

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№ 5 (84)/2000

Как реагировать на нарушения информационной безопасности

(RFC 2350, ВСП 21)

ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ



Как реагировать на нарушения информационной безопасности (RFC 2350, ВСП 21)

Нэвил Браунли, Эрик Гатмэн

СОДЕРЖАНИЕ

0. Аннотация	3
1. Введение	3
2. Область действия документа	4
2.1. Публикация правил и процедур группы реагирования	
2.2. Взаимоотношения различных групп реагирования	
2.3. Организация защищенных коммуникаций	
3. Информация, правила и процедуры	7
3.1. Получение документа	
3.2. Контактная информация	
3.3. Устав	
3.4. Правила	
3.5. Услуги	
3.6. Формы для доклада о нарушениях	
3.7. Отводы	
4. Литература	12
5. Адреса авторов	12
Приложение А. Терминологический словарь.....	12
Приложение В. Полезные ссылки	13
Приложение С. Известные группы реагирования.....	13
Приложение D. План бланка группы реагирования	14
Приложение Е. Пример заполненного бланка с информацией о группе	14

0. Аннотация

Цель настоящего документа — сформулировать ожидания Интернет-сообщества по отношению к группам реагирования на нарушения информационной безопасности (Computer Security Incident Response Teams, CSIRTs). Нет возможности определить набор требований, применимых ко всем группам, однако, можно и нужно перечислить и описать общий перечень тем и аспектов, представляющих интерес с точки зрения потребителей услуг таких групп.

Потребители имеют законное право (и необходимость) досконально понимать правила и процедуры работы «своей» группы реагирования. Один из способов обеспечить подобное понимание — предоставить на рассмотрение пользователям детальную информацию в виде формализованных бланков, заполненных представителями группы. Возможный вид таких бланков и образец их заполнения рассмотрены в приложениях.

1. Введение

Рабочая группа GRIP была создана для разработки документа, формулирующего ожидания Интернет-сообщества по отношению к группам реагирования на нарушения информационной безопасности (Computer Security Incident Response Teams, CSIRTs). Хотя потребность в по-

Группа реагирования должна реагировать на выявленные нарушения безопасности и на угрозы своим подопечным, действуя в интересах конкретного сообщества и способами, принятыми в этом сообществе

добном документе зародилась в широком Интернет-сообществе, сформулированные ожидания должны соответствовать также запросам более ограниченных сообществ.

В прошлом существовало неправильное понимание того, что можно ждать от групп реагирования. Цель настоящего документа — обеспечить основу для представления важных аспектов, касающихся реагирования на нарушения информационной безопасности.

Прежде чем двигаться дальше, необходимо четко уяснить, что понимается под термином «группа реагирования на нарушения информационной безопасности». В рамках настоящего документа мы будем считать, что имеется в виду группа, выполняющая, координирующая и поддерживающая реагирование на нарушения, затрагивающие информационные системы в пределах определенной зоны ответственности (более полное определение имеется в Приложении А). Следовательно, коллектив, называющий себя группой реагирования, должен реагировать на выявленные нарушения безопасности и на угрозы своим подопечным, действуя в интересах конкретного сообщества и способами, принятыми в этом сообществе.

Каждая группа реагирования должна определить круг своих подопечных и опубликовать свои правила, регламенты и порядок доклада о нарушениях.

Важно, чтобы каждый член сообщества понимал, что целесообразно ожидать от своей группы. Поэтому группа реагирования должна объяснить кого она опекает и определить предоставляемые услуги. Кроме того, каждая группа реагирования должна опубликовать свои правила и регламенты. Аналогично, члены сообщества должны знать, что группа реагирования ожидает от них. Это значит, что группа должна также опубликовать порядок доклада о нарушениях.

Brownlee N., Guttman E. Expectations for Computer Security Incident Response. — RFC 2350, BCP 21, 1998.

Перевод с сокращениями.

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 organisations, 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.

Пользователи должны точно знать, как их группа реагирования будет сотрудничать с другими группами и организациями и какая информация будет разделяться.

Мы опишем бланки, которые группы реагирования будут применять для доведения до пользователей описанной выше информации. Несомненно, пользователи могут предполагать, что им будут оказаны услуги, описанные в заполненных бланках.

Необходимо подчеркнуть, что без активного участия пользователей эффективность работы групп реагирования может заметно снизиться. Это особенно верно по отношению к докладам о нарушениях. Как минимум, пользователи должны знать, что о нарушениях информационной безопасности следует сообщать. Должны они знать и о том, как и куда направлять свои доклады.

Источники многих нарушений, затрагивающих внутренние системы, лежат за пределами контролируемого сообщества. С другой стороны, некоторые внутренние нарушения воздействуют на внешние системы. Следовательно, нарушения безопасности затрагивают многие системы и поэтому возможны разные группы реагирования. Расследование подобных инцидентов требует взаимодействия между отдельными системами и группами.

Пользователи должны точно знать, как их группа будет сотрудничать с другими группами и организациями, какая информация будет разделяться.

В оставшейся части документа будет описан набор тем и аспектов, которые группы реагирования должны разъяснить своим пользователям. Однако, мы не пытаемся дать «правильные» ответы, скорее мы поясняем, каково содержание той или иной темы, того или иного аспекта.

Следующий раздел представляет собой обзор трех важных областей:

- публикация информации группой реагирования;
- определение взаимоотношений с другими группами реагирования;
- организация защищенных коммуникаций.

Далее детально описываются все виды информации, которую необходимо знать о «своей» группе реагирования.

Для удобства использования описанная информация представлена в Приложении D в виде набора формализованных бланков. Подобные бланки можно использовать для получения информации о группе реагирования.

Мы надеемся, что по мере прояснения положений настоящего документа будет улучшаться взаимопонимание между сообществом пользователей и группами реагирования.

2. Область действия документа

Взаимодействие между группой реагирования на нарушения информационной безопасности и опекаемым сообществом требует, прежде всего, чтобы члены сообщества понимали правила и процедуры группы. Поскольку в процессе реагирования обычно участвует несколько групп, сообщество должно осознавать взаимосвязи между «своей» и другими группами. Наконец, в большинстве случаев для взаимодействия используется существующая общедоступная инфраструктура, поэтому сообщество должно знать, как в таких условиях организовать защищенное взаимодействие. Каждый из этих аспектов детально описывается в трех следующих пунктах.

2.1. Публикация правил и процедур группы реагирования

Каждый пользователь услуг группы реагирования на нарушения информационной безопасности должен заранее, задолго до возникновения реального инцидента, узнать как можно больше об этих услугах и порядке взаимодействия с группой.

Ясное изложение правил и процедур группы реагирования помогает пользователям понять, как сообщать о нарушениях и какую поддержку после этого ожидать. Поможет ли группа в расследовании инцидента? Поможет ли она избежать подобных нарушений в будущем? Доскональное понимание возможностей группы ре-

Каждый пользователь группы реагирования должен заранее получить как можно больше информации о возможностях, правилах и процедурах группы реагирования на нарушения информационной безопасности.

агирования и, в частности, ограничений в предоставляемых услугах сделает взаимодействие между пользователями и группой более эффективным.

Существуют разные виды групп реагирования. Некоторые опекают весьма широкие сообщества (например, Координационный центр CERT (Computer Emergency Response Team, см. <http://www.cert.org> — прим. перев.) опекает Интернет), у других сообщества более ограничены (например, DFN-CERT (опекает немецкую исследовательскую сеть DFN, см. <http://www.cert.dfn.de> — прим. перев.), CIAC (Computer Incident Advisory Capability, опекает Министерство энергетики США, см. <http://ciac.llnl.gov> — прим. перев.)), у третьих они могут быть совсем узкими (например, коммерческая или корпоративная группа реагирования). Однако, независимо от вида группы, ее пользователи должны знать соответствующие правила и процедуры. Следовательно, данная информация должна быть опубликована и доведена до пользователей.

Группа реагирования должна сообщать всю необходимую информацию о правилах и услугах в форме, отвечающей потребностям пользователей. Важно уяснить, что не все правила и процедуры следует делать общеизвестными. Например, нет необходимости разбираться в деталях внутреннего распорядка группы, чтобы взаимодействовать с ней, сообщать о нарушениях или получать рекомендации по анализу и защите систем.

Каждая группа реагирования должна разместить свои рекомендации и процедуры на своем информационном сервере.

Ранее некоторые группы реагирования выпускали документ с описанием основ своего функционирования, другие предоставляли ответы на часто задаваемые вопросы (FAQ), третьи публиковали официальные статьи и распространяли их на пользовательских конференциях, четвертые рассылали информационные бюллетени.

Мы рекомендуем, чтобы каждая группа реагирования разместила рекомендации и процедуры на своем информационном сервере (например, на Web-сервере). Тем самым пользователи получают свободный доступ к документам, хотя остается проблема поиска «своей» группы; требуется сообразить, что перед Вами группа, услугами которой Вы можете пользоваться.

Можно предположить, что заполненные бланки групп реагирования вскоре можно будет искать с помощью современных поисковых машин. Это поможет в распространении информации о существующих группах и о порядке доступа к их услугам.

Было бы весьма полезно иметь централизованное хранилище, содержащее все заполненные бланки групп реагирования. Пока такого хранилища нет, однако, со временем ситуация может измениться.

Независимо от источника, пользователь должен проверять аутентичность информации о группе. Настоятельно рекомендуется защищать подобные жизненно важные документы цифровой подписью. Это позволит проверить, что бланк на самом деле опубликован определенной группой реагирования и его целостность не была нарушена. (Предполагается, что читатель владеет техникой работы с электронной цифровой подписью.)

2.2. Взаимоотношения различных групп реагирования

В некоторых случаях группа реагирования может эффективно работать сама по себе, в тесном взаимодействии лишь с опекаемым сообществом. Но в условиях современных международных сетей гораздо более вероятно, что в большинство нарушений будут вовлечены третьи стороны. Следовательно, группа реагирования будет нуждаться во взаимодействии с другими группами и организациями за пределами «своего» сообщества.

Пользователи должны осознать природу и уровень этого сотрудничества, поскольку в процессе взаимодействия может быть раскрыта весьма критичная информация об отдельных членах сообщества.

При установлении взаимоотношений между группами реагирования должны быть определены соглашения, существующие между ними.

Межгрупповое взаимодействие может включать в себя получение рекомендаций от других групп, распространение знаний о возникших проблемах, а также совместную работу по ликвидации нарушения, затронувшего одно или несколько опекаемых сообществ.

При установлении взаимоотношений, обеспечивающих подобное взаимодействие, группы должны решить, какого рода соглашения могут существовать между ними (например, как разделяется информация о защите, может ли раскрываться факт существования взаимоотношений, и если может, то перед кем).

Заметим, что имеются различия между партнерским соглашением, когда группы договариваются о совместной работе и разделении информации, и простой кооперацией, когда группа (или любая другая организация) просто обращается к другой группе за помощью или советом.

Хотя установление подобных взаимоотношений весьма важно (оно влияет на возможность обслуживания пользователей), некоторые детали остаются на усмотрение соответствующих групп. Рекомендации по заключению соглашений находятся вне области действия данного документа. Однако, информация, использованная при формулировании ожиданий пользовательского сообщества, касающаяся разделения сведений, поможет всем сторонам понять цели и задачи конкретной группы, облегчит первый контакт.

2.3. Организация защищенных коммуникаций

После того, как одна из сторон решила разделять информацию с другой стороной или две стороны заключили соглашение о разделении информации или совместной работе — как того требует скоординированная реакция на нарушение информационной безопасности — появляется необходимость в защищенных коммуникационных каналах. (В данном контексте термин «защищенный» относится к процессу передачи информации, а не к порядку ее использования сторонами.)

Цели организации защищенных коммуникаций состоят в следующем:

- Обеспечение конфиденциальности: может ли кто-то еще получить доступ к передаваемым данным?
- Целостность: может ли кто-то еще манипулировать передаваемыми данными?
- Аутентичность: общаюсь ли я с «правильным» партнером?

Очень просто послать поддельное электронное письмо, не очень сложно выдать себя за другого в телефонном разговоре. Криптографические технологии, например, Pretty Good Privacy (PGP) или Privacy Enhanced Mail (PEM) могут обеспечить эффективную защиту электронной почты. С помощью соответствующего

оборудования можно защитить телефонные линии. Однако, прежде чем применять подобные средства, обе стороны должны сформировать

**Обеспечение аутентичности
криптографических открытых
и закрытых ключей, используемых
в защищенных коммуникациях,
является важным фактором
эффективной защиты**

«правильную» инфраструктуру, сделать, если можно так выразиться, заготовки на будущее. Наиболее важная заготовка — обеспечение аутентичности криптографических ключей, используемых в защищенных коммуникациях, а именно:

- Открытых ключей (для средств вида PGP и PEM). Поскольку они доступны через Интернет, аутентичность открытых ключей должна быть подтверждена до использования. Например, PGP полагается на «сеть доверия» (когда одни пользователи подписывают ключи других пользователей), а PEM основывается на иерархической организации (когда доверенные центры подписывают ключи пользователей).
- Секретных ключей (для средств вида DES и PGP/conventional encryption). Поскольку эти ключи должны быть известны и отправителю, и получателю, их необходимо сформировать и передать до начала общения по защищенному каналу.

Коммуникации критичны для всех аспектов реагирования. Группа может действовать наилучшим образом, только собрав и систематизировав всю относящуюся к делу информацию. Специфические требования (такие как звонок по определенному номеру для проверки аутентичности ключей) должны быть оговорены с самого начала. Бланки с данными о группе являются стандартным средством доставки подобных сведений.

Технические и административные проблемы защищенных коммуникаций находятся вне области действия настоящего документа. Мы утверждаем лишь, что группа реагирования должна поддерживать и применять какие-либо методы защиты коммуникаций с пользователями и/или другими группами. Какие это методы, какой уровень защиты они обеспечивают — решают соответствующие сообщества.

3. Информация, правила и процедуры

В предыдущем разделе было указано, что правила и процедуры группы реагирования должны быть опубликованы и доведены до пользователей. В данном разделе мы перечислим все виды информации, которую пользователи должны получить от своей группы. Способ доведения этой информации может зависеть от сообщества, равно как и специфическое информационное наполнение. Наша цель — ясно описать различные виды информации, которую сообщество ожидает получить от своей группы реагирования.

Чтобы облегчить понимание тем и аспектов, относящихся к взаимодействию пользователей со «своей» группой, мы предлагаем публиковать всю информацию, правила и процедуры в виде документа, следуя шаблону, приведенному в Приложении D. Шаблон играет организующую роль, облегчая поиск нужных сведений. В приложении E приведен пример заполненных бланков для вымышленного Университета XYZ. Мы не даем конкретных рекомендаций по выбору правил и процедур, однако, в качестве примеров рассматриваются различные варианты. Важнее всего то, что группа должна выработать набор правил, а те, кто взаимодействует с ней, должны иметь возможность получить и понять их.

Разумеется, мы не сможем затронуть все аспекты для всех ситуаций и/или групп. Наш обзор следует рассматривать как рекомендации. Каждая группа может по своему усмотрению включать то, что необходимо для поддержки опекаемого сообщества.

3.1. Получение документа

Детали работы группы со временем изменяются, поэтому заполненные бланки должны содержать дату последнего изменения. Кроме того, должно быть известно, как получать информацию о последующих изменениях. Без этого неизбежно появление со временем непонимания и недоразумений; устаревший документ может принести больше вреда, чем пользы.

- Дата последнего изменения. Ее должно быть достаточно для проверки актуальности сведений.
- Список рассылки. Почтовые списки — удобное средство распространения обновлений среди большого числа пользователей. Группа может решить, использовать ли свой собственный список или положиться на существующий при извещении пользователей о

Пользователи группы реагирования должны своевременно извещаться об изменениях в деталях работы данной группы.

произведенных изменениях. Обычно в список входят коллективы, с которыми группа реагирования активно взаимодействует. Извещения об изменениях должны заверяться электронной подписью группы.

- Расположение документа. Текущая версия документа должна быть доступна в рамках оперативных информационных сервисов группы. В таком случае пользователи смогут легко получить дополнительную информацию о группе, проанализировать недавние изменения. Эта версия также должна быть снабжена электронной подписью.

3.2. Контактная информация

В этом разделе бланков должна быть приведена исчерпывающая контактная информация, хотя ее характер может существенно различаться для разных групп. Например, может быть принято решение о неразглашении имен членов группы. Ниже пояснения приводятся только там, где это необходимо.

- Название группы реагирования.
- Почтовый адрес.
- Часовой пояс. Эта информация полезна при реакции на нарушения, затрагивающие несколько часовых поясов.
- Номер телефона.
- Номер факса.
- Другие способы связи (например, номер в закрытой телефонной сети).
- Адрес электронной почты.
- Открытые ключи и способы шифрования. Использование конкретных механизмов зависит от того, доступны ли партнерам по коммуникациям соответствующие программы, ключи и т.п. Наличие подобной информации дает возможность пользователям определить, могут ли они и каким образом организовать защищенное взаимодействие с группой реагирования.
- Члены группы.
- Часы работы. Должны быть указаны часы работы и расписание на выходные. Имеется ли постоянно действующая горячая линия?

- Дополнительная контактная информация. Существует ли какая-либо контактная информация для специфических пользователей?

Может быть представлена более детальная контактная информация, например, разные способы контакта для разных услуг, список оперативных информационных сервисов и т.п. Если существуют специфические процедуры для доступа к некоторым услугам (например, адреса для обращений к почтовому списку), они должны быть разъяснены в данном разделе.

3.3. Устав

Каждая группа реагирования должна иметь устав, который определяет, что группа должна делать и на каком основании. В уставе должны присутствовать, по крайней мере, следующие разделы:

- виды деятельности;
- клиентура;
- спонсоры и вышестоящие организации;
- полномочия.

3.3.1. Виды деятельности

В данном разделе следует сосредоточиться на основных видах деятельности группы, уже сформулированных в ее определении. Чтобы коллектив мог считаться группой реагирования на нарушения информационной безопасности, он должен поддерживать доклады о нарушениях, а также помогать пользователям, разбираясь с нарушениями.



Цели и задачи группы особенно важны, они должны быть определены ясно, недвусмысленно.

3.3.2. Клиентура

Клиенты (пользователи, опекаемые сообщества) группы реагирования могут быть определены несколькими способами. Например, ими могут быть сотрудники некоторой организации или платные подписчики. Возможно определение в технических терминах, например, как пользователей конкретной операционной системы.

Определение клиентуры должно задать рамки, в пределах которых группа будет предоставлять свои услуги. Раздел описания правил (см. ниже) должен разъяснить, как будут обрабатываться запросы, поступившие извне.

Если группа решает не раскрывать своих пользователей, она должна объяснить причины подобного решения. Например, коммерческие группы не будут перечислять своих клиентов, но укажут, что они предоставляют услуги большой группе пользователей, имена которых не разглашаются по условиям контрактов.

Сообщества пользователей могут перекрываться. Например, поставщик Интернет-услуг может обеспечивать реагирование для своих потребителей, возможно, имеющих собственные группы. В разделе «Полномочия» (см. ниже) подобные взаимосвязи необходимо разъяснить.

3.3.3. Организации-спонсоры и вышестоящие организации

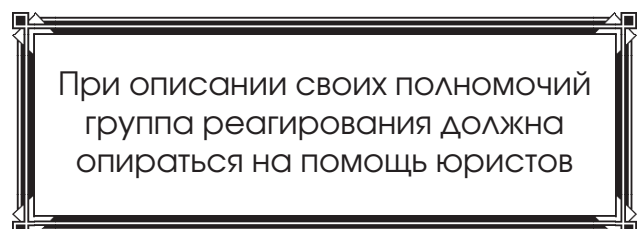
В этом разделе указываются организации, наделяющие группу полномочиями. Эти сведения помогут пользователям выяснить «корни», «крышу» и возможности группы, что необходимо для формирования доверительных отношений с клиентами.

3.3.4. Полномочия

Этот раздел существенно зависит от специфики группы, основанной на взаимоотношениях с пользователями. Например, полномочия корпоративной группы определяются руководством, общественная группа может поддерживаться и выбираться на началах самоуправления и играть консультативную роль и т.п.

Группа может иметь или не иметь полномочия на вмешательство в работу всех систем в пределах контролируемого периметра. Иными словами, область управления, вообще говоря, отличается от круга пользователей. В других случаях область управления может быть устроена иерархически, и тогда этот факт нужно зафиксировать с указанием подчиненных групп.

Описание полномочий группы может сделать ее уязвимой для судебных исков, поэтому в данном вопросе группа должна опираться на помощь юристов (см. также пункт 3.7, где юридические аспекты рассматриваются более подробно).



3.4. Правила

Критически важно, чтобы группа реагирования определила свои правила. В следующем пункте обсуждается доведение этих правил до пользователей.

3.4.1. Типы нарушений и уровень поддержки

В данном разделе должны быть перечислены типы нарушений, на которые группа способна реагировать, а также уровень поддержки, предоставляемой для каждого из заданных типов. В разделе «Услуги» (см. ниже) может быть помещено более детальное описание, а также затронуты темы, не имеющие прямого отношения к нарушениям.

Уровень поддержки пользователей может меняться в зависимости от многих факторов, которые должны быть описаны и разъяснены.

Уровень поддержки может меняться в зависимости от таких факторов, как загруженность группы и полнота доступной информации. Подобные факторы должны быть описаны, а их влияние разъяснено. Поскольку список известных типов нарушений будет неполон по отношению ко всем возможным или будущим инцидентам, должна быть описана поддержка для «прочих» нарушений.

Следует определить, будет ли группа действовать на основе получаемой информации о слабостях, которые делают возможными будущие нарушения. Согласие учитывать такую информацию в интересах своих пользователей рассматривается как дополнительная профилактическая услуга, а не как обязательный сервис группы реагирования.

3.4.2. Кооперация, взаимодействие и раскрытие информации

В этом разделе необходимо разъяснить, с какими родственными группами налажено взаимодействие. Подобное взаимодействие не обязательно происходит в рамках реагирования на нарушение, оно может быть направлено для укрепления сотрудничества в технических вопросах или услугах. Вовсе не обязательно приводить детали договоров о сотрудничестве; главная цель раздела состоит в том, чтобы дать пользователям общее понимание о существующих видах взаимодействия и их целях.

Принятие определенных соглашений между группами реагирования приводит к упрощению межгруппового сотрудничества.

Правила докладов и раскрытия информации должны разъяснять, кто и в каких случаях может являться получателем докладов группы. В них должно быть указано, ожидается ли работа силами другой группы или непосредственное взаимодействие с членом другого сообщества по вопросам, касающимся именно этого пользователя.

Организации, с которыми может осуществляться взаимодействие, перечислены ниже.

3.4.2.1. Группы реагирования

Необходимость взаимодействия с другими группами реагирования возникает часто. Например, корпоративная группа докладывает о нарушении национальной группе, которая, в свою очередь, передает доклад в другие страны, чтобы охватить все информационные системы, ставшие жертвами широкомасштабной атаки.

Сотрудничество между группами реагирования может привести к раскрытию информации. Ниже приводятся примеры подобного раскрытия, однако, список, разумеется, не претендует на полноту:

- Доклад о внутренних нарушениях, направленный другим группам. При этом могут стать общедоступными (в частности, доступными для прессы) сведения об информационной системе организации.
- Реагирование на внутренние нарушения, доклад о которых пришел извне (это означает, что утечка информации уже произошла).
- Доклад о наблюдениях в пределах контролируемых границ, указывающих на предполагаемые или подтвержденные внешние нарушения.
- Реагирование на основании докладов о внешних нарушениях.
- Передача информации об уязвимостях поставщикам, партнерским группам или непосредственно затронутым организациям, входящим или нет в число пользователей.
- Отклик на сообщения о нарушениях или уязвимостях.
- Предоставление контактной информации о пользователях, членах других сообществ, других группах, правоохранительных органах.

3.4.2.2. Поставщики

У некоторых поставщиков есть свои группы реагирования, а других нет. В последнем случае группа должна работать непосредственно с поставщиком, чтобы предложить улучшения или изменения, проанализировать техническую проблему или протестировать предлагаемые решения. Если продукты поставщика оказываются вовлеченными в нарушение, этот поставщик играет особую роль в реагировании.

3.4.2.3. Правоохранительные органы

Группы реагирования и пользователи должны соблюдать действующее законодательство, которое может существенно различаться в разных странах. Группа реагирования может давать рекомендации по техническим деталям атаки или запрашивать совета по правовым последствиям нарушения. В законодательстве могут содержаться специфические требования к представлению докладов и соблюдению конфиденциальности.

3.4.2.4. Пресса

Время от времени от прессы могут поступать запросы на информацию и комментарии.

Явные правила, касающиеся передачи информации в прессу, были бы весьма полезны, особенно в плане прояснения ожиданий пользователей. Эти правила должны разъяснять все вопросы как можно подробнее, поскольку обычно пользователи весьма болезненно воспринимают контакты с прессой.

3.4.2.5. Прочее

В этом разделе речь может идти об исследовательских работах или о взаимодействии с организацией-спонсором.

Подразумеваемый статус любой информации, получаемой группой и имеющей отношение к информационной безопасности, — «конфиденциально», однако, строгое следование этому положению превращает группу в информационную «черную дыру», что может уменьшить ее привлекательность как партнера для пользователей и других организаций. Необходимо определить, какая информация докладывается или раскрывается, кому и когда.

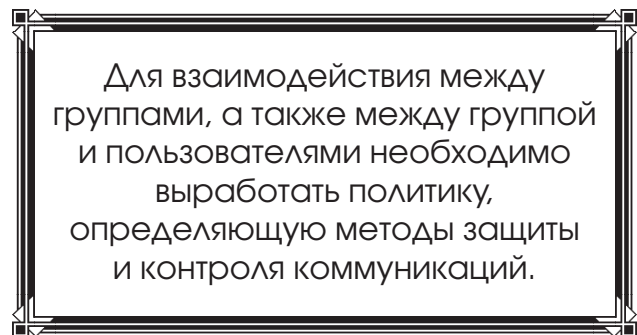
Возможно, разные группы будут являться субъектами разного законодательства, требующего или, напротив, ограничивающего раскрытия информации, особенно, если речь идет о группах из разных стран. Кроме того, группы могут руководствоваться требованиями на доклады, налагаемыми спонсорскими организациями. В сведениях о группе все такие ограничения должны быть специфицированы, чтобы прояснить ситуацию для пользователей и других групп.

Раскрытию информации может препятствовать также конфликт интересов, особенно коммерческих; мы не даем рекомендаций по разрешению такого рода конфликтов.

Обычно группы накапливают статистическую информацию. Если такая информация распространяется, в политике докладов и раскрытия сведений это должно быть явно оговорено, как и то, каким образом статистическую информацию можно получить.

3.4.3. Коммуникации и аутентификация

Необходимо иметь политику, определяющую методы защиты и контроля коммуникаций. Это необходимо как для взаимодействия между группами, так и между группой и пользователями. В бланках должны быть приведены открытые ключи или ссылки на них, ключевые отпечатки, а также указания, как использовать эту информацию для проверки аутентичности и что делать с поврежденной информацией (например, куда сообщать о повреждениях).



В настоящее время рекомендуется, чтобы каждая группа имела, как минимум, ключ PGP (если это возможно). Могут использоваться также и другие механизмы (например, PEM, MOSS, S/MIME), если это помогает группе или пользователям. Заметим, однако, что группы и пользователи должны соблюдать местное законодательство. В некоторых странах сильная криптография находится под запретом, либо на использование криптографических технологий налагаются специфические ограничения. В дополнение к максимально полному шифрованию критичной информации, ее следует снабжать цифровой подписью. (Отметим, что в большинстве стран защита аутентичности посредством электронной подписи не подпадает под действие криптографического законодательства.)

Если связь осуществляется по телефону или факсу, с потенциальными партнерами могут быть заранее согласованы секретные аутентификационные данные, такие как парольные слова или фразы. Очевидно, эти секретные данные не должны публиковаться, хотя факт их существования может быть обнаружен.

3.5. Услуги

Услуги, оказываемые группой реагирования, можно грубо разделить на две категории: действия в реальном времени, непосредственно связанные с главной задачей — реагированием на нарушения, и профилактические действия, играющие вспомогательную роль и осуществляемые не в реальном масштабе времени. Вторая категория и часть первой состоит из услуг, которые являются дополнительными в том смысле, что их предлагают не все группы реагирования.

3.5.1. Реагирование на нарушения

Реагирование на нарушения обычно включает оценку входящих докладов («классификация нарушений») и работу над поступившей информацией вместе с другими группами, поставщиками Интернет-услуг и иными организациями («координация реагирования»). Третья группа услуг, помощь локальным пользователям в восстановлении нормальной работы после нарушения («разрешение проблем») обычно состоит из дополнительных сервисов, предоставляемых лишь частью групп.

3.5.1.1. Классификация нарушений

Классификация нарушений обычно включает в себя следующие действия:

- Оценка докладов. Входящая информация интерпретируется, классифицируется по степени важности, соотносится с продолжающимися событиями и выявляемыми тенденциями.
- Верификация. Определяется, действительно ли имеет место нарушение и каковы его масштабы.

3.5.1.2. Координация реагирования

Под координацией реагирования обычно понимается:

- Категорирование информации. Информация, относящаяся к нарушению (регистрационные журналы, контактная информация и т.д.) категоризируется в соответствии с политикой раскрытия сведений.
- Координация. В соответствии с политикой раскрытия сведений о нарушении извещаются другие стороны.

3.5.1.3. Разрешение проблем

Услуги по разрешению проблем, обычно являющиеся дополнительными, включают в себя следующие действия:

- Техническая поддержка (например, анализ «взломанных» систем).
- Искоренение проблем. Устранение причин нарушения (использованных уязвимостей)

и его проявлений (например, прерывание сеанса пользователя-нарушителя).

- Восстановление. Помощь в возвращении систем и услуг к состоянию до нарушения безопасности.

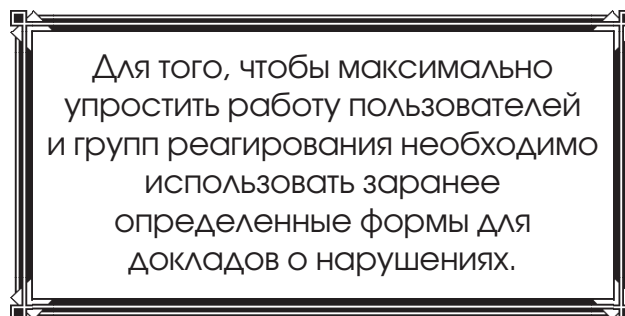
3.5.2. Профилактические действия

Обычно соответствующие услуги являются дополнительными. В них входят:

- Предоставление информации. Под этим понимается поддержка архива известных уязвимостей, заплат, способов разрешения прошлых проблем или организация списков рассылки с рекомендательными целями.
- Предоставление средств безопасности (например, средств аудита).
- Обучение и подготовка кадров.
- Оценка продуктов.
- Оценка защищенности организации, консультационные услуги.

3.6. Формы для доклада о нарушениях

Использование форм для докладов о нарушениях упрощает работу как пользователей, так и групп реагирования. Пользователи могут подготовить ответы на некоторые важные вопросы заранее, в спокойной обстановке. Группа сразу, в первом сообщении, получает всю необходимую информацию, что закладывает основу эффективного реагирования.



В зависимости от целей и набора услуг конкретной группы, может использоваться несколько форм. Например, форма для сообщения о новой уязвимости может существенно отличаться от формы доклада о нарушении.

Лучше всего предоставлять формы в рамках онлайн-овых информационных услуг группы. Точные ссылки на них должны присутствовать в документах, описывающих группу, вместе с описанием правил пользования и руководством по порядку работы с формами. Если для «докладов по форме» поддерживаются отдельные адреса электронной почты, они также должны быть указаны.

Одним из примеров подобной формы является форма для доклада о нарушениях координационного центра CERT:
ftp://info.cert.org/incident_reporting_form.

3.7. Отводы

Несмотря на то, что документы, описывающие группу реагирования, не являются контрактом, возможность последующих судебных санкций может вытекать из описания услуг и целей. По этой причине рекомендуется размещать в конце бланков соответствующих отвод (письменный отказ), предупреждающий пользователей о возможных ограничениях.

В ситуациях, когда оригинальная версия документа должна переводиться на другой язык, в переводе должен присутствовать соответствующий отвод и ссылка на оригинал. Пример:

«Хотя мы стремились аккуратно перевести первоначальный документ с немецкого на английский, мы не можем быть уверены, что оба документа выражают идентичные мысли на одном уровне детализации и корректности. Во всех случаях, когда между двумя версиями возникают различия, превалирует версия на немецком языке.»

Использование отводов и обеспечиваемая ими защита определяется действующим законодательством, которое группа должна знать. В сомнительных случаях следует посоветоваться с юристом.

4. 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.

5. 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

Приложение А. Терминологический словарь

В данном словаре определяются термины, используемые при описании нарушений безо-

пасности и групп реагирования. Включен ограниченный набор терминов. Другие определения можно найти в иных источниках, например, в словаре пользователя Интернет (Internet User's Glossary [RFC 1983]).

- **Опекаемое сообщество.** Деятельность группы реагирования предполагает существование опекаемого сообщества — группы пользователей, систем, сетей или организаций, обслуживаемых группой. Чтобы деятельность группы была эффективной, она должна признаваться опекаемым сообществом.
- **Нарушение безопасности.** В рамках данного документа этот термин является синонимом нарушения информационной безопасности — любого враждебного проявления, компрометирующего некоторые аспекты безопасности систем и/или сетей.

Определение нарушения в разных организациях может различаться, однако, общепринятыми признаются, по крайней мере, следующие категории:

- потеря конфиденциальности информации;
- нарушение целостности информации;
- нарушение доступности информационных услуг;
- неправомерное использование услуг, систем или информации;
- повреждение систем.

Это весьма общие категории. Например, замещение системной утилиты троянской программой служит примером нарушения целостности, а успешная атака на пароли — пример потери конфиденциальности. Атаки, даже если они оказались неудачными из-за правильно построенной защиты, могут трактоваться как нарушения.

В определении нарушения используется термин «компрометация». Иногда администратор может лишь «подозревать» нарушение. В процессе реагирования необходимо установить, действительно ли нарушение имело место.

- **Группа реагирования на нарушения информационной безопасности.** В соответствии с двумя данными выше определениями, группа реагирования координирует и поддерживает ответ на нарушения безопасности, затрагивающие опекаемое сообщество.

Чтобы считаться группой реагирования, необходимо:

- предоставлять (защищенный) канал для приема сообщений о предполагаемых нарушениях;
- предоставлять помощь членам опекаемого сообщества в ликвидации нарушений;

- распространять информацию, относящуюся к нарушению, в пределах опекаемого сообщества и другим заинтересованным сторонам.

Заметим, что здесь мы не имеем в виду правоохранительные органы, расследующие компьютерные преступления. На самом деле, членам группы достаточно прав, которыми располагают обычные граждане.

- Поставщик. Поставщик предоставляет продукты сетевых или вычислительных технологий и отвечает за их техническое содержание. Примерами продуктов служат аппаратное (настольные компьютеры, маршрутизаторы, коммутаторы и т.д.) и программное обеспечение (операционные системы, почтовые системы и т.п.).

Отметим, что продавец технологического продукта не обязательно является его поставщиком. Например, Интернет-провайдер может продавать своим пользователям маршрутизаторы, но поставщиком остается производитель, так как именно он, а не Интернет-провайдер, отвечает за техническое содержание маршрутизатора.

- Уязвимость. Это характеристика технологического фрагмента, которая может быть использована для осуществления нарушения безопасности. Например, если программа непреднамеренно позволяет обычным пользователям выполнять произвольные команды операционной системы в привилегированном режиме, то такая «особенность» является уязвимостью.

Приложение В. Полезные ссылки

Важные аспекты реагирования на нарушения безопасности на уровне организации описаны в «Руководстве по информационной безопасности предприятия» ([RFC 2196], см. также Jet Info, 1996, 11-12). Этот документ будет обновляться Рабочей группой Site Security Handbook (SSH), в него войдут рекомендации для местных правил и процедур, в первую очередь, помогающие избежать нарушений безопасности.

Другие документы, интересные в связи с обсуждением деятельности групп реагирования и стоящих перед ними задач, доступны по анонимному FTP. Подборки можно найти по адресу:

- <ftp://ftp.cert.dfn.de/pub/docs/csir/>. В файле 01-README содержатся сведения о содержимом данного каталога.

Другие особенно интересные в обсуждаемом контексте документы:

- <ftp://ftp.nic.surfnet.nl/surfnet/net-security/cert-nl/docs/reports/R-92-01>. Этот доклад содержит изложения основ функционирования CERT-NL, группы реагирования поставщика сетевых услуг из Нидерландов SURFnet.
- Интересующиеся деятельностью Форума групп безопасности и реагирования на нарушения FIRST (Forum of Incident Response and Security Teams) найдут дополнительную информацию в Приложении С.
- <http://hightop.nrl.navy.mil/news/incident.html>. Документ содержит ссылку на Справочник по реагированию на нарушения (NRL Incident Response Manual).
- <http://www.cert.dfn.de/eng/team/kpk/cert-bib.html>. Документ содержит аннотированную библиографию по деятельности групп реагирования со ссылками на многие материалы.
- ftp://info.cert.org/incident_reporting_form. Форма доклада о нарушениях, предоставляемая координационным центром CERT для сбора сведений о нарушениях и для устранения задержек, вызванных необходимостью запроса более детальной информации.
- <http://www.cert.org/cert.faqintro.html>. Подборка ответов на часто задаваемые вопросы, подготовленная координационным центром CERT.

Приложение С. Известные группы реагирования

В настоящее время имеется много различных групп реагирования, но нет единого источника, где все они были бы перечислены. Большинство заметных и давно созданных групп (первая группа была организована в 1988 году) являются теперь членами всемирного форума FIRST (Forum of Incident Response and Security Teams). В момент написания данного документа в FIRST входило более 55 групп (1 из Австралии, 13 из Европы, все остальные из Северной Америки). Информацию о FIRST можно найти по адресу:

- <http://www.first.org/>

Текущий список членов Форума вместе с контактной информацией и дополнительными сведениями, предоставляемыми отдельными группами, можно найти по адресу:

- <http://www.first.org/team-info/>

Группы, желающие присоединиться к Форуму, должны помнить, что для представления им нужен спонсор — группа, уже являющаяся полноправным членом FIRST. Дополнительную информацию можно найти по следующим адресам:

- http://www.first.org/about/op_frame.html. Изложения основ функционирования FIRST.
- <http://www.first.org/docs/newmem.html>. Руководство для групп, желающих присоединиться к Форуму.

Многие европейские группы, независимо от членства в FIRST, перечислены по странам на странице, поддерживаемой немецкой группой реагирования:

- <http://www.cert.dfn.de/eng/csir/europe/certs.html>

При поиске подходящей группы реагирования целесообразно обратиться в известную группу или к Интернет-провайдеру.

Приложение D. План бланка группы реагирования

В приведенном ниже плане в предельно сжатой форме перечислены вопросы, рассматриваемые в данном документе. План определяет рекомендуемый шаблон для описания группы реагирования, структура которого спроектирована так, чтобы облегчить передачу правил и процедур группы, а также иной информации о группе опекаемому сообществу и внешним организациям, например, другим группам. Пример заполненного бланка приведен в Приложении E.

1. Информация о документе

- 1.1. Дата последнего изменения
- 1.2. Список рассылки уведомлений
- 1.3. Расположение документа

2. Контактная информация

- 2.1. Название группы
- 2.2. Адрес
- 2.3. Часовой пояс
- 2.4. Номер телефона
- 2.5. Номер факса
- 2.6. Другие способы связи
- 2.7. Адрес электронной почты
- 2.8. Открытые ключи и способы шифрования
- 2.9. Члены группы
- 2.10. Прочая информация
- 2.11. Точки пользовательских контактов

3. Устав

- 3.1. Виды деятельности
- 3.2. Клиентура
- 3.3. Спонсоры и вышестоящие организации
- 3.4. Полномочия

4. Правила

- 4.1. Типы нарушений и уровень поддержки
- 4.2. Кооперация, взаимодействие и раскрытие информации
- 4.3. Коммуникации и аутентификация

5. Услуги

- 5.1. Реагирование на нарушения
 - 5.1.1. Классификация нарушений
 - 5.1.2. Координация реагирования
 - 5.1.3. Разрешение проблем
- 5.2. Профилактические действия

6. Формы для доклада о нарушениях

7. Отводы

Приложение E. Пример заполненного бланка с информацией о группе

Ниже приведен пример заполненного бланка с информацией о вымышленной группе реагирования XYZ-CSIRT. Подчеркнем, что это всего лишь пример, он не отражает предпочтений рабочей группы или IETF в плане правил и процедур. Разумеется, группы вольны использовать приведенный текст полностью или частично, это ни в коем случае не навязывается; более того, это не всегда уместно.

Описание группы реагирования XYZ-CSIRT

1. Информация о документе

1.1. Дата последнего изменения

Это версия 1.01, опубликованная 31/03/1997.

1.2. Список рассылки уведомлений

Уведомления об изменениях распространяются через наш список рассылки <xyz-cert-info@xyz-univ.ca>. Запросы на включение в список следует направлять на имя Majordomo в <xyz-cert-info@xyz-univ.ca>; тело сообщения должно состоять из слова «subscribe». Поставьте вместо него слово «help», если Вы не знаете, как работать с администратором списка Majordomo. Данный список рассылки модерируется.

1.3. Расположение документа

Текущая версия данного описания доступна через Web-сервер группы XYZ-CERT; соответствующий URL имеет вид:

<http://www.xyz-univ.ca/xyz-cert/english/CSIRT-descr.txt>

Une version française de ce document est également disponible:

<http://www.xyz-univ.ca/xyz-cert/francais/CSIRT-descr.txt>

Пожалуйста, убедитесь, что Вы используете последнюю версию.

1.4. Аутентификация документа

И английская, и французская версии данного документа подписаны PGP-ключом группы XYZ-CERT. Подписи также расположены на нашем Web-сервере:

<http://www.xyz-univ.ca/xyz-cert/english/CSIRT-descr.asc> <http://www.xyz-univ.ca/xyz-cert/francais/CSIRT-descr.asc>

2. Контактная информация

2.1. Название группы

«XYZ-CERT»: группа реагирования на нарушения информационной безопасности университета XYZ.

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. Номер телефона

+1 234 567 7890 (спросить XYZ-CERT).

2.5. Номер факса

+1 234 567 7899 (это НЕ защищенный факс).

2.6. Другие способы связи

Нет.

2.7. Адрес электронной почты

<xyz-cert@xyz-univ.ca>. Это почтовый алиас, перенаправляющий почту дежурным по группе XYZ-CERT.

2.8. Открытые ключи и способы шифрования

У группы XYZ-CERT есть PGP-ключ, его KeyID есть 12345678, а отпечаток -

11 22 33 44 55 66 77 88 88 77 66 55 44 33 22 11.

Ключ и его подписи можно найти на обычных общедоступных ключевых серверах.

Поскольку PGP до сих пор остается сравнительно новой технологией для университета XYZ, у ключа пока относительно немного подписей; прилагаются усилия, чтобы увеличить число ссылок на этот ключ из «сети доверия» PGP. Тем временем, поскольку в большинстве дружественных университетов Квебека есть хотя бы один сотрудник, знающий координатора группы XYZ-CERT Зо До, Зо До подписал ключ группы и

будет счастлив заверить его отпечаток своим ключом для всех желающих.

2.9. Члены группы

Зо До из отдела компьютерных услуг — координатор группы XYZ-CERT. Контактную информацию о других координаторах и членах группы вместе с описанием курируемых ими областей можно найти на сервере группы:

<http://www.xyz-univ.ca/xyz-cert/teamlist.html>

Управление, связь, контроль осуществляет Стив Три, заместитель директора по техническим вопросам отдела компьютерных услуг.

2.10. Прочая информация

Общую информация о группе XYZ-CERT, а также ссылки на различные рекомендуемые ресурсы по информационной безопасности можно найти по адресу:

<http://www.xyz-univ.ca/xyz-cert/index.html>

2.11. Точки пользовательских контактов

Предпочтительным способом обращения в группу XYZ-CERT является электронная почта. Адрес — <xyz-cert@xyz-univ.ca>. Сообщение, посланное по данному адресу, будет немедленно переадресовано дежурному специалисту. Если Вам нужна срочная помощь, поместите в поле subject слово «urgent».

Если по каким-либо причинам (например, по соображениям безопасности) использовать электронную почту невозможно, в XYZ-CERT можно обратиться по телефону (в рабочее время). Сообщения, оставленные на автоответчике, проверяются реже, чем почтовые.

Рабочее время группы XYZ-CERT ограничено обычными рамками: 09:00 — 17:00, с понедельника по пятницу, кроме праздников.

По возможности, при представлении доклада, используйте, пожалуйста, форму, упомянутую в разделе 6.

3. Устав

3.1. Виды деятельности

Целью группы XYZ-CERT является помощь сотрудникам университета XYZ в реализации профилактических мер, снижающих риск нарушений информационной безопасности и помощь в реагировании на такие нарушения, когда они все-таки происходят.

3.2. Клиентура

Опекаемое сообщество группы XYZ-CERT — сотрудники, студенты и аспиранты университета XYZ. Это определено в политике университета по отношению к вычислительным ресурсам, с которой можно ознакомиться по адресу <http://www-comperv.xyz-univ.ca/policies/pcf.html>

Подчеркнем, однако, что услуги группы распространяются только на производственные системы.

3.3. Спонсоры и вышестоящие организации

Спонсором группы XYZ-CERT является ACME Canadian Research Network, выступающая в Канаде и США в качестве вышестоящей организации для различных университетских групп реагирования, если они того пожелают.

3.4. Полномочия

Группа XYZ-CERT работает под покровительством и с полномочиями, делегированными отделом компьютерных услуг университета XYZ. Информацию о полномочиях этого отдела можно найти в политике университета по отношению к вычислительным ресурсам, см. <http://www-comp.serv.xyz-univ.ca/policies/pcf.html>

Ожидается, что группа XYZ-CERT работает во взаимодействии с системными администраторами и пользователями университета XYZ и, по возможности, избегает авторитарных отношений. Однако, под давлением обстоятельств, члены группы могут обратиться в отдел компьютерных услуг, чтобы при необходимости прямо или косвенно «употребить власть». Все члены группы XYZ-CERT входят в комитет системных администраторов и имеют все права и обязанности, полагающиеся администраторам в соответствии с политикой по отношению к вычислительным ресурсам, либо входят в руководящий состав университета.

Члены университетского сообщества, желающие обжаловать действия группы XYZ-CERT, должны обратиться к заместителю директора по техническим вопросам отдела компьютерных услуг. Если это не помогает, можно обратиться к директору отдела компьютерных услуг (в случае неверного понимания существующей политики) или в университетское бюро прав и обязанностей (в случае ошибочного применения существующей политики).

4. Правила

4.1. Типы нарушений и уровень поддержки

Группа XYZ-CERT уполномочена заниматься всеми видами нарушений безопасности, а также угрозами нарушений в университете XYZ.

Уровень поддержки, предоставляемой группой XYZ-CERT, зависит от типа и серьезности нападения, типа опекаемого сообщества, числа пострадавших, а также от количества наличных ресурсов, хотя в любом случае некоторый ресурс в течение рабочего дня будет выделен. Ресурсы выделяются в соответствии со следующими приоритетами, перечисленными по убыванию:

- угрозы физической безопасности людей;
- атаки на уровне суперпользователя или системном уровне на любую административную информационную систему или часть инфраструктуры магистральной сети;
- атаки на уровне суперпользователя или системном уровне на любую машину, предоставляющую крупный сервис, многопользовательский или специализированный;
- компрометация конфиденциальных счетов пользователей на сервисах ограниченного доступа или компрометация установок программного обеспечения, особенно тех, что используются администраторами и приложениями, работающими с конфиденциальными данными;
- атака на доступность сервисов, перечисленных в предыдущем пункте;
- любое из перечисленных выше нападений, направленных на другие системы и исходящих из университета XYZ;
- масштабные атаки любого типа, например, перехват пакетов, атаки в IRC путем морально-психологического воздействия, атаки на пароли;
- угрозы, причинение беспокойства и другие противоправные действия, направленные на отдельных пользователей;
- компрометация отдельных счетов пользователей в многопользовательских системах;
- компрометация настольных систем;
- подделка, неправильное представление и другие относящиеся к безопасности нарушения местных правил, например, подделка новостей и электронной почты, несанкционированное использование роботов IRC;
- атака на доступность отдельных счетов пользователей, например, применение почтовых бомб.

Типы нарушений, не перечисленные выше, получают приоритет в соответствии со своей наблюдаемой серьезностью и масштабом.

Отметим, что непосредственная помощь конечным пользователям не предоставляется; предполагается, что они будут взаимодействовать со своим системным или сетевым администратором или уполномоченным по отделу. С этими сотрудниками группа XYZ-CERT и будет работать.

В группе XYZ-CERT понимают, что уровень системных администраторов в университете XYZ может быть существенно разным. Группа XYZ-CERT будет стремиться предоставлять информацию и помощь в форме, понятной всем. Тем не менее, несмотря на эти обстоятельства, группа XYZ-CERT не может повышать квалификацию администраторов «на лету», равно как и администрировать системы вместо них. В боль-

шинстве случаев группа предоставляет ссылки на информацию, необходимую для принятия соответствующих мер.

Группа XYZ-CERT стремится информировать системных администраторов университета XYZ о потенциальных уязвимостях, по возможности до того, как их используют для нападений.

4.2. Кооперация, взаимодействие и раскрытие информации

Несмотря на то, что существуют законодательные и этические ограничения на раскрытие информации группой XYZ-CERT (многие из этих ограничений упомянуты в политике университета по отношению к вычислительным ресурсам; безусловно, все они будут соблюдаться), группа подтверждает свою приверженность духу сотрудничества, создавшему Интернет. Поэтому, принимая необходимые меры для сокрытия личной информации членов опекаемого сообщества и организаций-партнеров, группа XYZ-CERT будет по возможности свободно разделять информацию, если это целесообразно с точки зрения отражения или предупреждения нападений.

В тексте ниже под «пострадавшими сторонами» понимаются законные владельцы, операторы и пользователи соответствующих вычислительных систем. В этот круг не входят неавторизованные пользователи, а также авторизованные пользователи, работающие с вычислительными системами неавторизованным образом; такие злоумышленники не могут рассчитывать на сохранение конфиденциальности группой XYZ-CERT. Они могут иметь или не иметь законных прав на конфиденциальность; если такие права существуют, они, конечно, будут соблюдаться.

Информация, которая, возможно, будет распространяться, классифицируется следующим образом:

- Персональные данные пользователей. Это информация о конкретных пользователях или, в некоторых случаях, о конкретных приложениях, которая должна считаться конфиденциальной по юридическим, контрактным и/или этическим причинам.

Персональные данные пользователей не будут раскрываться в узнаваемой форме за пределами группы XYZ-CERT; исключения оговорены ниже. Если личность пользователя скрыта, информация может распространяться свободно (например, чтобы показать файл .cshrc, модифицированный злоумышленником, или продемонстрировать конкретную морально-психологическую атаку).

- Информация о злоумышленнике аналогична персональным данным пользователя, но относится к злоумышленнику.

Хотя информация о злоумышленнике (в частности, идентифицирующие данные) не будет превращаться в общедоступную (если только она уже не стала достоянием обществу, например, по причине возбуждения судебного преследования), ее будут свободно пересылать системным администраторам и группам реагирования, прослеживающим нарушение.

- Информация о частной системе есть техническая информация о конкретных системах или организациях.

Она не будет разглашаться без согласия соответствующих организаций. Исключения оговорены ниже.

- Информация об уязвимостях есть техническая информация об уязвимостях или атаках, включая исправления и сопутствующие меры.

Информация об уязвимостях будет распространяться свободно, хотя и будут прилагаться все усилия, чтобы соответствующий поставщик получил ее раньше других.

- Информация, бросающая тень. Под этим понимается сообщение о том, что нарушение имело место, а также сведения о его масштабе или серьезности. Информация, бросающая тень, может относиться к информационной системе или конкретному пользователю, или группе пользователей.

Информация, бросающая тень, не будет распространяться без разрешения соответствующих организаций или пользователей. Исключения оговорены ниже.

- Статистическая информация есть информация, бросающая тень, с удаленными идентифицирующими данными.

Статистическая информация будет распространяться по усмотрению отдела компьютерных услуг.

- Контактная информация позволяет обратиться к системным администраторам и группам реагирования.

Контактная информация будет распространяться свободно, если только контактное лицо или организация не попросит об обратном, или если группа XYZ-CERT не решит, что такое распространение вызовет недоверие.

Потенциальные получатели информации от группы XYZ-CERT классифицируются следующим образом:

- В силу природы их обязанностей, в том числе по соблюдению конфиденциальности, администраторы университета XYZ имеют право получать всю информацию, необходимую для эффективной реакции на нару-

шения безопасности, затрагивающие вверенные им системы.

- Члены бюро прав и обязанностей уполномочены получать всю запрашиваемую ими информацию, касающуюся нарушений безопасности или смежных вопросов, которые они должны решить. То же верно по отношению к отделу безопасности XYZ, когда возникает необходимость его участия в расследовании или когда расследование начинается по его инициативе.
- Системные администраторы университета XYZ также, в силу возложенных на них обязанностей, допущены к работе с конфиденциальной информацией. Однако, если эти лица не являются членами группы XYZ-CERT, они будут получать только те сведения, которые нужны им для проведения расследования или обеспечения безопасности вверенных им систем.
- Пользователи университетских систем допущены к информации, которая касается безопасности их собственных компьютерных счетов, даже если это означает утечку «информации о злоумышленнике» или «информации, бросающей тень» на другого пользователя. Например, если был скомпрометирован пользовательский счет aaaa и злоумышленник атаковал счет bbbb, пользователь bbbb имеет право знать, что счет aaaa был взломан и как развивалась атака на bbbb. Пользователь bbbb также имеет право запросить и получить информацию о счете aaaa, которая может помочь ему в прослеживании атаки. Например, если bbbb атакован злоумышленником, удаленно подключившимся к aaaa, bbbb должен узнать источник соединения с aaaa, даже если эта информация в обычных условиях считается личной для aaaa. Пользователи университета XYZ имеют право знать о том, что их счета, возможно, скомпрометированы.
- Университетское сообщество не будет получать никакой информации ограниченного распространения, если только стороны, затронутые нарушением, не дадут разрешения на распространение сведений. Статистическая информация может предоставляться обществу. Группа XYZ-CERT не считает себя обязанной информировать общественность о нарушениях, хотя и может делать это; в частности, вероятно, что группа XYZ-CERT сообщит всем заинтересованным сторонам о том, каким образом они были атакованы, или одобрит распространение этими сторонами подобной информации.
- Широкая общественность не получит никакой информации ограниченного распрост-

ранения. На самом деле, к ней не будут обращаться, хотя группа XYZ-CERT понимает, что сведения, сообщенные университетскому сообществу, могут стать всеобщим достоянием.

- Сообщество специалистов по информационной безопасности рассматривается наравне с широкой общественностью. Хотя члены группы XYZ-CERT могут принимать участие в дискуссиях в рамках этого сообщества, например, посредством телеконференций, списков рассылки (включая раскрывающий все детали список «bugtraq») и разного рода конференций, они (члены группы) рассматривают такие форумы как обращение к широкой общественности. Хотя технические вопросы (в том числе уязвимости) могут обсуждаться сколь угодно подробно, все примеры, взятые из опыта группы XYZ-CERT, будут изменены, чтобы сделать невозможной идентификацию затронутых сторон.
 - Пресса также рассматривается как часть широкой общественности. Группа XYZ-CERT не будет вступать в непосредственные контакты с прессой по поводу нарушений безопасности, если только речь не идет о распространении сведений, уже ставших достоянием общественности. При необходимости готовится информация для отдела внешних связей университета XYZ и для группы по связям с заказчиками, входящей в отдел компьютерных услуг. Все запросы по поводу нарушений будут переадресованы в эти две инстанции. Изложенное выше не влияет на право членов группы XYZ-CERT давать интервью по общим вопросам информационной безопасности; на самом деле, такие интервью приветствуются, поскольку они помогают обществу.
 - Другие организации и группы реагирования, являющиеся партнерами в расследовании нарушения безопасности, в некоторых случаях будут допускаться к конфиденциальной информации. При этом добропорядочность внешних организаций будет проверяться, а передаваемая информация будет сводиться к минимуму, полезному для ликвидации нарушения. Вероятнее всего, разделение информации будет происходить с организациями, хорошо известными группе XYZ-CERT (например, несколько университетов провинции Квебек имеют неформальные, но прочные рабочие отношения с университетом XYZ по подобным вопросам).
- Для целей ликвидации нарушений безопасности, полуконфиденциальная, но на самом деле относительно безобидная информация, такая как источник соединения с пользова-

тельским счетом, не будет считаться особенно критичной и может передаваться во внешние организации без чрезмерных предосторожностей. «Информация о злоумышленнике» будет передаваться свободно другим системным администраторам и группам реагирования. «Информация, бросающая тень», будет передаваться, только если есть основания полагать, что она останется конфиденциальной, и если она необходима для ликвидации нарушения.

- Поставщики, как правило, рассматриваются группой XYZ-CERT наравне с внешними группами реагирования. Приветствуется желание поставщиков всех видов сетевого и компьютерного оборудования, программного обеспечения и услуг повышать безопасность своих продуктов. С этой целью поставщикам будет передаваться информация об уязвимостях, обнаруженных в их продуктах, вместе с техническими деталями, позволяющими идентифицировать и ликвидировать проблему. Идентифицирующая информация будет передаваться поставщикам только с разрешения затронутых сторон.
- Правоохранительные органы получают от группы XYZ-CERT всю информацию, необходимую для проведения расследования, в соответствии с политикой по отношению к вычислительным ресурсам.

4.3. Коммуникации и аутентификация

Проанализировав типы информации, с которой имеет дело группа XYZ-CERT, можно сделать вывод, что телефоны без средств шифрования можно считать достаточно безопасными. Нешифрованную электронную почту нельзя считать особенно защищенной, однако, ее можно использовать для передачи данных низкой степени критичности. Если по электронной почте нужно передать критичные данные, будет использоваться PGP. С точки зрения безопасности передача файлов по сети рассматривается наравне с электронной почтой: критичные данные должны шифроваться.

Когда необходимо получить уверенность в подлинности партнера, например, перед началом действий на основе информации, предоставленной группе XYZ-CERT, или перед раскрытием конфиденциальной информации, будет с высокой степенью надежности проверяться его личность и репутация. В пределах университета XYZ и соседних известных организаций для проверки достаточно поручительства известного лица. В иных случаях будут применяться соответствующие методы, такие как поиск среди членов FIRST, использование сервиса WHOIS и другой имеющейся в Интернет регистрационной информации вместе с обратным дозвоном и обращением по электронной почте. Подлинность входящей электронной почты с кри-

тичной информацией будет проверяться вместе с отправителем или с помощью электронной подписи (желательно использование PGP).

5. Услуги

5.1. Реагирование на нарушения

Группа XYZ-CERT помогает системным администраторам в технических и организационных аспектах реагирования на нарушения. В частности, оказывается помощь или даются советы о следующих аспектах реагирования:

5.1.1. Классификация нарушений

- выяснение того, действительно ли имеет место нарушение;
- определение масштаба нарушения.

5.1.2. Координация реагирования

- выяснение первоначальной причины нарушения (использованной уязвимости);
- облегчение контактов с другими системами, возможно, затронутыми нарушением;
- облегчение контактов со службой безопасности университета XYZ и/или правоохранительными органами, если это необходимо;
- предоставление отчетов другим группам реагирования;
- составление уведомлений для пользователей, если это необходимо.

5.1.3. Разрешение проблем

- устранение уязвимостей;
- ликвидация последствий нарушения;
- оценка возможных дополнительных действий с учетом их стоимости и риска (например, исчерпывающее расследование или дисциплинарные действия: сбор улик после нарушения, накопление информации во время инцидента, установка ловушек для злоумышленников и т.п.);
- возможно, сбор улик для судебного преследования или университетских дисциплинарных акций.

Кроме того, группа XYZ-CERT накапливает статистическую информацию о нарушениях, затрагивающих университетское сообщество, и, при необходимости, информирует сообщество, чтобы помочь ему защититься от известных атак.

Чтобы воспользоваться услугами группы XYZ-CERT по реагированию на нарушения, следует направить электронное письмо в соответствии с рекомендациями пункта 2.11 выше. Пожалуйста, помните, что объем оказываемой помощи зависит от параметров, описанных в разделе 4.1.

5.2. Профилактические действия

Группа XYZ-CERT координирует и предоставляет следующие услуги в объеме, возможно, зависящем от наличия ресурсов:

- Информационное обслуживание:
 - Список контактных координат уполномоченных лиц по безопасности в отделах (административных и технических). Эти списки общедоступны по таким каналам, как Web и/или DNS.
 - Списки рассылки для информирования уполномоченных лиц о появлении новой информации, относящейся к их компьютерной среде. Эти списки доступны только для системных администраторов университета XYZ.
 - Хранилище защитных заплат, распространяемых поставщиками или источниками, для различных операционных систем. Это хранилище является общедоступным, если это позволяют лицензионные соглашения. Доступ к нему предоставляется по обычным каналам, таким как Web и/или ftp.
 - Хранилище защитного инструментария и документации для использования системными администраторами. По возможности предоставляются предварительно скомпилированные версии, готовые к установке. Как обычно, доступ предоставляется через Web или ftp.
 - Подготовка выжимок для различных информационных ресурсов, таких как основные списки рассылки и телеконференции. Результирующие выжимки распространяются либо через списки рассылки с ограниченным доступом или через Web, в зависимости от критичности и срочности информации.
- Повышение квалификации:
 - Члены группы XYZ-CERT периодически проводят семинары по различным аспектам информационной безопасности; эти семинары открыты для посещения системными администраторами университета XYZ.
- Аудит безопасности:
 - Проверка целостности основных файлов для Unix-машин, а также для других платформ, способных выполнять «trip-wire».
 - Присвоение уровней безопасности. Машины и подсети в университете XYZ

проверяются на предмет присвоения им уровня безопасности. Информация об уровнях доступна университетскому сообществу, чтобы упростить установку соответствующих прав доступа. Однако, детали анализа безопасности остаются конфиденциальными и доступны только для проверяемых сторон.

- Архивирование:
 - Централизованное протоколирование для машин, поддерживающих удаленное протоколирование в Unix-стиле. Регистрационные журналы автоматически просматриваются анализирующей программой, а события или тенденции, указывающие на потенциальные проблемы безопасности, доводятся до сведения соответствующих системных администраторов.
 - Сохранение записей о нарушениях безопасности. Хотя эти записи остаются конфиденциальными, периодически готовятся и распространяются в рамках университетского сообщества статистические отчеты.

Детальное описание перечисленных выше услуг вместе с инструкциями по присоединению к спискам рассылки, скачиванию информации или получению определенных услуг, таких как централизованное протоколирование или проверка целостности файлов, доступны через Web-сервер группы XYZ-CERT (см. выше раздел 2.10).

6. Формы для доклада о нарушениях

Группа XYZ-CERT пока не разработала специальных форм для доклада о нарушениях. По возможности следует использовать формы координационного центра CERT, см.:

ftp://info.cert.org/incident_reporting_form

7. Отводы

Хотя при подготовке информации, уведомлений и тревожных сообщений будут соблюдаться все возможные предосторожности, группа XYZ-CERT не несет ответственности за ошибки или упущения, равно как и за ущерб, нанесенный в результате использования поступившей от группы информации.

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Издатель: компания Джет Инфо Паблшер

Редактор: Дмитриев В.Ю. (vlad@jet.msk.su)
Технический редактор: Антонов А.Н. (silver@jet.msk.su)
Россия, 103006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
e-mail: JetInfo@jet.msk.su
<http://www.jetinfo.ru>

Подписной индекс по каталогу Роспечати

32555

