду вечером команда физической безопасности организации получает звонок от администратора по зарплате, которая видела, что неизвестный человек покинул её пост, бежал по коридору и вышел из здания. Администратор оставляла свою рабочую станцию открытой и без присмотра в течение только нескольких минут. Кроме того, программа платежной ведомости находилась в главном меню, как это было, когда она оставила его, но администратор замечает, что мышь, кажется, была перемещена. Команду реагирования на инциденты попросили получить свидетельства, связанные с инцидентом и определить, какие действия были выполнены.

Следующее - дополнительные вопросы для этого сценария:

1. Как команда определила бы, какие действия были выполнены?
2. Как бы изменилась обработка этого инцидента, если бы администратор по зарплате признал человека, покинувшего её пост, как бывшего сотрудника департамента платежных ведомостей?
3. Как бы изменилась обработка этого инцидента, если бы у команды была причина полагать, что человек был действующим сотрудником?
4. Как бы изменилась обработка этого инцидента, если бы команда физической безопасности определила, что человек использовал методы социальной инженерии, чтобы получить физический доступ к зданию?
5. Как бы изменилась обработка этого инцидента, если бы журналы регистрации с предыдущей недели показали необычно большое количество неудавшихся попыток удаленного входа в систему, используя идентификатор пользователя администратора по зарплате?

6. Как бы изменилась обработка этого инцидента, если бы команда реагирования на инциденты обнаружила, что двумя неделями ранее на компьютере был установлен регистратор нажатия клавиш?

Сценарий 7: Исчезнувший хост

В четверг днем сетевой датчик обнаружения вторжений делает запись активности по сканированию уязвимостей, направленной на внутренние хосты, которая генерируется внутренним IP адресом. Поскольку аналитик обнаружения вторжений не знает о какой-либо санкционированной, запланированной активности по сканированию уязвимостей, он сообщает об активности команде реагирования на инциденты. Когда команда начинает анализ, она обнаруживает, что активность остановилась и что больше нет хоста, использующего IP адрес.

Следующее - дополнительные вопросы для этого сценария:

1. Какие источники данных могли бы содержать информацию относительно идентификации хоста, сканировавшего уязвимости?
2. Как команда определила бы, кто выполнял сканирование уязвимостей?
3. Как бы изменилась обработка этого инцидента, если бы сканирование уязвимостей было направлено на самые критически хосты организации?
4. Как бы изменилась обработка этого инцидента, если бы сканирование уязвимостей было бы направлено на внешние хосты?
5. Как бы изменилась обработка этого инцидента, если бы внутренний IP адрес был связан с гостевой беспроводной сетью организации?
6. Как бы изменилась обработка этого инцидента, если бы персонал физической безопасности обнаружил, что кто-то проник на объект за полчаса до того, как произошло сканирование уязвимостей?

Сценарий 8: Компрометация дистанционного доступа

В субботу ночью сетевое программное обеспечение обнаружения вторжений делает запись входящей связи, происходящей из списка наблюдения IP адресов. Аналитик обнаружения вторжений решает, что связь устанавливается с сервером VPN организации и связывается с командой реагирования на инциденты. Команда рассматривает журналы обнаружения вторжений, межсетевого экрана и сервера VPN и определяет идентификатор пользователя, который был аутентифицирован для сессии и имя пользователя, связанного с идентификатором пользователя.

Следующее - дополнительные вопросы для этого сценария:

1. Как команда должна затем поступить (например, позвонить пользователю домой, отключить идентификатор пользователя, разъединить сессию VPN)? Почему этот шаг должен быть выполнен первым? Какой шаг должен быть выполнен вторым?
2. Как бы изменилась обработка этого инцидента, если бы внешний адрес IP принадлежал открытому прокси?
3. Как бы изменилась обработка этого инцидента, если бы ID использовался, чтобы инициировать VPN соединения от нескольких внешних IP адресов без ведома пользователя?
4. Предположим, что компьютер опознанного пользователя скомпрометирован игрой, содержащей Троянский конь, которая была загружена членом семьи. Как это затронуло бы команду анализа инцидента? Как это затронуло бы сбор и обработку свидетельств? Что команда должна сделать с точки зрения удаления инцидента из компьютера пользователя?
5. Предположим, что пользователь установил антивирусное программное обеспечение и определил, что троянский конь включал регистратор нажатия клавиш. Как это затронуло бы обработку инцидента? Как это затронуло бы обработку инцидента, если бы пользователь был системным администратором? Как это затронуло бы обработку инцидента, если бы пользователь был высокопоставленное лицо в организации?

Сценарий 9: Анонимная угроза

В четверг днем команда физической безопасности организации получает звонок от менеджера по ИТ, сообщающей, что два из ее сотрудников только что получили анонимные угрозы от систем организации. На основе расследования команда физической безопасности полагает, что к угрозам нужно отнестись серьезно и уведомляют об угрозах соответствующие внутренние команды, включая команду реагирования на инциденты.

Следующее - дополнительные вопросы для этого сценария:

1. Что команда реагирования на инциденты должна делать по-другому в разных случаях, в ответ на уведомление об угрозах?
2. Какие усиленные меры обеспечения физической безопасности в ответ на воздействие могут иметься у команды реагирования на инциденты?

Сценарий 10: Одноранговый совместный доступ к файлам

Организация запрещает использование одноранговых сервисов совместного доступа к файлам. Сетевым датчикам обнаружения вторжений организации имеют сигнатуры, которые могут обнаружить использование нескольких популярных одноранговых сервисов совместного доступа к файлам. В понедельник вечером аналитик обнаружения вторжений замечает, что несколько сигналов совместного доступа к файлам имели место в течение прошлых трех часов, все содержали тот же самый внутренний IP адрес.

1. Какие факторы должны использоваться, чтобы расположить по приоритетам обработку этого инцидента (например, допустимое содержание файлов, которые совместно используются)?
2. Какие рассмотрения приватности могут повлиять на обработку этого инцидента?
3. Как бы изменилась обработка этого инцидента, если бы компьютер, выполняющий одноранговый совместный доступ к файлам, содержал также чувствительную персональную идентификационную информацию?

Сценарий 11: Неизвестная точка доступа

В понедельник утром справочная служба организации получает звонки от трех пользователей на том же самом этаже здания, которые заявляют, что у них есть проблемы с их беспроводным доступом. Сетевой администратор, которого просят помочь в решении проблемы, приносит ноутбук с беспроводным доступом на этаж пользователей. Рассматривая свою конфигурацию беспроводной сети, он замечает, что есть новая точка доступа, перечисленная как являющаяся доступной. Он сверяется со своими коллегами по команде и решает, что эта точка доступа не была развернута его командой, так, что это была наиболее вероятно точка доступа нарушителя, которая была установлена без разрешения.

1. Каков должен быть первый главный шаг в обработке этого инцидента (например, физически найти точку доступа нарушителя, логически подключиться к точке доступа)?
2. Какой самый быстрый путь, чтобы определить местонахождение точки доступа? Какой самый скрытный путь, чтобы определить местонахождение точки доступа?
3. Как бы изменилась обработка этого инцидента, если бы точка доступа была развернута третьей стороной (например, подрядчиком), временно работающим в офисе организации?
4. Как бы изменилась обработка этого инцидента, если бы аналитик обнаружения вторжений сообщил бы о признаках подозрительной активности, включающей некоторые рабочие станции на том же самом этаже здания?
5. Как бы изменилась обработка этого инцидента, если бы точка доступа была удалена, в то время как команда пыталась физически определить её местонахождение?

Приложение B — Элементы данных, связанные с инцидентом

Организации должны определить стандартный набор связанных с инцидентом элементов данных, которые будут собираться для каждого инцидента. Это усилие не только облегчит более эффективную и непротиворечивую обработку инцидента, но также и поможет организации учесть применимые требования отчетности об инцидентах. Организация должна определить ряд основных элементов (например, имя информатора об инциденте, номер телефона и местоположение), которые должны быть собраны, когда сообщают об инциденте, и дополнительный набор элементов, которые должны быть собраны обработчиками инцидента во время их реагирования. Два набора элементов были бы основой для базы данных отчетности об инцидентах, ранее обсужденной в Разделе 3.2.5. Списки ниже предоставляют предложения того, какая информация должна собираться для инцидентов и не предназначены, чтобы быть всесторонними. Каждая организация должна создать свой собственный список элементов на основе нескольких факторов, включая модель и структуру её команды реагирования на инциденты и её определение понятия «инцидент».

B.1 Элементы исходных данных

- Контактная информация для информатора об инциденте и обработчика
  - Имя
  - Роль
  - Организационная единица (например, агентство, департамент, отдел, команда) и принадлежность
  - Адрес электронной почты
  - Номер телефона
  - Местоположение (например, почтовый адрес, номер офисной комнаты)
- Детали инцидента
  - Дата/метки времени изменения статуса (включая часовой пояс): когда инцидент начался, когда инцидент был определён/обнаружен, когда об инциденте сообщили, когда инцидент был решен/завершён и т.д.
  - Физическое местоположение инцидента (например, город, штат)
  - Текущий статус инцидента (например, продолжающаяся атака)
  - Источник/причина инцидента (если известны), включая имена хостов и IP адреса
  - Описание инцидента (например, как он был обнаружен, что произошло),
  - Описание затронутых ресурсов (например, сети, хосты, приложения, данные), включая имена хостов систем, IP адреса и функции
  - Если известно, категория инцидента, векторы атак, связанных с инцидентом, и индикаторы, относящиеся к инциденту (образцы трафика, ключи реестра, и т.д.)
  - Приоритеты факторов (функциональное воздействие, информационное воздействие, восстанавливаемость и т.д.)
  - Смягчающие факторы (например, украденный ноутбук, содержащий чувствительные данные, использовал полное дисковое шифрование),
  - Выполненные действия по реагированию (например, отключение хоста, разъединение хоста от сети)
  - Контакты с другими организациями (например, программный вендор)
- Замечаниями общего порядка

B.2 Элементы данных обработчика инцидента

- Текущий статус реагирования на инциденты
- Резюме инцидента
- Действия по обработке инцидента
  - – Журнал регистрации мер, принятых всеми обработчиками
  - – Контактная информация для всех участвующих сторон
  - – Список собранных свидетельств
- Комментарии обработчика инцидента
- Причина инцидента (например, неправильно сконфигурированное приложение, не обновлённый хост),
- Стоимость инцидента
- Влияние инцидента на деятельность [49]

[49] Влияние инцидента на деятельность может быть описано или эффектом инцидента (например, департамент бухгалтерского учета неспособен выполнить задачи в течение двух дней) или категорией воздействия на основе стоимости (например, «серьёзный» инцидент имеет стоимость более чем 100 000$).

Приложение C — Глоссарий

Отобранные термины, использованные в публикации, определены ниже.

Принятие за основу (Baselining): Мониторинг ресурсов по определению таких образцов типичного использования, чтобы могли быть обнаружены значительные отклонения.

Инцидент компьютерной безопасности (Computer Security Incident): см. «инцидент».

Команда реагирования на инциденты компьютерной безопасности (Computer Security Incident Response Team (CSIRT)): возможность, установленная в целях помощи в реагировании на инциденты, связанные с компьютерной безопасностью; также называется Команда реагирования на компьютерные инциденты (Computer Incident Response Team (CIRT)) или CIRC (Computer Incident Response Center, Computer Incident Response Capability) Центр реагирования на компьютерные инциденты, Возможность реагирования на компьютерные инциденты.

Событие (Event): Любая заметная ситуация в сети или системе.

Ложный сигнал (False Positive): сигнал, который неправильно указывает, что злонамеренная работа происходит.

Инцидент (Incident): нарушение или непосредственная угроза нарушения политик компьютерной безопасности, политик допустимого использования или методов стандартной защиты.

Обработка инцидента (Incident Handling): смягчение нарушений политик безопасности и рекомендуемых методов.

Реагирование на инциденты (Incident Response): См., “обработка инцидента”.

Индикатор (Indicator): знак того, что инцидент, возможно, произошел или может произойти в настоящее время.

Система обнаружения и предотвращения вторжений (Intrusion Detection and Prevention System (IDPS)): Программное обеспечение, которое автоматизирует процесс мониторинга событий, происходящих в компьютерной системе или сети и анализирующее их по признакам возможных инцидентов и пытающееся остановить обнаруженные возможные инциденты.

Вредоносное программное обеспечение (Malware): вирус, червь, троянский конь или другая основанная на коде злонамеренная сущность, которая успешно заражает хост.

Предшественник (Precursor): знак того, что атакующий, возможно, готов вызвать инцидент.

Профилирование (Profiling): Измерение характеристик ожидаемой активности так, чтобы изменения к ним могли быть более легко определены.

Сигнатура (Signature): распознаваемый, различающийся образец, связанный с атакой, такой как двоичная строка у вируса или определенный набора нажатий клавиш, используемый для получения несанкционированного доступа к системе.

Социальная техника (Social Engineering): попытка обмануть кого-то в раскрывающей информации (например, пароль), которая может использоваться, чтобы атаковать системы или сети.

Угроза (Threat): потенциальный источник неблагоприятного события.

Уязвимость (Vulnerability): слабость в системе, приложении или сети, которая является субъектом использования или неправильного употребления.

Приложение D — Акронимы

Отобранные акронимы, используемые в публикации, определены ниже.

CCIPS Секция компьютерных преступлений и интеллектуальной собственности
CERIAS Центр образования и исследований в Информационном доверии и Безопасности
CERT®/CC Координационный центр CERT®
CIO Директор по информации
CIRC Центр реагирования на компьютерные инциденты
CIRC Возможность реагирования на компьютерные инциденты
CIRT Команда реагирования на компьютерные инциденты
CISO Директор по информационной безопасности
CSIRC Возможность реагирования на инциденты компьютерной безопасности
CSIRT Команда реагирования на инциденты компьютерной безопасности
DDoS Распределенный отказ в обслуживании
DHS Министерство национальной безопасности
DNS Система доменных имен
DoS Отказ в обслуживании
FAQ Часто задаваемые вопросы
FBI Федеральное бюро расследований
FIPS Федеральный стандарт обработки информации
FIRST Форум команд реагирования на инциденты и безопасности
FISMA Закон об управлении безопасностью федеральной информации
GAO Офис общей ответственности
GFIRST Правительственный форум команд реагирования на инциденты и безопасности
GRS Порядок ведения общей документации
HTTP Гипертекстовый протокол передачи
IANA Орган назначения интернет номеров
IDPS Система обнаружения и предотвращения вторжений
IETF Специальная комиссия по интернет-разработкам
IP Интернет-протокол
IR Межведомственный отчет
IRC Чат ретранслируемый в интернете
ISAC Центр совместного пользования и анализа информации
ISP Поставщик интернет-услуг
ИТ Информационная технология
ITL Лаборатория информационных технологий
MAC Контроль доступа к носителю информации
MOU Меморандум о взаимопонимании
MSSP Поставщик услуг по управлению безопасностью
NAT Преобразование сетевого адреса
NDA Соглашение о неразглашении
NIST Национальный институт стандартов и технологий
NSRL Национальная библиотека руководств по программному обеспечению
NTP Протокол сетевого времени
NVD Национальная база данных уязвимостей
OIG Офис Генерального Инспектора
OMB Министерство управления и бюджета

ОС Операционная система

ПИИ Персональная идентификационная информация

PIN Персональный идентификационный номер

POC Точка контакта

REN-ISAC Центр исследований и образования по совместному использованию и анализу сетевой информации

RFC Запрос комментариев

RID Межсетевая оборона в реальном времени

SIEM Управление информацией и событиями по безопасности

SLA Соглашение о сервисном обслуживании

SOP Стандартный режим работы

SP Специальная публикация

TCP Протокол TCP

TCP/IP Протокол TCP / интернет-Протокол

TERENA Трансъевропейская ассоциация исследований и образования по сетям

UDP Пользовательский дейтаграммный протокол

URL унифицированный указатель ресурсов

US-CERT Команда готовности к компьютерным чрезвычайным ситуациям Соединенных Штатов

VPN Виртуальная частная сеть

Приложение E — ресурсы

Списки ниже предоставляют примеры ресурсов, которые могут быть полезными в установлении и поддержании возможностей реагирования на инциденты.

Организации реагирования на инциденты

Организация	URL
Рабочая группа по антифишингу (APWG)	http://www.antiphishing.org/
Секция компьютерных преступлений и интеллектуальной собственности (CCIPS), Министерство юстиции США	http://www.cybercrime.gov/
Координационный центр CERT®, Carnegie Mellon University (CERT®/CC)	http://www.cert.org/
Европейское агентство по сетям и информационной безопасности (ENISA)	http://www.enisa.europa.eu/activities/cert
Форум команд реагирования на инциденты и безопасности (FIRST)	http://www.first.org/
Правительственный форум команд реагирования на инциденты и безопасности (GFIRST)	http://www.us-cert.gov/federal/gfirst.html
Ассоциация расследований преступлений в области высоких технологий(HTCIA)	http://www.htcia.org/
InfraGard	http://www.infragard.net/
Internet Storm Center (ISC)	http://isc.sans.edu/
Национальный консилиум по ISACs	http://www.isaccouncil.org/
Команда готовности к компьютерным чрезвычайным ситуациям Соединенных Штатов (US-CERT)	http://www.us-cert.gov/

Публикации NIST

Имя ресурса	URL
NIST SP пересмотр 800-53 3, Рекомендуемые меры безопасности для федеральных информационных систем и организаций	http://csrc.nist.gov/publications/PubsSPs.html#800-53
NIST SP 800-83, Руководство по предотвращению и обработке инцидентов с вредоносным кодом	http://csrc.nist.gov/publications/PubsSPs.html#800-83
NIST SP 800-84, Руководство по программам проверки, обучения и подготовки для ИТ планов и возможностей	http://csrc.nist.gov/publications/PubsSPs.html#800-84
NIST SP 800-86, Руководство к интеграции технологий расследования в реагирование на инциденты	http://csrc.nist.gov/publications/PubsSPs.html#800-86
NIST SP 800-92, Руководство по управлению журналами регистрации компьютерной безопасности	http://csrc.nist.gov/publications/PubsSPs.html#800-92
NIST SP 800-94, p\Руководство по системам обнаружения и предотвращения вторжений (IDPS)	http://csrc.nist.gov/publications/PubsSPs.html#800-94

NIST SP 800-115, Техническое руководство по тестированию и оценке информационной безопасности	http://csrc.nist.gov/publications/PubsSPs.html#800-115
NIST SP 800-128, Руководство по управлению конфигурацией информационных систем, направленному на безопасность	http://csrc.nist.gov/publications/PubsSPs.html#800-128

Спецификации обмена данными, применимыми к обработке инцидента

Название	Описание	Дополнительная информация
AI	Идентификация активов	http://csrc.nist.gov/publications/ PubsNISTIRs.html#NIST-IR-7693
ARF	Формат результатов активов	http://csrc.nist.gov/publications/ PubsNISTIRs.html#NIST-IR-7694
CAPEC	Общая нумерация и классификация образца атак	http://capec.mitre.org/
CCE	Общее перечисление конфигураций	http://cce.mitre.org/
CEE	Общее представление событий	http://cee.mitre.org/
CPE	Общая нумерация платформ	http://cpe.mitre.org/
CVE	Общие уязвимости и воздействия	http://cve.mitre.org/
CVSS	Система общего обозначения уязвимостей	http://www.first.org/cvss/cvss-guide
CWE	Общая нумерация слабостей	http://cwe.mitre.org/
CybOX	Cyber Observable eXpression	http://cybox.mitre.org/
MAEC	Нумерация и характеристика вредоносного кода	http://maec.mitre.org/
OCIL	Интерактивный язык открытых контрольных списков	http://csrc.nist.gov/publications/ PubsNISTIRs.html#NIST-IR-7692
OVAL	Открытый язык по оценке уязвимостей	http://oval.mitre.org/
RFC 4765	Формат обмена сообщениями по обнаружению вторжений (IDMEF)	http://www.ietf.org/rfc/rfc4765.txt
RFC 5070	Формат обмен описаниями объекта инцидента (IODEF)	http://www.ietf.org/rfc/rfc5070.txt
RFC 5901	Расширения к IODEF для сообщений по фишингу	http://www.ietf.org/rfc/rfc5901.txt
RFC 5941	Обмен данныи о мошенничестве	http://www.ietf.org/rfc/rfc5941.txt
RFC 6545	Real-time Inter-network Defense (RID)	http://www.ietf.org/rfc/rfc6545.txt
RFC 6546	Передача в реальном времени через HTTP/TLS сообщений о межсетевой защите (RID)	http://www.ietf.org/rfc/rfc6546.txt
SCAP	Протокол автоматизации контента безопасности	http://csrc.nist.gov/publications/PubsSPs.html #SP-800-126% преподобного 202
XCCDF	Расширяемый формат описания контрольных списков конфигурации	http://csrc.nist.gov/publications/ PubsNISTIRs.html#NIST-IR-7275-r4

Приложение F — часто задаваемые вопросы

У пользователей, системных администраторов, сотрудников информационной безопасности и других лиц в организациях могут быть вопросы относительно реагирования на инциденты. Ниже приведены часто задаваемые вопросы (FAQ). Организации поощрены адаптировать эти часто задаваемые вопросы и сделать их доступными для их сообщества пользователей.

1. Что такое инцидент?

В целом инцидент - нарушение политик компьютерной безопасности, политик допустимого использования или стандартных методов компьютерной безопасности. Примеры инцидентов:

- Атакующий подаёт команду ботнету о посылке большого количества требований о соединении к одному из веб-серверов организации, заставляя его потерпеть крах.
- Пользователи обмануты при открытии «квартального отчета», посланного по электронной почте, который является на самом деле вредоносным программным обеспечением; запускаемый инструмент заразил их компьютеры и установил связи с внешним хостом.
- Преступник получает несанкционированный доступ к чувствительным данным и угрожает опубликовать детали, если организация не заплатит определяемую денежную сумму.
- Пользователь предоставляет незаконные копии программного обеспечения другим через одноранговые сервисы совместного доступа к файлам.

2. Что такое обработка инцидента?

Обработка инцидента - процесс обнаружения и анализа инцидентов и ограничения эффекта инцидентов. Например, если атакующий проникает в систему через Интернет, процесс обработки инцидента должен обнаружить нарушение защиты. Обработчики должны проанализировать данные и определить, насколько серьезно нападение. Будет определён приоритет инцидента и обработчики инцидента примут меры, чтобы гарантировать, что прогресс инцидента остановлен и что затронутые системы возвращаются к нормальному функционированию как можно скорее.

3. Что такое реагирование на инциденты?

Термины “обработка инцидента” и «реагирование на инциденты» синонимичны в этом документе.[50]

4. Что такое команда реагирования на инциденты?

Команда реагирования на инциденты (также известная как Computer Security Incident Response Team [CSIRT]) ответственна за предоставление услуг реагирования на инциденты для части или всей организации. Команда получает информацию относительно возможных инцидентов, исследует их и принимает меры, чтобы гарантировать, что ущерб, нанесенный инцидентами, минимизирован.

5. Какие услуги команда реагирования на инциденты предоставляет?

Конкретные услуги, которые обычно предоставляет команда реагирования на инциденты, значительно различаются среди организаций. Помимо осуществления обработки инцидента, большинство команд также принимает на себя ответственность за мониторинг и управление системой обнаружения вторжений. Команда может также доводить оповещения относительно новых угроз и обучить пользователей и персонал ИТ по их ролям в предотвращении и обработке инцидента.

6. Кому нужно сообщать об инцидентах?

Организации должны установить ясные точки контакта (POC) для сообщения об инцидентах внутри организации. Некоторые организации структурируют свою способность реагирования на инциденты так, чтобы обо всех инцидентах сообщили непосредственно команде реагирования на инциденты, тогда как другие будут использовать существующую структуры поддержки, такую как справочная служба ИТ, для начальной POC. Организация должна определить, какие третьи стороны, такие как другие команды реагирования на инциденты, должны быть проинформированы о некоторых инцидентах. Федеральные агентства должны в соответствии с законом, сообщать обо всех

[50] Определения “обработки инцидента” и «реагирования на инциденты» значительно различаются. Например, CERT®/CC использует термин “обработка инцидента”, чтобы определять полный процесс обнаружения инцидента, сообщения, анализа и реакции, тогда как «реагирование на инциденты» относится только к сдерживанию инцидента, восстановлению и уведомлению о других. См. http://www.cert.org/csirts/csirt_faq.html для получения дополнительной информации.

инцидентах Компьютерной команде Соединенных Штатов готовности к чрезвычайной ситуации (US - CERT).). Все организации поощрены сообщать об инцидентах своим соответствующим Командам реагирования на инциденты компьютерной безопасности (CSIRTs). Если у организации нет своей собственной CSIRT для связи, она может сообщать об инцидентах другим организациям, включая Центры совместного пользования и анализа информации (ISACs)**.**

7. Как сообщают об инцидентах?

У большинства организаций есть много способов для сообщения об инциденте. Разные способы сообщения, могут быть предпочтительными в зависимости от навыков человека, сообщающего об активности, экстренности инцидента и чувствительности инцидента. Должен быть установлен номер телефона, чтобы сообщать о чрезвычайных ситуациях. Адрес электронной почты может быть предусмотрен для неформального сообщения об инцидентах, а веб-форма может быть полезной для формальной отчетности об инцидентах. Чувствительная информация может быть предоставлена команде при помощи открытого ключа, изданного командой, чтобы зашифровать материал.

8. Какая информация должна быть предоставлена при сообщении об инциденте?

Чем более подробна информация, тем лучше. Например, если рабочая станция, возможно, была заражена вредоносным программным обеспечением, сообщение о происшествии должно включать как можно большее количество следующих данных:

- Имя пользователя, идентификатор пользователя и контактная информация (например, номер телефона, адрес электронной почты)
- Местоположение рабочей станции, номер модели, порядковый номер, имя и IP адрес хоста
- Дата и время, когда инцидент произошел
- Пошаговое объяснение того, что произошло, включая то, что было сделано с рабочей станцией после инфекции. Это объяснение должно быть детализировано, включая точную формулировку сообщений, таких как показанные вредоносным программным обеспечением или сигналами антивирусного программного обеспечения.

9. Как быстро команда реагирования на инциденты отвечает на сообщение о инциденте?

Время отклика зависит от нескольких факторов, таких как тип инцидента, критичность ресурсов и данных, которые затронуты, серьезность инцидента, существующие Соглашения об уровне сервиса (SLA) для затронутых ресурсов, время и день недели и другие инциденты, которые обрабатывает команда. Обычно самый высокий приоритет обработки относится к инцидентам, которые, вероятно, нанесут наибольший ущерб организации или другим организациям.

10. Какое лицо должно контактировать по инциденту с правоохранительными органами?

Связь с правоохранительными органами должна быть начата членами команды реагирования на инциденты, директором по информации (CIO) или другим назначенным сотрудником — пользователи, системные администраторы, владельцы систем и другие стороны контактировать не должны.

11. Что должен сделать тот, кто обнаруживает, что система подверглась нападению?

Человек должен немедленно прекратить использовать систему и связаться с командой реагирования на инциденты. Человек, возможно, должен помочь в начальной обработке инцидента — например, физически контролируя систему, пока обработчики инцидента не прибыли, чтобы защитить свидетельства в системе.

12. Что должен сделать тот, с кем связывается пресса относительно инцидента?

Человек может ответить на вопросы прессы в соответствии с политикой организации относительно инцидентов и внешних сторон. Если человек не уполномочен представлять организацию с точки зрения обсуждения инцидента, человек не должен комментировать относительно инцидента, кроме как направить посетителя в офис связей с общественностью организации. Это позволит офису связей с общественностью предоставлять точную и непротиворечивую информацию средствам информации и обществу.

G приложения — Шаги кризисной обработки

Это - список главных шагов, которые должны быть выполнены, когда технический профессионал полагает, что произошел серьезный инцидент, и организация не имеет в наличии возможности реагирования на инциденты. Это служит основной справкой о том, что делать тому, кто столкнулся с кризисом и не имеет времени, чтобы прочитать весь этот документ.

1. **Зарегистрируйте все.** Это усилие включает каждое действие, которое выполнено, каждую часть свидетельств и каждый разговор с пользователями, владельцами систем и другими лицами относительно инцидента.
2. **Найдите коллегу, который может предоставить помощь.** Обработка инцидента будет намного легче, если два или больше человека будут сотрудничать. Например, один человек может выполнять действия в то время как другие документировать их.
3. **Проанализируйте свидетельства, чтобы подтвердить, что инцидент произошел.** Выполните, по мере необходимости, дополнительные исследования (например, интернет-поисковых систем, программной документации), чтобы лучше понять свидетельства. Обратитесь к другим техническим профессионалам в организации для дополнительной помощи.
4. **Уведомьте соответствующих людей в организации**. Это должно включать директора по информации (CIO), руководителя информационной безопасности и менеджера по объектовой защите. Будьте осторожны, обсуждая детали инцидента с другими; говорите только с людьми, которым необходимо это знать и используйте коммуникационные механизмы, которые достаточно безопасны. (Если атакующий ставил под угрозу почтовые сервисы, не посылайте электронные письма об инциденте.)
5. **Уведомьте US – CERT и/или другие внешние организации** для помощи в обработке инцидента.
6. **Остановите инцидент, если он всё ещё происходит.** Наиболее распространенный способ сделать это - разъединить затронутые системы от сети. В некоторых случаях конфигурации межсетевого экрана и маршрутизатора, возможно, должны быть изменены, чтобы остановить сетевой трафик, который является частью инцидента, такого как нападение типа отказ в обслуживании (DoS).
7. **Предохраните свидетельства от инцидента.** Сделайте резервные копии (предпочтительно резервные копии образа диска, а не резервные копии файловой системы) затронутых систем. Сделайте копии файлов журналов, которые содержат свидетельства, связанные с инцидентом.
8. **Удалите все результаты инцидента.** Это усилие включает вредоносные инфекции, несоответствующие материалы (например, пиратское программное обеспечение), файлы троянского коня и любые другие изменения, внесенные в системы инцидентами. Если система полностью ставилась под угрозу, переустановите её с нуля или восстановите её из известной хорошей резервной копии.
9. **Определите и сократите все уязвимости, которые использовались.** Инцидент, возможно, произошел, использовав в своих интересах уязвимости в операционных системах или приложениях. Очень важно определить такие уязвимости и устранить или иначе сократить их так, чтобы инцидент не повторился.
10. **Подтвердите, что функционирование вернулось к нормальному.** Удостоверьтесь, что данные, приложения и другие сервисы, затронутые инцидентом, были возвращены к нормальному функционированию.
11. **Создайте итоговый отчет.** Этот отчет должен детализировать процесс обработки инцидента. Он также должно предоставить резюме того, что произошло и как формализованная способность реагирования на инциденты поможет более быстро справляться с ситуацией, снижать риск и ограничивать ущерб.