Network Working Group
Request for Comments: 2350
BCP: 21
Category: Best Current Practice

N. Brownlee
The University of Auckland
E. Guttman
Sun Microsystems

June 1998

Ожидания сообщества по поводу реакции на компьютерные инциденты

Expectations for Computer Security Incident Response

Статус документа

Этот документ относится к категории обмена опытом (Internet Best Current Practices) среди членов сообщества Internet и служит приглашением к дискуссии в целях дальнейшего совершенствования. Документ можно распространять без ограничений.

Авторские права

Copyright (C) The Internet Society (1998). All Rights Reserved.

Тезисы

Цель этого документа состоит в том, чтобы выразить ожидания сообщества Internet от групп CSIRT[1]. Невозможно определить набор требований, применимых ко всем таким группам, но вполне возможно и полезно описать общий круг проблем и вопросов, которые беспокоят сообщество в части компьютерной безопасности.

Клиенты CSIRT хотят и имеют законные права полностью понимать правила и процедуры, установленные их группой CSIRT. Единственным способом обеспечить такое понимание является предоставление детальной информации, которую клиенты могут рассмотреть, в формате шаблона, заполняемого CSIRT. В документе приводится схема такого шаблона и пример его заполнения.

Оглавление

[1]Computer Security Incident Response Team - группа реагирования на инциденты, связанные с компьютерной безопасностью.

1 Введение

Рабочая группа GRIP была сформирована для создания документа, описывающего ожидания сообщества от групп CSIRT. Хотя потребность в таком документе испытывают все члены сообщества Internet, описанные ожидания должны соответствовать и представлениям более ограниченных групп.

В прошлом приходилось неоднократно сталкиваться с ошибочными ожиданиями по поводу групп CSIRT. Целью настоящего документа является создание основы для представления важных (в контексте реакции на инциденты) тем, которые беспокоят сообщество.

Прежде, чем продолжить, остановимся на толковании термина Computer Security Incident Response Team. В настоящем документе термин CSIRT обозначает группу, которая выполняет, координирует и поддерживает операции по реагированию на инциденты, связанные с безопасностью, в которые вовлечены сайты определенного круга клиентов (более полное определение приведено в Приложении A). Любая группа, называющая себя CSIRT для определенной клиентуры, должна, следовательно, реагировать на сообщения о связанных с безопасностью инцидентах и угрозы «своей» клиентуре в интересах соответствующей группы.

Поскольку жизненно важно понимание каждым членом сообщества того, что он может ожидать от своей команды, CSIRT следует четко указывать, кто входит в команду, и описывать предлагаемые сообществу услуги. Кроме того, каждой CSIRT следует публиковать свои правила и рабочие процедуры. Клиенты должны понимать, что они могут ждать в результате использования услуг команды. Это также требует от команды информации о том как и где она публикует данные об инцидентах.

Данный документ детализирует шаблон, который может применяться CSIRT для коммуникаций со своими клиентами. Клиенты должны понимать, что они могут воспользоваться услугами, указанными CSIRT в заполненном шаблоне.

Следует подчеркнуть, что без активного участия клиентов эффективность CSIRT может существенно снизиться. По крайней мере клиенты должны знать, что им следует сообщать об инцидентах, а так же понимать, когда и как это следует делать.

Многие инциденты в сфере безопасности инициируются из-за пределов локального сообщества и происходят внутри сайта, а иные могут исходить из локального сообщества и воздействовать на внешние хосты и пользователей. Следовательно, зачастую обработка инцидентов будет вовлекать множество сайтов и в ней может участвовать множество CSIRT. Разрешение таких инцидентов потребует взаимодействия между сайтами и командами CSIRT, а также между разными CSIRT.

Сообществу клиентов нужно точно знать, как их CSIRT будет работать с другими CSIRT и организациями за пределами сообщества, а также понимать, какая информация при этом может передаваться.

Оставшаяся часть этого документа посвящена темам и вопросам, которые CSIRT должна осветить для своих клиентов. Однако это не является попыткой дать «правильный» ответ на все вопросы. Обсуждается, скорее, значение каждой темы или аспекта.

В разделе 2 приведен обзор трех основных направлений — публикация данных об инцидентах, связи с другими группами реагирования и необходимость защиты коммуникаций. В разделе 3 подробно рассматриваются все типы информации, которую сообщество должно знать применительно к командам реагирования на инциденты.

Для простоты использования эти темы представлены в виде шаблонов, приведенных в Приложении D. Заполненные шаблоны клиенты могут использовать для получения информации о своих CSIRT.

Члены рабочей группы искренне надеются, что приведенные здесь разъяснения помогут повысить уровень понимания между CSIRT и их клиентами.

2 Контекст

Для взаимодействия между группой реагирования на инциденты и сообществом ее клиентов нужно сначала обеспечить понимание этим сообществом правил и процедур работы группы реагирования. Во-вторых, поскольку при обработке инцидентов группы часто взаимодействуют друг с другом, сообщество должно понимать отношения своей группы реагирования с другими группами. При взаимодействии могут использоваться существующие открытые инфраструктуры и сообщество должно знать, насколько защищены такие коммуникации. Каждый из этих аспектов будет подробно рассмотрен в трех следующих параграфах.

2.1 Публикация правил и процедур CSIRT

Каждому клиенту, имеющему доступ к CSIRT, следует как можно больше узнать об услугах команды и взаимодействии с ней до появления реальной необходимости в таком взаимодействии.

Четкое изложение правил и процедур CSIRT поможет клиентам понять, как лучше сообщать об инцидентах и какой помощи можно ждать при их возникновении. Поможет ли CSIRT в разрешении инцидента? Будет ли команда оказывать помощью в предотвращении инцидентов впредь? Четкое понимание, особенно в части возможных ограничений в предлагаемых услугах CSIRT, будет упрощать взаимодействие и повышать его эффективность.

Существует множество разных CSIRT – одни имеют очень широкий круг клиентов (например, CERT Coordination Center), другие работают со сравнительно узким кругом (например, DFN-CERT, CIAC), есть также группы, работающие только с ограниченным кругом (например, коммерческие или корпоративные CSIRT). Независимо от типа группы, ее клиенты должны знать принятые командой правила и процедуры. Следовательно, группа реакции на отклики должна публиковать соответствующую информацию для своих клиентов.

CSIRT следует предоставлять всю необходимую информацию о своих правилах и процедурах в подходящей для клиентов форме. Важно понимать, что не все правила и процедуры следует публиковать в открытом доступе. Например, нет необходимости понимать внутренние механизмы взаимодействия в команде для работы с ней, при информировании об инцидентах или получении рекомендаций об анализе или защите систем.

В прошлом некоторые группы реагирования предоставляли своего рода схемы работы (Operational Framework), другие - списки ответов на наиболее распространенные вопросы (FAQ[1]), а кто-то писал статьи для распространения среди пользователей или публикации в новостных изданиях.

Рекомендуется каждой CSIRT публиковать свои руководства и процедуры на информационном сервере компании (например, WWW). Это обеспечит простоту доступа для клиентов, хотя и не решит полностью проблемы поиска CSIRT в «ближайшем окружении».

Предполагается, что заполнение приведенных шаблонов CSIRT позволит упростить поиск информации о CSIRT с помощью современных поисковых машин, поскольку эти шаблоны включают базовые сведения о команде и информацию о контактах.

Будет весьма полезно иметь централизованный репозиторий, на котором хранятся все заполненные шаблоны CSIRT. В настоящее время такого репозитория не существует, но в будущем ситуация может измениться.

Независимо от источника информации читатель заполненного шаблона должен проверить его аутентичность. Для этого настоятельно рекомендуется сопровождать такие документы цифровыми подписями. Это позволит пользователям убедиться в том, что шаблон действительно опубликован CSIRT и не является подделкой. В данном документе предполагается знакомство читателей с использованием цифровых подписей и проверкой аутентичности документов.

2.2 Отношения между разными CSIRT

В некоторых случаях CSIRT могут эффективно работать самостоятельно, контактирую со своими клиентами. Однако в современных международных сетях это стало значительно сложнее, поскольку во многих случаях инциденты, обрабатываемые командой, будут включать стороны, не являющиеся клиентами данной CSIRT. Следовательно, команде потребуется взаимодействие с другими CSIRT и сайтами, не являющимися их клиентами.

Сообщество клиентов должно понимать природу такого взаимодействия и возможность раскрытия при этом некоторых важных для конкретного клиента сведений.

Взаимодействие между CSIRT может включать консультации, обмен опытом решения проблем, а также совместные действия по обработке инцидента, затрагивающего клиентов нескольких CSIRT.

Для организации контактов в поддержку таких взаимодействий команда CSIRT должна принять решение о возможных соглашениях между сторонами в части обмена информацией и также раскрытия самого факта сотрудничества.

Следует отличать метить различие между случаями, когда CSIRT заключают соглашение о совместной работе и обмене информацией и ситуациями, где CSIRT (или иная организация) просто обращается к другой CSIRT за помощью или советом.

Хотя организация таких отношений очень важна и воздействует на возможности CSIRT по поддержке своих клиентов, принятие решения о сотрудничестве и его деталях является делом самой команды. Рекомендации в части принятия таких решений выходят за рамки данного документа. Тем не менее, та же информация, которая позволяет клиентам представить ожидания в плане обмена информацией группами реагирования с другими сторонами, поможет разобраться с целями и услугами конкретной CSIRT при первых контактах.

2.3 Организация защищенных коммуникаций

После того, как одна сторона решила поделиться информацией с другой или две стороны согласовали между собой совместное использование информации или кооперацию (для работы по инцидентам в сфере компьютерной безопасности), всем участникам процесса следует организовать защищенные каналы связи. В этом контексте «защита» относится к обмену информацией и не включает вопросов корректности использования информации.

Целями защиты коммуникаций служат:

- конфиденциальность:

  Может ли кто-то чужой получить доступ к информации?

- целостность:

  Может ли кто-то чужой изменить информацию?

- аутентификация:

  Общаюсь ли я с «нужным» человеком?

Очень просто отправить обманное сообщение по электронной почте и достаточно просто представиться другим человеком при телефонном разговоре. Криптографические методы (например, PGP[2] или PEM[3]) могут обеспечить эффективную защиту электронной почты. Имеется также оборудование для защиты телефонных разговоров. Однако до применения таких механизмов обе стороны должны организовать соответствующую инфраструктуру. Наиболее важным элементом такой подготовки является обеспечение аутентичности криптографических ключей, используемых для защиты коммуникаций:

- Открытые (Public) ключи (для методов типа PGP и PEM). Поскольку открытый ключ можно сделать доступным через Internet, его следует аутентифицировать до использования. PGP работает на основе «паутины доверия» (Web of Trust), где пользователи подписывают ключи других пользователей. PEM использует иерархическую модель, где ключи пользователей подписываются удостоверяющими центрами.

- Секретные ключи (для методов типа DES и PGP/традиционное шифрование). Поскольку ключ должен быть известен обеим сторонам, требуется организовать обмен ключами до организации защищенного канала.

[1]Frequently Asked Questions — часто задаваемые вопросы.
[2]Pretty Good Privacy — надежная конфиденциальность.
[3]Privacy Enhanced Mail — электронная почта с защитой приватности.

Коммуникации важны для всех аспектов обработки инцидентов. Команда сможет лучше поддерживать упомянутые выше методы, постоянно собирая относящуюся к делу информацию. Конкретные требования (например, звонок по конкретному номеру для проверки аутентичности ключа) следует делать изначально понятными. Шаблоны CSIRT предлагают стандартизованные способы доставки такой информации.

Технические и административные вопросы, связанные с защищенными коммуникациями, выходят за рамки этого документа. Группа реагирования должна поддерживать и использовать методы защиты коммуникаций внутри себя и со своими клиентами (или другими группами реагирования). Независимо от используемых механизмов должен обеспечиваться уровень защиты, устраивающий сообщество клиентов.

3 Информация, правила, процедуры

В разделе 2 отмечено, что правила и процедуры группы реагирования на инциденты должны быть опубликованы для сообщества клиентов. В этом разделе будут перечислены все типы информации, которую сообщество должно получить от группы реагирования. Способ обмена этой информацией с сообществом будет меняться от группы к группе, равно как и конкретное содержимое информации. Целью данного раздела является четкое описание различных видов информации, которую сообщество клиентов желает получить от группы реагирования.

Для упрощения понимания вопросов и тем, относящихся к взаимодействию клиентов с их CSIRT, мы предлагаем CSIRT публиковать всю информацию, правила и процедуры, адресованные клиентам, в форме отдельного документа, следуя шаблону, приведенному в Приложении D. Структура шаблона организует темы, упрощая предоставление конкретной информации. В Приложении E приведен пример заполненного шаблона для вымышленного XYZ University. Хотя конкретных рекомендаций для CSIRT по адаптации правил и процедур не дается, рассмотрены различные возможности в качестве примеров. Важно, чтобы CSIRT имела правила, а те, кто взаимодействует с CSIRT могли получить и понять эти правила.

Как обычно, документ не может учесть все аспекты для каждой среды и,или группы реагирования. Приведенные схемы следует рассматривать лишь в качестве предложения. Каждая группа реагирования может включить в свой документ все, что она сочтете нужным опубликовать для своих клиентов.

3.1 Получение документов

С течением времени информация CSIRT будет изменяться, поэтому корректно заполненный шаблон должен указывать дату последней редакции. Кроме того, следует предоставлять информацию о способах поиска обновленных документов. Без этого время от времени неизбежно будут возникать проблемы непонимания — устаревшие документы могут быть хуже отсутствия таковых.

- Дата обновления — Позволяет каждому заинтересованному оценить актуальность данного документа.
- Список распространения — Списки рассылок обеспечивают удобный механизм распространения обновленной информации среди большого числа пользователей. Группа реагирования может воспользоваться существующим списком или создать свой для уведомления пользователей об изменении документа. Список может также включать CSIRT с которыми данная группа часто взаимодействует.

  Для передаваемых группой CSIRT сообщениях об обновлении документа следует использовать цифровые подписи.
- Место хранения документа — Место, где можно получить текущую версию документа через сетевые службы группы реагирования. Клиенты в этом случае легко смогут получить дополнительную информацию о группе и проверить наличие обновлений. Доступные через сеть документы следует также сопровождать цифровой подписью.

3.2 Контактные данные

Здесь следует указать полные данные для контактов с CSIRT (набор таких данных может существенно различаться для разных групп — например, некоторые группы могут публиковать имена своих сотрудников).

- Название CSIRT
- Почтовый адрес
- Часовой пояс — Эта информация полезна для контактов с территориально удаленными клиентами.
- Номер телефона
- Номер для факсимильной связи
- Другие способы контактов — Те или иные способы защищенной голосовой связи (например, STU III).
- Адрес электронной почты
- Открытые ключи и метод шифрования — Использование конкретных методов зависит от возможностей сторон получать доступ к программам, ключам и т. п. Следует предоставить всю имеющую отношение к делу информацию, чтобы дать пользователям возможность определить применимые средства защиты коммуникаций с CSIRT.
- Члены группы реагирования

- Часы работы — Время работы группы в обычные дни и выходные. Поддержка круглосуточных обращений.

- Дополнительные контактные данные

Можно представить и более подробную информацию для контактов. Такая информация может включать данные для контактов с отдельными службами или список сетевых информационных ресурсов группы реагирования. Если для доступа к некоторым данным существуют особые процедуры доступа, они должны быть описаны здесь.

3.3 Устав

Каждая группа CSIRT должна иметь устав, в котором указано, что делает группа и ее полномочия. В устав следует включать по крайней мере:

- задачи группы;
- круг клиентов;
- принадлежность группы к другим структурам (спонсирование);
- полномочия.

3.3.1 Задачи группы

Описание задач следует сконцентрировать на основной деятельности группы, которая заявлена в определении CSIRT. Для того, чтобы команду видели в качестве группы реагирования на инциденты в сфере компьютерной безопасности, требуется публиковать отчеты об инцидентах и поддержке клиентов, у которых инциденты возникали.

Очень важно четко и однозначно описать цели и задачи команды.

3.3.2 Круг клиентов

Клиентов CSIRT можно определить несколькими способами. Например, это могут быть сотрудники компании или платные подписчики. Можно также определить клиентов на основе используемой ими технологии (например, конкретной операционной системы).

Заданный круг клиентов должен определить потенциальных потребителей услуг группы реагирования. Задающая правила часть документа (см. ниже) должна объяснять, как обрабатываются запросы, исходящие не из круга клиентов.

Если CSIRT считает возможным раскрытие своих клиентов, следует объяснить причины этого. Например, коммерческие CSIRT не будут раскрывать список своих клиентов, но будут декларировать предоставление услуг большим группам заказчиков. Это позволяет сохранить конфиденциальность, которая может быть условием контракта.

Клиенты могут перекрываться, как в случае, когда провайдер ISP поддерживающий CSIRT, предоставляет услуги заказчикам, у которых есть «свои» CSIRT. Раздел «Полномочия» в описании CSIRT (см. ниже) должен описывать такие отношения.

3.3.3 Принадлежность к другим структурам

Далее следует указать организацию-спонсора, которая предоставляет полномочия CSIRT. Эта информация поможет пользователям понять и оценить перспективы взаимодействия с данной CSIRT и весьма важна с точки зрения доверия между клиентом и CSIRT.

3.3.4 Полномочия

Этот раздел может существенно различаться для разных CSIRT в силу различий в их отношениях с клиентами. Организационные полномочия предоставляются CSIRT руководством компании, однако сообщество CSIRT будет выбираться и поддерживаться клиентами (обычно в качестве консультанта).

CSIRT может иметь полномочия по вмешательству в работу всех систем внутри своего периметра. Следует различать сферу контроля группы от круга ее клиентов. Если внутри периметра CSIRT существуют иерархические отношения с другой группой реагирования, это следует указать с упоминанием других CSIRT.

Раскрытие полномочий команды может раскрывать зону ее ответственности. Каждой группе следует получить правовые консультации по этому вопросу (см. параграф 3.7).

3.4 Правила

Для группы реагирования на инциденты очень важно определить свою политику (правила). В последующих параграфах рассматривается доведение этих правил до сообщества клиентов.

3.4.1 Типы инцидентов и уровень поддержки

Здесь следует в виде списка привести типы инцидентов, которые группа может решать, с указанием обеспечиваемого для каждого типа уровня поддержки. В описанном ниже разделе «Услуги» приведены рекомендации по более детальному описанию этих вопросов и освещению не связанных с инцидентами тем.

Уровень поддержки может изменяться в зависимости от текущей загрузки команды и полноты доступной информации. Факторы и их степень влияния на уровень поддержки следует разъяснять. Поскольку список известных типов инцидентов не может быть полным, CSIRT следует также предоставить некоторую информацию о предоставляемых «по умолчанию» услугах для новых типов инцидентов.

Группе следует указать, как она будет поступать с полученной информацией об уязвимостях, которые могут использоваться при новых инцидентах. Намерение действовать с такой информацией от имени (по запросу) клиента не является общим правилом, но может быть полезно в предупредительной работе с клиентами CSIRT.

3.4.2 Кооперация, взаимодействие и раскрытие информации

В этом разделе должны быть явно указаны CSIRT, с которыми взаимодействует данная группа. Взаимодействие может быть не связано с обработкой инцидентов и зачастую может заключаться в обмене опытом или технической кооперации. Здесь не нужно раскрывать детали взаимодействия, достаточно предоставить клиентам информацию для базового понимания кооперации с другими группами и целей такого взаимодействия.

Кооперация между CSIRT может быть упрощено за счет использования уникальных идентификаторов инцидентов в комбинации с явно описанными процедурами передачи обслуживания. Это снизит вероятность недоразумений и дублирования действий, поможет в отслеживании инцидентов и предотвратит коммуникационные «петли».

Политика отчетов и раскрытия информации должна ясно указывать круг получателей отчетов CSIRT в любых обстоятельствах. Следует также указать, что команда может работать совместно с другими CSIRT или напрямую с другим клиентом по вопросам, относящихся к этому клиенту.

Связанные группы CSIRT будут взаимодействовать с перечисленными ниже организациями.

Команды реагирования на инциденты.

CSIRT зачастую требуется взаимодействие с другими командами CSIRT. Например, CSIRT крупной компании может потребоваться уведомление национальной CSIRT о происходящем инциденте, а национальной команде CSIRT может потребоваться уведомлять национальные команды CSIRT в других странах для того, чтобы требуемые действия были выполнены на всех сайтах, вовлеченных в крупномасштабную атаку.

Взаимодействие между CSIRT может приводить к раскрытию (утечке) информации. Ниже приведен список примеров возможных утечек, который, естественно, не исчерпывает всех возможных вариантов утечек.

- Сообщения об инцидентах в зоне ответственности других команд. В таких случаях относящаяся к сайту информация может стать общедоступной (в частности, для прессы).
- Обработка инцидентов в своей зоне ответственности с передачей информации за пределы этой области (в предположении, что какая-то информация об инциденте уже вышла наружу).
- Сообщения из зоны ответственности команды, указывающие или подтверждающие инциденты за пределами этой зоны.
- Действия в связи с сообщениями об инцидентах извне.
- Передача информации об уязвимостях производителям, партнерским CSIRT или непосредственно на сайты, находящиеся вне зоны ответственности.
- Взаимодействие с организациями, сообщившими об инцидентах или уязвимостях.
- Предоставление контактных данных, относящихся к зоне ответственности команды, зонам ответственности других команд или правоохранительным организациям.

Производители.

Некоторые разработчики имеют свои команды CSIRT. В таких случаях эти команды напрямую взаимодействуют с производителем, внося предложения по улучшению или изменению продукции, анализирую технические проблемы или проверяя предлагаемые решения. Производители играют особую роль в инцидентах, включающих использование уязвимостей в их продукции.

Правоохранительные организации.

К таким организациям относятся полиция и детективные агентства. Командам CSIRT и пользователям приведенных здесь шаблонов следует соблюдать местное законодательство и нормы, которые могут существенно различаться в разных местах. CSIRT может сообщать технические детали атаки или обращаться за консультациями по правовым вопросам, связанным с инцидентом. Местные законы и нормы могут включать специфические требования по передаче информации и обеспечению конфиденциальности.

Пресса.

CSIRT могут время от времени общаться с представителями СМИ для их информирования или комментирования событий.

Полезны будут явные правила в части раскрытия информации при контактах с прессой, особенно в части разъяснения зоны ответственности CSIRT. Правила контактов с прессой должны дополнительно описывать рассмотренные выше вопросы передачи информации, поскольку СМИ могут оказывать существенное воздействие на свою аудиторию.

Прочие.

К этой категории относятся исследования и взаимодействие с организациями-спонсорами.

По умолчанию любая и все связанная с безопасностью информация, которую получает команда, обычно является конфиденциальной, однако жесткое следование этому правилу порождает «информационный вакуум», который может осложнить сотрудничество с клиентами и другими организациями. В шаблоне CSIRT следует указать, какая информация, кому и когда может быть опубликована или раскрыта.

Очевидно, что для разных команд будут действовать различные требования и ограничения в части раскрытия информации, особенно если команды находятся в разных юрисдикциях. Кроме того, дополнительные требования могут исходить от финансирующей команду организации. В шаблоне каждой команды следует указывать такие особенности для уведомления пользователей и других команд об их наличии.

Конфликты интересов (в частности, коммерческих) могут вносить дополнительные требования к раскрытию информации. Данный документ не содержит рекомендаций по разрешению таких конфликтов.

Команды обычно собирают статистику. Если собранная информация распространяется, в шаблоне следует описать правила раскрытия информации и способы получения статистических данных.

3.4.3 Аутентификация коммуникаций

Вы должны иметь правила, описывающие безопасные и проверяемые методы коммуникаций, которые будут применяться. Это необходимо для коммуникаций между командами CSIRT, а также между CSIRT и их клиентами. В шаблон следует включать открытые ключи или ссылки на них вместе с отпечатками ключей, а также рекомендации по использованию этой информации для проверки аутентичности и работы с поврежденными данными (например, способы информирования о повреждении).

В настоящий момент рекомендуется, как минимум, иметь каждой команде CSIRT ключ PGP (если это возможно). Команда может также применять другие механизмы (например, PEM, MOSS, S/MIME) в соответствии со своими потребностями и потребностями клиентов. Отметим, однако, что CSIRT и пользователи должны принимать во внимание местные законы и нормативные документы. В некоторых странах не разрешается криптостойкое шифрование или заданы правила использования технологий шифрования. Им также, что в большинстве стран для аутентификации с применением цифровых подписей не применяются нормативы, регулирующие шифрование.

Для телефонной и факсимильной связи CSIRT могут применять хранящиеся в секрете данные аутентификации партнеров (например, пароль или условная фраза). Обычно такие данные не публикуются, но об их существовании может быть известно.

3.5 Услуги

Услуги, предоставляемые командами CSIRT, можно поделить на две категории — действия в реальном масштабе времени, относящиеся к основной задаче реагирования на инциденты, и упреждающие действия для поддержки задач реагирования на инциденты. Вторая категория и часть первой включают услуги, не являющиеся обязательными и предлагаемые не всеми командами CSIRT.

3.5.1 Реакция на инциденты

Обработка инцидентов обычно включает в себя оценку входящей информации о них (Incident Triage — оценка инцидента) и последующие действия вместе с другими CSIRT, ISP и сайтами (Incident Coordination — координация действий). Третьей категорией услуг является помощь местным сайтам при восстановлении после инцидента (Incident Resolution — предотвращение последствий), эта услуга является необязательной для CSIRT и не все команды оканывают такие услуги.

3.5.1.1 Оценка инцидента

При оценке инцидента обычно выполняется:

- оценка информации - интерпретация поступивших сведений, расстановка приоритетов, сопоставление с прошлыми инцидентами и тенденциями;
- проверка сведений — верификация достоверности данных об инциденте и сфере его действия.

3.5.1.2 Координация действий

В процессе координации бействий обычно выполняется:

- категоризация сведений — разделение связанной с инцидентом информации по категориям (журнальные файлы, контактные данные и т. д.) с учетом политики раскрытия информации;
- координация — уведомление вовлеченных в инцидент и его обработку сторон с учетом политики раскрытия информации.

3.5.1.3 Предотвращение последствий

Обычно эти дополнительные (не обязательные) услуги по устранению последствий инцидентов могут включать:

- техническая поддержка — может включать анализ скомпрометированных систем;
- обучение — выяснение причин инцидента (использованных уязвимостей) и их воздействий (например, сохраняющийся доступ злоумышленника в систему);
- восстановление — возвращение в нормальное состояние поврежденных или остановленных в результате инцидента систем и служб.

3.5.2. Упреждающие действия

Обычно эти дополнительные (не обязательные) услуги по предотвращению инцидентов могут включать:

- информационное обеспечение — может включать архив известных уязвимостей, исправлений для решения известных проблем, списки рассылок;
- средства обеспечения безопасности — могут включать инструменты для аудита безопасности сайта;
- обучение и тренировка;
- оценка различных видов оборудования и программ;
- аудит и консультации в части безопасности сайта.

3.6 Формы отчетов об инцидентах

Использование готовых форм для заполнения упрощает действия при инцидентах как пользователям, так и командам реагирования. Пользователь может ответить на некоторые важные вопросы еще до контакта с командой реагирования на инциденты и, следовательно, быть более подготовленным к такому контакту. Команда реагирования получает всю требуемую информацию сразу в заполненной форме и сможет эффективно работать с инцидентом.

В зависимости от целей и услуг конкретной команды CSIRT могут использоваться разные варианты форм. Например, форма отчета о найденной уязвимости может существенно отличаться от формы сообщения об инциденте.

Наиболее эффективным путем распространения форм является их размещение на публично доступном сайте команды. Точные ссылки на такие формы должны быть приведены в документе, описывающем CSIRT, вместе с рекомендациями по использованию и заполнению форм. Если для передачи заполненных форм используется отдельный адрес электронной почты, этот адрес также следует указывать.

Одним из примеров может служить форма сообщения об инциденте (Incident Reporting Form) Координационного центра CERT — ftp://info.cert.org/incident_reporting_form[1].

3.7 Отказ от ответственности

Хотя описывающий CSIRT документ не является договором, на основе описания целей и услуг могут возникать предположения об ответственности. Рекомендуется включать в конце документа заявления об отказе от ответственности, которое будет предупреждать пользователей о возможных ограничениях.

В ситуациях, когда исходный документ должен переводиться на другой язык, в перевод следует включать заявление об отказе от ответственности и ссылку на оригинал документа. Ниже приведен пример такого текста.

> Хотя мы постарались аккуратно перевести исходный документ с немецкого языка на английский, мы не можем гарантировать сохранение полной идентичности обоих документов в части детализации и корректности. При возникновении каких-либо разночтений или разнотолков немецкая версия документа считается приоритетной.

Применимость заявлений об отказе от ответственности регулируется местным законодательством и нормативными актами, которые должны быть известны CSIRT. При возникновении сомнений следует получить консультации юристов.

Приложение A: Словарь терминов

В этом глоссарии определены термины, используемые в описаниях инцидентов в сфере безопасности и CSIRT. Список включает ограниченное число терминов, дополнительные определения можно найти, в частности, в [RFC 1983].

Constituency - клиентура

Неявное целью команд CSIRT является наличие клиентуры, к каковой относится группа пользователей, сетей и организаций, обслуживаемых командой. Для эффективной работы команды она должна быть признана клиентами.

Security Incident — инцидент в сфере безопасности

В этом документе термин является синонимом «инцидента в сфере компьютерной безопасности» (Computer Security Incident) — любого неблагоприятного события, ставящего под угрозу те или иные аспекты безопасности компьютеров или сетей.

Определения инцидентов могут существенно различаться, но перечисленные ниже категории применимы к большинству случаев:

- утечка информации;
- нарушение целостности информации;
- отказ служб;
- злоупотребление службами, системами или информацией;
- повреждение систем.

Это наиболее общие категории. Например, подмена системной утилиты «троянской программой» является примером «нарушения целостности», а успешный подбор пароля — примером «утечки информации». Атаки, даже если они не завершились успехом, могут трактоваться, как инциденты.

При определении инцидентов используется термин compromised («взломан», «находится под угрозой»). Иногда администратор может лишь «предполагать» инцидент. При обработке инцидента следует четко различать реальный инцидент от предполагаемого.

Computer Security Incident Response Team — команда реагирования на инциденты

С учетом двух приведенных выше определений, CSIRT представляет собой команду, которая координирует и поддерживает действия в ответ на инциденты безопасности, в которые вовлечены сайты, относящиеся к клиентам данной команды.

Команда CSIRT должна:

- поддерживать (защищенный) канал для получения информации об инцидентах;
- обеспечивать содействие своим клиентам при возникновении инцидентов;
- распространять связанную с инцидентами информация среди своих клиентов и иных вовлеченных в инцидент сторон.

Отметим, что здесь не упомянуты полиция и другие правоохранительные органы, которые могут быть вовлечены в расследование компьютерных преступлений. Командам CSIRT для своей работы не требуется каких-либо специальных полномочий сверх доступных обычным гражданам.

Vendor - производитель

Термин vendor используется для обозначения любого производителя сетевых или компьютерных технологий, отвечающего за технические аспекты этой технологии. К «технологиям» в данном случае можно отнести оборудование (компьютеры, маршрутизаторы, коммутаторы и т. п.) и программы (операционные системы, приложения и т. п.).

Отметим, что поставщики технологий не обязательно являются их производителями (vendor). Например Internet-провайдеры (ISP) могут поставлять своим заказчикам маршрутизаторы, но производителем таковых не являться и не отвечать за технические аспекты работы маршрутизаторов.

[1] На момент публикации перевода приведенная ссылка утратила актуальность. *Прим. перев.*

Vulnerability - уязвимость

Уязвимостью называется некая часть технологии, которой можно воспользоваться для создания инцидента в сфере безопасности. Например, если программа позволяет обычному пользователю выполнять произвольные системные команды в привилегированном режиме, это «свойство» является уязвимостью программы.

Приложение B. Дополнительные материалы

Важные вопросы связанные с обработкой инцидентов на уровне сайта рассмотрены в [RFC 2196] (Site Security Handbook), подготовленном рабочей группой SSH[1]. Этот документ будет обновлен группой SSH и будет включать рекомендации в части локальных правил и процедур, связанные, прежде всего, с предотвращением инцидентов.

По вопросам CSIRT и решаемых командами задач в сети имеется много документов, анонимно доступных по протоколу FTP. Коллекция таких документов доступна на сайте

ftp://ftp.cert.dfn.de/pub/docs/csir/[2]

Содержимое каталога описано в текстовом файле 01-README.

Некоторые документы, представляющие интерес в контексте обсуждаемых здесь вопросов доступны по ссылке

ftp://ftp.nic.surfnet.nl/surfnet/net-security/cert-nl/docs/reports/R-92-01[2]

Отчет включает Operational Framework групп CERT-NL, CSIRT SURFnet (провайдер из Нидерландов).

Читатели, интересующиеся работой FIRST[3], могут найти дополнительную информацию в Приложении C.

- http://hightop.nrl.navy.mil/news/incident.html[2] - руководство NRL по откликам на инциденты;
- http://www.cert.dfn.de/eng/team/kpk/certbib.html[2] - аннотированный список литературы, документов и файлов, связанных с работой CSIRT, со ссылками.
- ftp://info.cert.org/incident_reporting_form[2] - форма отчета об инциденте от Координационного Центра CERT для сбора информации и сокращения задержек связанных с необходимостью запроса дополнительной информации от вовлеченного в инцидент сайта;
- http://www.cert.org/cert.faqintro.html[2] - ответы на часто задаваемые вопросы (FAQ) от Координационного Центра CERT.

Приложение C: Известные группы CSIRT

В настоящее время имеется множество разных CSIRT, но какой-то общий список таких групп отсутствует. Большинство основных и давно существующих команд (первая CSIRT появилась в 1988 г.) являются членами всемирного форума FIRST. На момент написания этого документа форум объединял более 55 команд (1 в Австралии, 13 в Европе, остальные в Северной Америке). Информацию о FIRST можно найти по приведенным ниже ссылкам.

- http://www.first.org/

  Текущий список участников с контактными данными и некоторой дополнительной информацией.

- http://www.first.org/team-info/[2]

  Для CSIRT, которые хотят стать участниками форума (отметим, что для вступления нужна рекомендация одного из действительных членов FIRST), the following files contain more information:

- http://www.first.org/about/op_frame.html[2]

  Описание работы FIRST.

- http://www.first.org/docs/newmem.html[2]

  Рекомендации для команд, желающих вступить в FIRST.

Многие из европейских команд, независимо от их участия в FIRST, указаны по странам в списке, поддерживаемом немецкой CSIRT

- http://www.cert.dfn.de/eng/csir/europe/certs.html[2]

Для получения информации об имеющихся командах зачастую уместно задать вопрос участникам одной из известных команд или провайдеру Internet.

Приложение D: Схема формы для CSIRT

Это приложение резюмирует рассмотренные в документе вопросы и содержит рекомендуемый шаблон документа с описанием CSIRT. Структура шаблона разработана так, чтобы упростить читателям понимание правил и процедур CSIRT, а также предоставить иную информацию по части взаимодействия с клиентами и другими командами CSIRT. Пример заполненного шаблона приведен в Приложении E.

1. Информация о документе

1.1 Дата обновления

1.2 Список распространения уведомлений

1.3 Где можно найти документ

---

[1]Site Security Handbook.
[2]На момент публикации перевода приведенная ссылка утратила актуальность. *Прим. перев.*
[3]Forum of Incident Response and Security Teams — Форум групп по реагированию на инциденты и компьютерной безопасности.

Приложение E: Пример заполненной формы для CSIRT

Ниже приведен пример заполненной формы для вымышленной команды CSIRT под названием XYZ-CSIRT. Текст представлен лишь в качестве примера и не выражает мнение рабочей группы или IETF по отношению к тому или иному набору процедур и правил. Тем не менее, реальные CSIRT могут воспользоваться по своему желанию нужными фрагментами приведенного ниже текста, если они соответствуют реалиям команды.

Описание XYZ-CERT

---

1. О документе

1.1 Дата обновления

Документ версии 1.01 опубликован 31.03.1997.

1.2 Список распространения уведомлений

Уведомления о внесенных в документ обновлениях распространяются через список почтовых рассылок <xyz-cert-info@xyz-univ.ca>. Запросы на включение в этот список следует направлять Majordomo по адресу <xyz-cert-info-request@xyz-univ.ca>, включив в текст запроса слово subscribe (подписать). Для получения информации о списке рассылок включите в текст сообщения слово help (помогите). Список рассылки модерируется.

1.3 Где можно найти документ

Текущая версия данного описания CSIRT доступна на Web-сайте XYZ-CERT по ссылке http://www.xyz-univ.ca/xyz-cert/english/CSIRT-descr.txt. При использовании документа убедитесь в актуальности имеющейся у вас версии.

1.4 Аутентификация документа

Версии этого документа на английском и французском языке подписаны ключом PGP группы XYZ-CERT. Подписи доступны на Web-сайте по ссылкам http://www.xyz-univ.ca/xyz-cert/english/CSIRT-descr.asc, http://www.xyz-univ.ca/xyz-cert/francais/CSIRT-descr.asc.

2. Контактные данные

2.1 Название команды

XYZ-CERT — команда реагирования на компьютерные инциденты университета XYZ (XYZ University Computer Emergency Response Team).

2.2 Адрес

XYZ-CERT

XYZ University, Computing Services Department

12345 Rue Principale

UniversityTown, Quebec

Canada H0H 0H0

2.3 Часовой пояс

Canada/Eastern (GMT-0500, GMT-0400 с апреля по октябрь).

2.4 Телефонный номер

+1 234 567 7890 (спросить XYZ-CERT).

2.5 Номер для факсимильной связи

+1 234 567 7899 (факсимильная связь **не защищена**).

2.6 Другие способы связи

Нет.

2.7 Адрес электронной почты

<xyz-cert@xyz-univ.ca> Направленные по этому адресу сообщения пересылаются сотрудникам XYZ-CERT.

2.8 Открытые ключи и другая информация о шифровании

XYZ-CERT использует ключ PGP с KeyID = 12345678 и отпечатком 11 22 33 44 55 66 77 88 88 77 66 55 44 33 22 11.

Ключ и его подписи можно найти на обычных больших серверах ключей.

Поскольку PGP остается сравнительно новой технологией в университете XYZ, этот ключ имеет относительно небольшое число подписей, однако прилагаются усилия по увеличению числа ссылок на этот ключ в сети доверия (web of trust) PGP. В то же время, благодаря наличию в большинстве университетов Квебека хотя бы одного человека, знакомого с координатором XYZ-CERT Zoe Doe, последний подписал ключ XYZ-CERT и будет рад подтвердить его отпечаток своим ключом для тех людей, с которыми он знаком по телефонному общению или лично.

2.9 Члены команды

Zoe Doe из Computing Services является координатором XYZ-CERT. Другие координаторы и остальные члены команды вместе с описаниями их опыта, сферы ответственности и контактными данными перечислены на сайте XYZ-CERT по ссылке http://www.xyz-univ.ca/xyz-cert/teamlist.html.

Управление, связи и контроль обеспечивает помощник директора Computing Services по техническим вопросам Steve Tree.

2.10 Прочая информация

Общая информация о XYZ-CERT, а также ссылки на рекомендуемые командой ресурсы по вопросам безопасности, приведены на странице http://www.xyz-univ.ca/xyz-cert/index.html.

2.11 Точки контактов с клиентами

Предпочтительным способом связи с командой XYZ-CERT является электронная почта, сообщения, направленные по адресу <xyz-cert@xyz-univ.ca>, пересылаются соответствующим специалистам и их заместителям незамедлительно. Если сообщение требует незамедлительных действий, включите слово urgent (срочно) в тему.

При невозможности (или нежелательности по соображениям безопасности) использования электронной почты с XYZ-CERT можно связаться по телефону в обычные часы работы команды. Телефонные сообщения просматриваются реже электронной почты.

Время работы XYZ-CERT в нормальных условиях совпадает с общепринятым (с 09:00 до 17:00 с понедельника по пятницу, за исключением праздников).

По возможности при отправке информации используйте форму, приведенную в разделе 6.

3. Устав

3.1 Заявленные цели

Целью XYZ-CERT является, во-первых, оказание помощи членам сообщества университета XYZ в реализации упреждающих мер по снижению рисков инцидентов в сфере компьютерной безопасности, а во-вторых, оказание помощи сообществу XYZ при обработке возникших инцидентов.

3.2 Круг клиентов

Клиентами XYZ-CERT является сообщество университета XYZ, определенное в контексте «Политики университета XYZ в части использования компьютерных ресурсов», доступной по ссылке http://www-compserv.xyz-univ.ca/policies/pcf.html

Однако следует отметить, что перечисленные выше услуги предоставляются только для систем, относящихся к университетскому сайту.

3.3 Спонсоры и участие в других организациях

Спонсором XYZ-CERT является ACME Canadian Research Network. Команда поддерживает связи с группами CSIRT других университетов Канады и США при возникновении необходимости.

3.4 Полномочия

XYZ-CERT работает под эгидой и с полномочиями, предоставленными Department of Computing Services университета XYZ. Дополнительную информацию о правах и полномочиях Department of Computing Services можно найти в документе Policy on Computing Facilities, доступном на сайте университета XYZ по ссылке http://www-compserv.xyz-univ.ca/policies/pcf.html

XYZ-CERT предполагает рабоать совместно с системными администраторами и пользователями университета XYZ University, избегая, по возможности, авторитарных отношений. Однако при возникновении необходимости XYZ-CERT будет обращаться в Department of Computing Services для получения требуемых полномочий. Все участники XYZ-CERT являются членами CCSA[1] и имеют все права, полномочия и обязанности, предоставленные системным администраторам правилами работы с компьютерными системами (Policy on Computing Facilities) или руководящим составом университета.

Членам сообщества университета XYZ, желающим участвовать в работе XYZ-CERT, следует обращаться к помощнику директора Computing Services по техническим вопросам. Если помощник не доступен, можно обратиться напрямую к директору (в случае обнаружения проблем с существующими правилами) или в Office of Rights and Responsibilities университета XYZ (в случае обнаружения проблем с применением существующих правил).

4. Правила

4.1 Типы инцидентов и уровень поддержки

Команда XYZ-CERT уполномочена работать со всеми типами инцидентов в сфере компьютерной безопасности, которые возникают или угрожают возникнуть в университете XYZ.

Уровень поддержки от XYZ-CERT будет существенно меняться в зависимости от типа и важности инцидента или проблемы, типа клиента, размера сообщества, на которое влияет инцидент и доступных в данный момент ресурсов XYZ-CERT, хотя во всех случаях команда обеспечит тот или иной отклик в течение одного рабочего дня. Ресурсы будут выделяться в соответствии с приведенными ниже приоритетами (в порядке убывания):

- угроза физической безопасности людей;
- атаки системного уровня на любую из информационных систем управления (MIS[2]) или любую часть инфраструктуры опорной сети;
- атаки системного уровня на любую из больших машин, обеспечивающих публичный сервис (многопользовательскую или специализированную);
- возникновение риска, связанного с использованием привилегированных учетных записей или специальных программ, которые, в частности, могут обеспечить доступ к приложениям MIS с конфиденциальными данными или системному администрированию;
- атаки на службы, связанные с любым из 3 предыдущих пунктов;
- все вышеперечисленное на других сайтах университета XYZ;
- масштабные атаки всех видов (например, перехват трафика, атаки с использованием социальной психологии в IRC, подбор пародей);
- угрозы, преследования и другие уголовные преступления, связанные с учетными записями отдельных пользователей;
- возникновение риска, связанного с учетными записями отдельных пользователей в многопользовательских системах;
- возникновение риска для настольных систем;
- подделки, введение в заблуждение и другие, связанные с безопасностью нарушения местных правил и норм (например, обманное использование электронной почты или сетевых новостей, неуполномоченное применение ботов IRC);
- атаки на службы для учетных записей отдельных пользователей (например, спам в конкретный адрес).

Не указанные в списки типы инцидентов будут приоритизироваться и обрабатываться в соответствии с воспринимаемым для ниж уровнем важности и масштабом.

Отметим, что прямой поддержки конечным пользователям команда не предоставляет — предполагается, что они взаимодействуют со своим системным или сетевым администратором и непосредственным руководством, а те, в свою очередь, получают поддержку от XYZ-CERT.

[1]Committee of Computer Systems Administrators — комитет администраторов компьютерных систем.
[2]Management Information System.

Хотя XYZ-CERT понимает, что уровни системных администраторов в университете XYZ могут сильно различаться, и будет стремиться предоставить информацию и помощь в соответствии с персональным уровнем, XYZ-CERT не сможет обучить системных администраторов «на лету» и не может поддерживать системы от их имени. В большинстве случаев XYZ-CERT будет просто указывать источники информации, требуемой для реализации конкретных мер.

XYZ-CERT стремится своевременно информировать системных администраторов университета XYZ о возможных уязвимостях, до того, как ими реально кто-либо воспользуется.

4.2 Кооперация, взаимодействие и раскрытие информации

Хотя существуют правовые и морально-этические ограничения на распространение информации из XYZ-CERT, большинство из которых указаны также в правилах пользования компьютерными ресурсами университета XYZ и эти ограничения будут безусловно соблюдаться, XYZ-CERT подтверждает свое стремление поддерживать существующий в Internet дух сотрудничества. Следовательно, соблюдая меры по сокрытию информации о конкретных лицах из числа клиентов и соседних сайтов, XYZ-CERT будет открыто распространять информацию, которая может помочь другим в предотвращении или преодолении инцидентов в сфере безопасности.

Ниже слова «затрагиваемые стороны» (affected parties) служат для обозначения законных владельцев, операторов и пользователей соответствующих компьютерных средств. Они не относятся к не имеющим полномочий пользователям, включая тех пользователей, которые пытаются выйти за пределы своих полномочий, - такие пользователи считаются нарушителями и не могут ожидать от XYZ-CERT сохранения своих имен в тайне. Если их конфиденциальность защищена законом, это будет приниматься во внимание.

Перед выдачей информации наружу она классифицируется по приведенным ниже критериям.

- Информация о конкретных пользователях, а в некоторых случаях и об отдельных приложениях, должна рассматривать, как конфиденциальная в соответствии с требованиями законодательства, договорами и/или этическими соображениями.

  Информация о частных лицах, позволяющая идентифицировать конкретных людей, не может выходить за пределы XYZ-CERT за исключением указанных ниже случаев. Данные, не позволяющие идентифицировать конкретных людей, могут распространяться свободно (например, образец изменения файла .cshrc злоумышленником, или описание конкретной социально-психологической атаки).

- Информация о нарушителях рассматривается подобно другой информации о пользователях, но с некоторыми исключениями.

  Хотя информация о нарушителях (в частности, позволяющая идентифицировать конкретных людей) не может выходить наружу (если она не становится достоянием общественности в результате уголовного расследования), она может передаваться системным администраторам и другим командам CSIRT, связанным с инцидентом.

- Приватной информацией о сайте является техническая информация о конкретных системах или сайтах.

  Такая информация не распространяется без разрешения со стороны рассматриваемого сайта за исключением указанных ниже случаев.

- Информация об уязвимостях — это технические сведения об уязвимостях и атаках, включая исправления и способы устранения уязвимостей.

  Информация об уязвимостях может распространяться свободно, хотя всякий раз следует информировать производителя до того, как сделать информацию общедоступной.

- Информация о факте инцидента, области его воздействия и значимости. Такая информация может относиться к сайту в целом, отдельным пользователям и группам.

  Сведения такого рода не распространяются без согласия затронутого сайта или пользователей, за исключением отмеченных ниже случаев.

- Статистическая информация представляет собой сведения об инциденте, из которых исключены идентификационные данные.

  Статистическая информация может распространяться по решению Computing Services Department.

- Контактные сведения указывают способы связи с системными администраторами и CSIRT.

  Контактные данные распространяются свободно, за исключением случаев, когда запрашиваются сведения о человеке или объекте, не имеющем отношения к деятельности команды, или XYZ-CERT по тем или иным причинам не желает распространять такую информацию.

Потенциальных получателей информации от команды XYZ-CERT можно разделить на несколько классов.

- По самой природе их ответственности и связанных с этим ожиданий конфиденциальности управляющий состав университета XYZ имеет право получать любую информацию, которая может облегчить обработку инцидентов в сфере компьютерной безопасности, происходящих в их юрисдикции.

- Члены Office of Rights and Responsibilities имеют право получать любую запрошенную ими информацию об инцидентах в сфере компьютерной безопасности или связанную с такими инцидентами, которая требуется для преодоления инцидента. Такими же правами пользуются члены XYZ Security Department, участвующие в расследовании инцидента или запросившие такое расследование.

- Системные администраторы университета XYZ, являющиеся членами CCS, в силу своих обязанностей также имеют доступ к конфиденциальным данным. Однако, если эти люди не входят также в состав XYZ-CERT, они будут получать лишь часть информации, которая нужна им для участия в расследовании или обеспечения безопасности их систем.

- Пользователи из университета XYZ имеют право на получение информации, связанной с безопасностью их учетных записей, даже если такая информация относится к атакующему или раскрывает сведения о другом пользователе. Например, если учетная запись аааа взломана и атакующий использует ее для атаки на учетную запись bbbb, пользователь bbbb имеет право знать о взломе аааа и способах использования этой записи для атаки на bbbb. Пользователь bbbb имеет также право получить по запросу информацию об учетной записи аааа, которая может поспособствовать расследованию атаки. Например, если bbbb атакован кем-то, удаленно подключившимся к аааа, пользователю bbbb следует предоставить данные о подключениях к аааа, даже если в обычных условиях такие сведения рассматриваются, как приватные данные аааа. Пользователи из университета XYZ имеют право получать информацию о подозрениях в части взлома их учетных записей.

- Сообщество университета XYZ не будет получать информацию с ограниченным доступом за исключением тех случаев, когда затрагиваемые стороны дают разрешение на распространение такой информации. Статистическая информация может быть доступна большей части сообщества XYZ. Команда XYZ-CERT не принимает на себя обязательств в части информирования сообщества об инцидентах, но может делать это по своему усмотрению. В частности, очевидно, что XYZ-CERT будет информировать все затронутые стороны о возможных способах воздействия на них, а также давать рекомендации по преодолению последствий инцидента.

- Информация с ограниченным доступом не распространяется публично. Фактически, не будет предприниматься никаких усилий по публичному распространению информации, хотя XYZ-CERT признает, что доступная сообществу университета XYZ информация становится публичной и, впоследствии команда будет распространять такую информацию.

- Сообщество компьютерной безопасности будет трактоваться так же, как все прочие люди. Хотя члены XYZ-CERT могут участвовать в дискуссиях этого сообщества (соседние команды, почтовые конференции, включая открытые списки bugtraq) и конференциях, такое общение считается публичным раскрытием информации. Несмотря на возможность рассмотрения технических вопросов (включая уязвимости) на любом уровне детализации, любые примеры из практики XYZ-CERT должны исключать возможность идентификации затронутых сторон.

- Контакты с прессой также рассматриваются, как публичное раскрытие информации. Команда XYZ-CERT не будет напрямую взаимодействовать с журналистами по вопросам инцидентов в сфере безопасности за исключением обсуждения тем, которые уже раскрыты публично. При необходимости информация будет представлена департаменту университета по связям с общественностью (XYZ University Public Relations Department) и группе по взаимодействию с заказчиками (Customer Relations) Computing Services Department. Все связанные с инцидентами запросы будут направляться в эти две организации. Сказанное выше не запрещает членам XYZ-CERT давать интервью по общим вопросам компьютерной безопасности; фактически их призывают давать такие интервью для повышения информированности сообщества.

- Другим сайтам и группам CSIRT, когда они являются партнерами по расследованию инцидента в сфере компьютерной безопасности, в некоторых случаях может предоставляться конфиденциальная информация. Это может происходить лишь в тех случаях, когда добропорядочность внешнего сайта или группы может быть проверена, а передаваемая информация ограничивается сведениями, которые явно будут полезны для преодоления инцидента. Очевидно, что подобная передача информации может осуществляться сайтам, хорошо известным команде XYZ-CERT (например, с некоторыми университетами Квебека университет XYZ имеет неформальные но очень тесные связи).

- При обработке инцидентов некоторая, сравнительно приватная, но достаточно безвредная информация (типа сведений о точках, из которых пользователи подключались к системе) не будет считаться конфиденциальной и может быть передана внешним сайтам без излишних предосторожностей. Информация о нарушителях будет свободно передаваться другим системным администраторам и CSIRT. Информация, способная поставить кого-либо в неловкое положение, может быть передана с разумными мерами предосторожности в части ее конфиденциальности и при условии реальной потребности в ней для преодоления инцидента.

- В большинстве случаев производители будут рассматриваться в плане распространения информации, как внешние команды CSIRT. XYZ-CERT желает призвать всех производителей сетевого и компьютерного оборудования, программ и услуг повышать уровень безопасности своей продукции. Для достижения этой цели информация о всех найденных в продукции уязвимостях будет сообщаться соответствующим производителям вместе с техническими деталями, нужными для идентификации и исправления. Информацию, позволяющая идентифицировать те или иные стороны, не будет передаваться производителям без разрешения этих сторон.

- Сотрудникам правоохранительных органов будет обеспечиваться полное взаимодействие с XYZ-CERT, включая предоставления любой информации, которая может послужить расследования инцидента, в соответствии с правилами Policy on Computing Facilities.

4.3 Связь и аутентификация

С учетом типов информации, с которой скорей всего будет иметь дело XYZ-CERT, телефонную связь можно считать достаточно защищенной даже без использования шифрования. Нешифрованная электронная почта не является достаточно защищенной, но ее вполне можно использовать для передачи некритичной информации. При необходимости отправки по электронной почет конфиденциальных сведений будет использоваться шифрование PGP. Копирование файлов через сеть похоже на передачу электронной почты и конфиденциальные сведения следует шифровать для передачи через сеть.

Там, где нужно организовать доверительные отношения (например, перед использованием информации, полученной XYZ-CERT извне или перед раскрытием конфиденциальных сведений) идентификация и добросовестность другой стороны проверяется. В рамках университета XYZ и с хорошо известными соседями для такой проверки достаточно будет мнения известных людей, которым можно доверять. В других ситуациях применяются подходящие методы типа опроса членов FIRST, использования данных WHOIS и других регистрационных баз Internet и т. п., вплоть до телефонных звонков и электронных сообщений чтобы убедиться в том, что другой стороной не является самозванец. Входящие сообщения электронной почты, которым можно доверять, проверяются прямым контактом с отправителем либо по цифровым подписям (в частности, поддерживается PGP).

5. Услуги

5.1 Обработка инцидентов

XYZ-CERT будет помогать системным администраторам при решении технических и административных вопросов во время инцидентов. В частности, команда будет обеспечивать помощь и содействие при решении перечисленных ниже вопросов.

5.1.1 Классификация инцидентов

- Проверка самого факта наличия инцидента.
- Определение сферы охвата для инцидента.

5.1.2 Координация действий

- Определение исходной причины инцидента (использованной уязвимости).
- Помощь в контактах с другими сайтами, которые могут быть вовлечены в инцидент.
- Помощь в контактах со службой безопасности университета XYZ и/или правоохранительными органами (при необходимости).
- Подготовка информации для других команд CSIRT.
- Подготовка информации для пользователей (если нужно).

5.1.3 Предотвращение последствий инцидента

- Устранение уязвимости.
- Защита систем от воздействия инцидента.
- Оценка возможных действий с точки зрения их стоимости и связанных рисков (в частности, действий, связанных с возможным преследованием или дисциплинарным взысканием, сбор доказательств, наблюдение за развитием инцидента, установка ловушек для злоумышленников и т. п.).
- Сбор доказательств для уголовного преследования или дисциплинарного воздействия (если это планируется).

В дополнение к этому XYZ-CERT будет собирать статистику инцидентов в сообществе университета XYZ и инцидентов, в которые это сообщество оказалось вовлечено, а также по мере необходимости будет уведомлять сообщество о мерах защиты от известных атак.

Для обращения в XYZ-CERT при возникновении инцидента следует отправить письмо по электронной почте, как описано выше в параграфе 2.11. Следует помнить, что уровень возможной помощи может существенно меняться в зависимости от параметров, описанных в параграфе 4.1.

5.2 Упреждающие действия

XYZ-CERT координирует и поддерживает перечисленные ниже услуги в зависимости от наличия свободных ресурсов.

- *Информационные услуги*
  - Список административных и технических контактов департамента безопасности. Такие списки будут общедоступными по каналам общего пользования типа WWW[1] и DNS[2].
  - Списки рассылок для информирования связанных с безопасностью пользователей о новостях, относящихся к их компьютерным системам. Эти списки доступны только системным администраторам университета XYZ.
  - Хранилище предоставляемых производителями и другими организациями связанных с безопасностью исправлений (patch) для различных операционных систем. Это хранилище является общедоступным с учетом лицензионных ограничений. Доступ к хранилищу обеспечивается через службы общего назначения типа WWW и/или ftp.
  - Хранилище связанного с безопасностью инструментария и документации для системных администраторов. По возможности в хранилище будут помещаться скомпилированные и готовые к установке версии программ. Хранилище доступно по обычным каналам WWW и/или ftp.
  - Выборки из различных ресурсов (типа списков рассылок и почтовых конференций), распространяемые через список рассылки или web-сервер в зависимости от уровня открытости и важности информации.
- *Обучение*
  - Члены XYZ-CERT будут периодически проводить семинары по вопросам, связанным с компьютерной безопасностью, для системных администраторов университета XYZ.
- *Аудит*
  - Проверка центральных файловых хранилищ на Unix-машинах и других платформах, с которыми работает tripwire.
  - Классификация по уровням безопасности — машины и подсети университета будут проверяться и оцениваться по уровням безопасности. Информация об этих уровнях будет доступна сообществу

[1]World Wide Web.
[2]Domain Name Service.

университета XYZ с целью установки соответствующих прав доступа. Однако детали аудита и оценки считаются конфиденциальными и будут доступны лишь затрагиваемым сторонам.

- *Архивирование*
  - Централизованные системные журналы для машин, поддерживающих удаленную запись событий в стиле Unix. Записи журнал автоматически просматриваются программами-анализаторами с выделением событий и тенденций, которые могут вызывать проблемы безопасности, и уведомлением соответствующих системных администраторов.
  - Запись и хранение сведений о возникших инцидентах в сфере безопасности. Сами записи считаются конфиденциальными, но периодически на их основе выпускаются статистические отчеты, доступные для сообщества университета XYZ.

Подробные описания перечисленных выше услуг и инструкции по подключению к спискам рассылок, загрузке информации или участии в некоторых работах (например, централизованная запись событий и проверка целостности файлов) доступны на web-сервере XYZ-CERT по приведенной в параграфе 2.10 ссылке.

6. Форма сообщений об инцидентах

Формы по уведомлению XYZ-CERT еще не разработаны. По возможности следует использовать Incident Reporting Form Координационного центра CERT (Pittsburgh, PA). Текущая версия этого документа доступна по ссылке ftp://info.cert.org/incident_reporting_form[1].

7. Отказ от ответственности

Несмотря на то, что при подготовке информации, уведомлений и сигналов принимаются меры предосторожности, XYZ-CERT не предполагает какой-либо ответственности за допущенные ошибки или опечатки, а также за повреждения или нарушения, возникшие в результате использования представленной командой информации.

4 Благодарности

Редакторы благодарят Anne Bennett за внесенный вклад и редакторские правки. Спасибо также Don Stikvoort за помощью в правке описания услуг команд по реагированию на инциденты.

5 Литература

[RFC 2196] Fraser, B., "Site Security Handbook", FYI 8, RFC 2196, September 1997.

[RFC 1983] Malkin, G., "Internet Users' Glossary", FYI 18, RFC 1983, August 1996.

6 Вопросы безопасности

В этом документе рассмотрены вопросы работы команд по реагированию на инциденты в сфере компьютерной безопасности и взаимодействия таких команд с их клиентами и другими организациями. Документ, следовательно, не связан напрямую с безопасностью протоколов, приложений и сетевых систем. Он не связан даже с конкретными откликами и реакцией на инциденты в сфере безопасности, а служит лишь описанием откликов, предлагаемых командами CSIRT.

Тем не менее, жизненно важна безопасная работа самих CSIRT, что требует организации защищенных каналов связи с другими командами и клиентами. Команды также должны поддерживать высокий уровень безопасности для своих систем и инфраструктуры, а также обеспечивать конфиденциальность данных об идентификации угроз, а также своих информаторов о связанных с безопасностью инцидентах.

7 Адреса авторов

Nevil Brownlee

ITSS Technology Development

The University of Auckland

Phone: +64 9 373 7599 x8941

EMail: n.brownlee@auckland.ac.nz

Erik Guttman

Sun Microsystems, Inc.

Bahnstr. 2

74915 Waibstadt Germany

Phone: +49 7263 911484

EMail: Erik.Guttman@sun.com

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

[1]На момент публикации перевода приведенная ссылка утратила актуальность. *Прим. перев.*

8 Полное заявление авторских прав

Copyright (C) The Internet Society (1998). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.