



ПОШАГОВОЕ РУКОВОДСТВО ПО СОЗДАНИЮ CSIRT

Включая примеры и контрольные таблицы
в форме проектного плана.

Результат программы WP2006/5.1(CERT-D1/D2)



Содержание

1	О данном руководстве	2
2	Правовое уведомление	2
3	Благодарности	2
4	Введение	3
4.1	ЦЕЛЕВАЯ АУДИТОРИЯ	4
4.2	КАК ИСПОЛЬЗОВАТЬ ДАННЫЙ ДОКУМЕНТ	4
4.3	СОГЛАШЕНИЯ, ИСПОЛЬЗОВАННЫЕ В ДАННОМ ДОКУМЕНТЕ	5
5	Общая стратегия планирования и создания CSIRT	6
5.1	ЧТО ТАКОЕ CSIRT	6
5.2	СЕРВИСЫ, ПРЕДОСТАВЛЯЕМЫЕ CSIRT	10
5.3	АНАЛИЗ ЦЕЛЕВОЙ ГРУППЫ И ЗАЯВЛЕНИЕ О НАМЕРЕНИЯХ	12
6	Разработка бизнес-плана	18
6.1	ОПРЕДЕЛЕНИЕ ФИНАНСОВОЙ МОДЕЛИ	18
6.2	ОПРЕДЕЛЕНИЕ ОРГАНИЗАЦИОННОЙ СТРУКТУРЫ	20
6.3	НАЕМ НУЖНОГО ПЕРСОНАЛА	24
6.4	ИСПОЛЬЗОВАНИЕ ОФИСА И ОБОРУДОВАНИЯ	26
6.5	РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	28
6.6	ПОИСК СОТРУДНИЧЕСТВА С ДРУГИМИ CSIRT И ВОЗМОЖНЫМИ НАЦИОНАЛЬНЫМИ ИНИЦИАТИВАМИ	29
7	Продвижение Бизнес Плана	31
7.1	ОПИСАНИЕ БИЗНЕС ПЛАНОВ И УПРАВЛЕНЧЕСКИХ МЕХАНИЗМОВ	33
8	Примеры операционных и технических процедур (рабочих потоков)	36
8.1	ОЦЕНКА УСТАНОВОЧНОЙ БАЗЫ КЛИЕНТА	37
8.2	СОЗДАНИЕ СИГНАЛОВ ТРЕВОГИ, ПРЕДУПРЕЖДЕНИЙ И ОБЪЯВЛЕНИЙ	38
8.3	ПРОЦЕСС ОБРАБОТКИ ИНЦИДЕНТОВ	45
8.4	ОБРАЗЕЦ ГРАФИКА РЕАГИРОВАНИЯ	51
8.5	ДОСТУПНЫЕ ИНСТРУМЕНТЫ ДЛЯ РАБОТЫ CSIRT	52
9	CSIRT-тренинг	54
9.1	TRANSITS	54
9.2	CERT/CC	55
10	Пример: создание рекомендаций	56
11	Заключение	61
12	Описания плана проекта	62
	ПРИЛОЖЕНИЕ	64
A.1	ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА	64
A.2	СЕРВИСЫ CSIRT	65
A.3	ПРИМЕРЫ	72
A.4	ПРИМЕР МАТЕРИАЛОВ ИЗ КУРСОВ CSIRT	76

1 О данном руководстве

Данный документ детально описывает процесс создания Computer Security and Incident Response Team (CSIRT) с точки зрения управления бизнес-процессом, а также технической перспективы. Данный документ является результатом проделанной работы Европейского Агентства по Сетевой и Информационной Безопасности (ENISA) в рамках программы WP-2006, описанной в главе 5.1:

- Данный документ: *является отчётом о пошаговом процессе создания CSIRT, или схожей с ней структурой, включая пример (CERT-D1)*
- Глава 12: допускает *удобное применение Плана Действий на практике (CERT-D2), за исключением его использования в пронумерованной форме*

2 Правовое уведомление

Данный документ представляет точку зрения и трактовку его авторов и редакторов, до тех пор, пока не заявлено обратное. Данный документ не должен быть интерпретирован как руководство к действию со стороны ENISA или представителей ENISA до тех пор, пока не будет соответственно адаптирован под регуляцию ENISA (EC) No 460/2004. Данный документ не обязательно должен соответствовать последним достижениям и может быть обновлён своевременно.

Информация, представленная третьими сторонами выделена и цитирована соответственно. ENISA не несёт ответственности за информацию внешних источников, включая Интернет-ресурсы, упомянутые в данном документе.

Данный документ предназначен для использования только в образовательных и информационных целях. Ни ENISA, ни кто-либо другой, действующий от её имени не несёт ответственности за использование информации, содержащейся в данном документе.

Все права защищены. Ни одна часть данного документа не может быть скопирована, сохранена или передана в любой форме и любыми методами: электронными, механическими, фотокопированием, записью или каким-либо иными способами:

- без предварительного на то письменного разрешения со стороны ENISA
- в случае явного разрешения со стороны правоохранительных органов
- если существуют условия соглашения, заранее обговоренные с соответствующими организациями.

Источник информации должен быть подтверждён каждый раз. Запросы на копирование данного документа должны быть посланы на адрес указанный ниже.

© European Network and information Security Agency (ENISA), 2006

3 Благодарности

ENISA выражает глубокую благодарность всем организациям и людям, которые внесли вклад в создание данного документа. Особенно мы хотели бы поблагодарить:

- Henk Bronk, консультанта, создавшего первую версию данного документа
- CERT/CC и особенно группу разработчиков CSIRT, написавшую крайне полезные материалы курсов и примеры, представленные в дополнении
- GovCERT.NL за предоставление инструментария CERT
- Группу TRANSITS, предоставившую примеры курсов, представленных в дополнении.
- Наших коллег из Технического Отдела, ответственных за Политику Безопасности и за их особый вклад в написании главы 6.6
- Бесчисленное количество редакторов этого документа

4 Введение

Информационно-коммуникационные системы стали одним из существенных и основных факторов экономического и социального развития. Компьютеры и компьютерные сети используются в настоящее время столь же повсеместно, как электричество или водоснабжение.

Безопасность коммуникационных сетей и информационных систем, особенно их работоспособность и отказоустойчивость, стала крайне актуальной темой для нынешнего общества. Эта тревога объясняется риском появления проблем в ключевых информационных системах, которые могут возникнуть из-за их сложности, склонности к авариям и ошибкам, а также из-за атак на инфраструктуры, предоставляющие критические сервисы для большей части Европейских граждан.

10 марта 2004 было создано Европейское Агентство Сетевой и Информационной Безопасности (ENISA)¹. Целью данного агентства стало обеспечение высокого уровня сетевой и информационной безопасности сообщества, а также разработка концепции сетевой и информационной безопасности для граждан, потребителей, предприятий и организаций государственного сектора Европейского Союза (ЕС), нацеленных на устойчивое функционирование внутреннего рынка.

В течение последних нескольких лет некоторые группы специалистов в области компьютерной безопасности, такие как CERT/CSIRT, Конфликтные комиссии и группы WARP, совместно работали над тем, чтобы сделать Интернет более безопасным. ENISA планирует и дальше поддерживать эти группы в их стремлениях, предоставляя информацию об индикаторах, необходимых для обеспечения качества сервиса соответствующего уровня. Более того, ENISA намеревается повысить свой уровень и начать консультировать государства членов ЕС, а также государственные организации ЕС по вопросам предоставления сервисов безопасности для определенных групп пользователей. Для этого в 2005 году была создана специализированная рабочая группа CERT по взаимодействию и поддержке вопросов предоставления адекватных сервисов безопасности («сервисы CERT») для специфических пользователей.

ENISA поддерживает создание новых групп CSIRT путем опубликования данного отчета «Пошаговое руководство по созданию CSIRT с дополнительными контрольными таблицами», который поможет Вам создать ваш собственный CSIRT.

¹ Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. A "European Community agency" is a body set up by the EU to carry out a very specific technical, scientific or management task within the "Community domain" ("first pillar") of the EU.

4.1 Целевая аудитория

Основными целевыми группами, рассматриваемыми в данном документе, являются государственные и другие учреждения, решившие создать CSIRT для защиты своей собственной или партнерской информационной инфраструктур.

4.2 Как использовать данный документ

Этот документ ознакомит Вас с информацией о том, что такое CSIRT, какие сервисы она может предоставлять, и каковы должны быть необходимые шаги для его создания. Это должно предоставить читателю полное и прагматичное представление о структуре и содержании руководства по созданию CSIRT.

Глава 4. «Введение»

Ознакомление с данным отчетом.

Глава 5. «Общая стратегия планирования и создания CSIRT»

Первая часть дает определение CSIRT и предоставляет информацию о различных средах применения CSIRT и о сервисах, которые они могут предоставлять.

Глава 6. «Разработка бизнес плана»

В этой главе описывается бизнес подход к процессу создания и управления CSIRT.

Глава 7. «Продвижение бизнес плана»

В этой главе описываются вопросы делопроизводства и финансирования.

Глава 8. «Примеры операционных и технических процедур (технология)»

В этой главе описываются процедуры сбора информации и перевода её в периодическое издание по безопасности. В данной главе также даётся описание процесса обработки инцидентов.

Глава 9. «Обучение CSIRT»

В этой главе дается краткое описание доступных CSIRT тренингов. Для примера материалы одного из курсов предоставлены в дополнении.

Глава 10. «Упражнение - создание рекомендаций»

Эта глава содержит упражнения по поддержке одного из основных (ключевых) сервисов, оказываемых CSIRT - создание периодических изданий (или рекомендаций) по безопасности.

Глава 12. «Описание Плана Проекта»

Эта глава содержит дополнительный план проекта (контрольные перечни), предусмотренного данным руководством. Этот план позиционируется как простейшее средство по реализации данного руководства.

4.3 Соглашения, использованные в данном документе

Каждая глава начинается с краткого описания шагов, пройденных ранее в процессе создания CSIRT. Эти описания выделены в рамки, подобные следующей:

Мы сделали первый шаг

Каждая глава будет заканчиваться примером описанных ранее шагов. В данном документе «Условная CSIRT» будет представлена нами в качестве примера как CSIRT для средне размерной компании или учреждения.

Условная CSIRT

5 Общая стратегия планирования и создания CSIRT

Для успешного начала процесса создания CSIRT важно ясное видение возможных сервисов, предоставляемых этой группой своим клиентам в «мире CSIRT», более известных как «клиенты». Для этого необходимо понимать, что необходимо клиенту для своевременного и качественного предоставления соответствующих сервисов

5.1 Что такое CSIRT

CSIRT - Группа Реагирования на Инциденты Компьютерной Безопасности. Термин CSIRT используется преимущественно в Европе для обозначения, защищенного авторским правом термина CERT, официально зарегистрированного в США Координационной Группой CERT (CERT/CC).

Существуют различные аббревиатуры, обозначающие данные группы:

- CERT или CERT/CC (Группа Оперативного Реагирования на Компьютерные Инциденты / Координационная Группа)
- CSIRT (Группа Реагирования на Инциденты Компьютерной Безопасности)
- IRT (Группа Реагирования на Инциденты)
- CIRT (Группа Реагирования на Компьютерные Инциденты)
- SERT (Группа Оперативного Реагирования на Инциденты Безопасности)

Первая крупная вспышка компьютерного червя в глобальной IT инфраструктуре произошла в конце 80х годов. Компьютерного червя прозвали «Моррисом»² и распространялся он молниеносно, эффективно заражая огромное количество IT систем по всему миру.

Этот инцидент подействовал на общество как сигнал тревоги, после которого люди внезапно осознали сильную потребность в кооперации и координации совместных действий между системными администраторами и IT-менеджерами для дальнейшей борьбы с подобными инцидентами. Учитывая тот факт, что время простоя является основным критическим фактором в данной ситуации, необходимо иметь более организованный и структурированный подход к процессу обработки инцидентов компьютерной безопасности. Несколько дней спустя «инцидента Морриса» Агентство передовых оборонных исследовательских проектов (DARPA) создало первую CSIRT - CERT/CC³, располагавшийся в университете Carnegie Mellon в Питсбурге (Пенсильвания).

Эта модель вскоре была адаптирована в Европе, и в 1992 году датский академический провайдер SURFnet создал первую CSIRT в Европе под названием SURFnet –CSIRT⁴. Многие группы последовали этому примеру и в данный момент по сведениям «Реестра ENISA по деятельности CERT в Европе»⁵ насчитывается более 100 европейских CSIRT.

По прошествии лет группы CERT расширили свой потенциал от всего лишь простых откликов на инциденты до предоставления полного списка сервисов безопасности, включая предупредительные сервисы, такие как предупреждения, рекомендации по безопасности, тренинги и управление системами безопасности. Термин «CERT» вскоре стал считаться недостаточным. В результате, в конце 90х годов был принят новый термин «CSIRT». В настоящее время оба термина (CERT и CSIRT) используются как синонимы, однако CSIRT является более точным термином.

² Больше информации о черве Моррис: http://en.wikipedia.org/wiki/Morris_worm

³ CERT-CC, <http://www.cert.org>

⁴ SURFnet-CERT: <http://cert.surfnet.nl/>

⁵ Реестр ENISA http://www.enisa.europa.eu/cert_inventory/

5.1.1 Термин Клиенты

Отныне и впредь мы будем использовать термин хорошо известный в CSIRT-кругах, как “Клиенты”, для обозначения клиентов CSIRT. Мы будем говорить “клиент” в случае одного клиента и “клиенты” в случае групп клиентов.

5.1.2 Определение CSIRT

Термином CSIRT называется группа экспертов в области IT безопасности, чья основная обязанность реагировать на инциденты компьютерной безопасности. Эти группы также предоставляют необходимые сервисы для обработки инцидентов и поддержки своих клиентов в процессе восстановления после обнаружения брешей в системах безопасности.

В порядке уменьшения рисков и минимизации количества числа, требуемых ответов, большинство CSIRT также предоставляют профилактические и образовательные сервисы для своих клиентов. Они создают рекомендации по устранению уязвимостей в программном обеспечении и используемом оборудовании, а также информирует пользователей о эксплоитах и вирусах во время их распространения. Таким образом, клиенты могут быстро залатать и обновить свои системы. См. главу 5.2 «Сервисы, предоставляемые CSIRT» для получения справки о полном списке оказываемых сервисов.

5.1.3 Преимущества существования CSIRT

Наличие команды IT безопасности в организации способствует уменьшению и предотвращению основного количества инцидентов, а также помогает защищать её дорогостоящее имущество.

Возможные преимущества существования CSIRT:

- Наличие централизованной координации вопросов IT безопасности внутри организации (Контактное лицо).
- Централизованная и специализированная система обработки сообщений об инцидентах и реакции на них.
- Наличие экспертизы и поддержки в процессе быстрого восстановления инцидентов безопасности.
- Взаимодействие в юридических вопросах и сохранение доказательств в случае судебных процессов.
- Сохранение информации о развитии в сфере безопасности.
- Стимулирование взаимодействия клиентов по вопросам IT безопасности (повышение осведомлённости).

Условная CSIRT (шаг 0)

Понимание того, что такое CSIRT:

К примеру, предположим, что наша CSIRT будет обслуживать средних размеров организацию, состоящую из 200 сотрудников. В организации имеется IT департамент и 2 филиала по стране. IT играет ключевую роль в организации, так как используется для обмена внутренней информацией, предоставляет и поддерживает сеть передачи данных и электронный бизнес в режиме 24x7. Организация обладает собственной сетевой инфраструктурой и располагает резервированными каналами связи с Интернет предоставляемыми двумя различными ISP.

5.1.4 Определение различных сред применения SCIRT

Мы сделали первый шаг.

1. Понимание что такое CSIRT и возможности, которые он предоставляет.

>> Следующий наш шаг - это ответ на вопрос: "Какому сектору сервисы CSIRT будут предоставляться?"

Для того, чтобы создать CSIRT (аналогично и любому другому бизнесу крайне необходимо в кратчайшие сроки определить круг потенциальных клиентов и иметь четкое понимание того, в какой среде будут оказываться сервисы, предоставляемые CSIRT. В данный момент мы можем определить следующие "секторы" применения CSIRT перечисленные ниже:

- Академический
- Коммерческий
- CIP/CIIP
- Государственный
- Внутренний
- Военный
- Национальный
- Малый и Средний бизнес
- Торговый

CSIRT в Академическом секторе

Фокус

CSIRT в Академическом секторе сфокусирована на предоставлении сервисов академическим и научно-образовательным организациям, таким как университеты и научно-исследовательские институты и их территориальные инфраструктуры.

Клиенты

Типичными клиентами этой категории CSIRT, являются работники и студенты университетов.

Коммерческая CSIRT

Фокус

Коммерческая CSIRT предоставляет сервисы клиентам на коммерческой основе. В случае с ISP CSIRT в основном предоставляет сервисы предотвращения злоупотреблений в сети Интернет конечными пользователями (Dialup, ADSL), а также и другие сервисы.

Клиенты

Коммерческая CSIRT обычно предоставляет свои сервисы клиентам, которые их оплачивают.

CSIRT в CIP/CIIP секторе

Фокус

CSIRT в этом секторе главным образом сфокусирована на защите критической информации и/или инфраструктуры. В большинстве случаев данный тип CSIRT тесно сотрудничает с Государственными CIIP агентствами. Он покрывает все критические IT секторы страны и защищает граждан этой страны.

Клиенты



Правительство; критические IT бизнесы; граждане.

CSIRT в Государственном секторе

Фокус

CSIRT в Государственном секторе предоставляет сервисы государственным агентствам, а в некоторых странах, и гражданам.

Клиенты

Правительство и государственные агентства, а в некоторых странах сервисы оповещения предоставляются гражданам (Бельгия, Венгрия, Нидерланды, Великобритания и Германия).

Внутренняя CSIRT

Фокус

Внутренняя CSIRT предоставляет сервисы только организации (компания-владелец), внутри которой он был создан. Данный тип CSIRT характеризуется как более функциональный (корпоративный) по сравнению с другими типами CSIRT. Многие телекоммуникационные компании и банки имеют свои собственные внутренние CSIRT. Обычно эти CSIRT не поддерживают предоставление публичных сервисов.

Клиенты

IT департамент и работники организации.

CSIRT в Военном секторе

Фокус

CSIRT в Военном секторе предоставляет сервисы военным ведомствам и IT инфраструктурам, используемых для нужд оборонной сферы.

Клиенты

Работники военных ведомств или близких по роду деятельности организаций, к примеру, Министерство Обороны.

Национальная CSIRT

Фокус

CSIRT, сфокусированная на национальном уровне, представляет собой основное контактное лицо по вопросам IT безопасности. В некоторых случаях государственная CSIRT также действует как национальное контактное лицо (UNIRAS в Великобритании).

Клиенты

Данный тип CSIRT обычно не имеет ярко выраженного клиента, так как национальная CSIRT всего лишь играет посредническую роль в масштабе всей страны.

CSIRT в Малом и Среднем бизнесе

Фокус

Такие CSIRT предоставляют сервисы собственному бизнесу и своим партнёрам.

Клиенты

Работники малого и среднего бизнеса, либо специализированные группы пользователей, например, такие как "Ассоциация жителей города и Муниципалитетов".

CSIRT в Торговом секторе

Фокус

CSIRT в Торговом секторе сфокусированы на поддержке продуктов того или иного производителя. Зачастую, его целями являются разработка и предоставление решений,



нацеленных на устранение уязвимостей и уменьшение потенциально негативного эффекта от повреждения продукта.

Клиенты

Владельцы того или иного продукта.

Как было указано выше (параграф о Национальной CSIRT), возможны и случаи, когда CSIRT предоставляет сервисы нескольким секторам. Это в свою очередь отражается на дополнительном изучении потребностей клиентов.

Условная CSIRT (шаг 1)

Начальная фаза:

На первом этапе наша новая CSIRT задумана как Внутренняя, предоставляющая сервисы компании-владельцу, IT департаменту и работникам организации. CSIRT также поддерживает и координирует процесс обработки инцидентов происходящих в филиалах.

5.2 Сервисы, предоставляемые CSIRT

Были проделаны следующие шаги:

1. Понимание что такое CSIRT и возможности, которые он предоставляет.
2. Какому сектору новая команда CSIRT будет предоставлять свои сервисы.

>> Следующий наш шаг - это ответ на вопрос: "Какие сервисы мы будем предоставлять нашим клиентам?"

Существует огромное количество сервисов, которые CSIRT может предоставлять своим клиентам, но до сих пор ни одна из существующих CSIRT не предоставляет все эти сервисы в совокупности. Поэтому выбор соответствующего списка предоставляемых сервисов является крайне важной задачей. Ниже вы получите краткое описание всех известных сервисов описанные в книге "Справочник CSIRT", опубликованной CERT/CC⁶.

⁶ CERT/CC CSIRT handbook <http://www.cert.org/archive/pdf/csirt-handbook.pdf>

<u>Сервисы реагирования</u>	<u>Профилактические сервисы</u>	<u>Обработка артефактов</u>
• Оповещение и предупреждение • Обработка инцидентов • Анализ инцидентов • Реакция на инциденты • Координация реагирования на инциденты • Реакция на инциденты на месте • Обработка уязвимостей • Анализ уязвимостей • Реакция на уязвимости • Координация реагирования на уязвимости	• Объявления • Слежение за развитием технологий • Анализ и оценка систем безопасности • Конфигурирование и поддержка систем безопасности • Разработка средств обеспечения безопасности • Обнаружение вторжения • Распространение информации о системах безопасности	• <u>Анализ артефактов</u> • <u>Реакция на артефакт</u> • <u>Координация реагирования на артефакты</u>
		<u>Управление качеством систем безопасности</u> • <u>Анализ рисков</u> • <u>Непрерывность рабочего процесса и восстановление при аварийных ситуациях</u> • <u>Консультирование по вопросам безопасности</u> • <u>Повышение осведомлённости</u> • <u>Обучение / Тренинги</u> • <u>Оценка продукта и Сертификация</u>

Рис.1: Список сервисов CSIRT от CERT/CC⁷

Базовые сервисы (выделенные жирным шрифтом) делятся на две категории: Сервисы реагирования и Профилактические сервисы. Профилактические сервисы нацелены на предотвращение инцидентов посредством повышения осведомлённости и тренингов, в то время как Сервисы реагирования направлены на обработку инцидентов и уменьшение потенциального ущерба.

Обработка артефактов состоит из анализа любого файла или объекта найденного в системе, который может быть использован вредоносными программами, такими как остатки вирусов, компьютерные черви, скрипты, трояны и т.д. Данные сервисы также включают в себя обработку и распространение итоговой информации производителям и другим заинтересованным сторонам во избежание дальнейшего распространения вредоносного ПО, содержащего в себе вирусы, компьютерные черви, а также уменьшению общего числа рисков.

Сервис **Управления качеством систем безопасности** имеет долгосрочные цели и состоит из консультирования и образовательных мероприятий.

Смотрите *Приложение В* с детальным описанием сервисов CSIRT.

Правильный выбор сервисов предоставляемых своим клиентам является важным шагом, и в дальнейшем мы будем ссылаться на него в главе 6.1 *Определение финансовой модели*.

Большинство CSIRT начинают с предоставления базовых сервисов 'Оповещение и предупреждение', рассылают 'Объявления' и предоставляют 'Обработку инцидентов' своим конституантам. Обычно эти базовые сервисы определяют степень общественного интереса и внимания со стороны клиентов и в основном рассматриваются как самые важные.

⁷ CSIRT Services list from CERT/CC: <http://www.cert.org/csirts/services.html>

Рекомендуется создание малой группы так называемых “пилотных” клиентов, предоставление базовых сервисов в течение определённого периода времени (пилотного периода) и получение отзывов о качестве предоставленных им сервисов.

Заинтересованные “пилотные” клиенты обычно предоставляют конструктивный отзыв и помогают разработать список необходимых сервисов, адаптированных под их нужды.

Условная CSIRT (шаг 2)

Выбор правильных сервисов

На начальном этапе было решено, что новая CSIRT будет в основном сфокусирована на предоставлении некоторых базовых сервисов работникам организации.

Было также решено, что по окончании пилотного периода времени будет рассмотрен вопрос расширения портфеля предоставляемых сервисов и вполне возможно, что некоторые сервисы ‘Управления систем безопасности’ будут добавлены. Данное решение будет основано на отзыве “пилотных клиентов” и рекомендациях отдела Контроля Качества.

5.3 Анализ целевой группы и заявление о намерениях

Были проделаны следующие шаги:

1. Понимание что такое CSIRT и возможности, которые он предоставляет.
2. Какому сектору новая команда CSIRT будет предоставлять свои сервисы.
3. Какого типа сервисы может предоставить CSIRT своим клиентам.

>> Следующий наш шаг - это ответ на вопрос: *“Какой метод создания CSIRT мы будем использовать?”*

Следующим нашим шагом мы должны глубже изучить клиентов для того, чтобы определить правильные методы взаимодействия с ними:

- Определить методы взаимодействия с клиентами
- Сформировать заявление о намерениях
- Создать реальный план реализации проекта
- Определить сервисы, предоставляемые CSIRT
- Определить организационную структуру
- Определить Политику информационной безопасности
- Нанять на работу компетентный персонал
- Использовать офис CSIRT
- Скооперироваться с другими CSIRT и другими возможными национальными инициативами

Далее в этой главе мы детально рассмотрим все эти шаги и попытаемся создать исходный бизнес план проекта.

5.3.1 Методы взаимодействия с клиентами

Как было упомянуто ранее, крайне важно знать потребности клиентов, а также собственную стратегию взаимодействия с ними, включая подходящие каналы распространения информации.

В теории управления указаны несколько возможных подходов к проблеме анализа целевой группы. В этом документе мы рассмотрим два из них, так называемые SWOT анализ и PEST анализ.

Анализ SWOT

Так называемый анализ SWOT представляет собой стратегический инструмент планирования, используемый для оценки таких параметров, как **Достоинства**, **Недостатки**, **Возможности** и **Угрозы**, необходимый для проектов, бизнес-предприятия или в любых других ситуациях связанных с вопросом принятия решения. Данная технология была разработана Альбертом Хамфреем (Albert Humphrey), возглавлявшим научные проекты Станфордского Университета (Stanford University) в 1960-70х годах, использовавшим данные более из 500 компаний по версии журнала Fortune.⁸

Достоинства	Недостатки
Возможности	Угрозы

Рис.2: Анализ SWOT

⁸ SWOT analysis at Wikipedia: http://en.wikipedia.org/wiki/SWOT_analysis

Анализ PEST

Анализ PEST является ещё одним важным и широко используемым инструментом анализа клиентов с точки зрения Политических, Экономических, Социально-культурных и Технологических обстоятельств среды, в которой оперирует CSIRT. Данный анализ помогает определить, является ли планирование точным по отношению к среде и помогает ли избежать действий, основанных на ложном предположении.

Политические • Проблемы Экологии / Окружающей среды • Текущее законодательство внутреннего рынка • Будущее законодательство • Европейское/Международное законодательство • Процесс и Органы регулирования • Государственные политики • Правительственный срок и его смена • Торговые политики • Финансирование, субсидии и инициативы • Лоббирование на внутреннем рынке / влиятельные группы • Влиятельные международные группы	Экономические • Экономическая ситуация на внутреннем рынке • Экономические тенденции на внутреннем рынке • Тенденции иностранных экономик • Основные положения налогообложения • Особенности налогообложения продукции / сервисов • Факторы сезонности • Рыночные и торговые циклы • Факторы специфичных производств • Рыночные маршруты и тенденции распространения • Мотивация потребителя / конечного пользователя • Выгода и курсы валют
Социально-культурные • Тенденции стиля жизни • Демография • Мнения и позиции потребителя • Средства массовой информации • Изменения законодательства, влияющие на социальные факторы • Бренд, компания, технологическая концепция • Покупательская способность потребителя • Разновидность и ролевые модели • Основные события и их влияние • Покупательский подход и тенденции • Религиозный / этнический фактор	Технологические • Развитие конкурентной технологии • Финансирование исследований • Ассоциированные / зависимые технологии • Замещаемые технологии / решения • Совершенство технологии • Объем и совершенство производства • Информация и коммуникации • Механизм / технология принятия решения (потребителем) при покупке • Технологическое законодательство • Потенциал инноваций • Доступ к технологии, лицензирование, патенты • Интеллектуальная собственность

Рис.3: Анализ PEST

Детализированное описание PEST анализа можно получить в Википедии⁹.

Оба метода дают всеобъемлющее и структурированное представление о потребностях клиентов. Результаты анализов будут дополнять бизнес план и, тем самым, способствовать получению финансирования для создания CSIRT.

Каналы взаимодействия

Одна из важнейших тем, необходимых для изучения - это возможные каналы взаимодействия и методы распространения информации ("Каким образом обмениваться информацией с клиентом?")

⁹ PEST analysis at Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

Если это возможно, то необходимо рассмотреть возможность регулярного посещения клиентов. Доказано, что личные встречи ("с глазу на глаз") упрощают сотрудничество. Если обе стороны желают работать совместно, то такие встречи обязательно приведут к более открытым взаимоотношениям.

Обычно CSIRT используют несколько методов обмена информацией с клиентом. Доказано на практике, что следующие методы являются полезными, а также заслуживающими нашего внимания:

- Публичный веб-сайт
- Приватная зона доступа на веб-сайте
- Веб-форма для сообщения об инциденте
- Списки рассылки
- Персонализированные электронные письма
- Телефон / Факс
- Служба СМС
- «Старомодные» бумажные письма
- Ежемесячные или ежегодные отчёты

Кроме тех способов обмена информацией описанных выше, большинство CSIRT публикуют свои рекомендации по безопасности на общедоступном веб-сайте и рассылают их с помощью списков рассылки для того, чтобы ускорить процесс обработки инцидентов.

! Информация должна распространяться в защищённой форме, если это возможно. К примеру, электронная почта может быть заверена системой PGP и важная информация относительно инцидента должна всегда передаваться зашифрованной.

Для получения дополнительной информации смотрите главу 8.5 *Доступный CSIRT инструментарий*, а так же главу 2.3 Запроса на обсуждение (RFC) №2350¹⁰.

Условная CSIRT (шаг 3а)

Проведение анализа потребностей клиентов и соответствующих каналов обмена информацией

Совместный мозговой штурм между ключевыми лицами совета правления организации и клиентам создал достаточное количество входной информации, необходимой для SWOT анализа. Результат анализа показал необходимость предоставления базовых сервисов:

- Оповещение и предупреждение
- Обработка инцидентов (анализ, реагирование и координация инцидентов)
- Объявления

Необходимо удостовериться, что информация распространяется в хорошо организованном порядке для того, чтобы она достигла как можно большую часть клиентов. Было принято решение о том, что оповещения, предупреждения и объявления будут публиковаться на выделенном веб-сайте, а также рассылаться с помощью списков рассылки в виде рекомендаций по безопасности. Для получения отчётов об инцидентах CSIRT будет использовать средства электронной почты, телефонной и факсимильной связи. На следующем этапе планируется разработка единой веб-формы.

Далее смотрите пример использования SWOT анализа.

¹⁰ <http://www.ietf.org/rfc/rfc2350.txt>

Достоинства - У компании есть определенные знания - Им нравится план, и они хотят сотрудничать - Поддержка и финансирование со стороны совета правления	Недостатки - Недостаточное взаимодействие между различными отделами и филиалами - Отсутствие координации по вопросам IT инцидентов - Большое количество “малых отделов”
Возможности - Огромный поток неструктурированной информации об уязвимостях - Сильная потребность в координации - Снижение потерь в результате инцидентов - Большое количество незащищённых участков в вопросах IT безопасности - Обучение сотрудников принципам IT-безопасности	Угрозы - Недостаточный объем финансирования - Недостаточное количество сотрудников - Большие надежды - Культура

Рис.4: Пример SWOT анализа

5.3.2 Заявление о намерениях

После анализа потребностей и пожеланий клиентов относительно сервисов, оказываемых CSIRT необходимо приступить к написанию черновой версии заявления о намерениях.

Заявление о намерениях описывает основные функции организации в обществе с точки зрения производимой продукции и оказываемых сервисов своим клиентам. Это позволяет чётко взаимодействовать уже существующему CSIRT и лучше функционировать новой CSIRT.

Рекомендуется создание заявления о намерениях компактным, но не слишком сжатым, так как обычно оно остаётся неизменным в течение нескольких лет.

Ниже приведены примеры заявлений о намерениях уже существующих CSIRT:

“<Название CSIRT> предоставляет информацию и содействует своим <клиентам (укажите своих клиентов)> в процессе внедрения профилактических мероприятий, нацеленных на уменьшение рисков инцидентов компьютерной безопасности, а также реагирует на данные инциденты в случае их возникновения”.

“Для предоставления технической поддержки <Клиентам> по вопросам предотвращения и реагирования на Инциденты IT Безопасности¹¹”

Заявление о намерениях является крайне важным и необходимым первоначальным шагом. Пожалуйста, ссылайтесь на главу 2.1 или RFC2350¹² для получения более детального описания того, какую информацию CSIRT должны публиковать.

¹¹ Mission statement of Govcert.nl: <http://www.govcert.nl>

¹² <http://www.ietf.org/rfc/rfc2350.txt>

Условная CSIRT (шаг 3b)

Руководство условной CSIRT приняло следующее заявление о намерениях:

“Условная CSIRT предоставляет информацию и содействует работникам компании-владельца в процессе внедрения профилактических мероприятий, нацеленных на уменьшение рисков инцидентов компьютерной безопасности, а также реагирует на данные инциденты в случае их возникновения”.

Таким образом, условная CSIRT четко указывает на то, что она является внутренней CSIRT и ее основная обязанность работать с вопросами, связанными с IT безопасностью.

6 Разработка бизнес-плана

Были проделаны следующие шаги:

1. Понимание что такое CSIRT и возможности, которые он предоставляет.
2. Какому сектору новая команда CSIRT будет предоставлять свои сервисы
3. Какого типа сервисы может предоставить CSIRT своим клиентам.
4. Анализ окружающего сообщества и потенциальной клиентуры.
5. Определение основных целей и положений

>> Следующий шаг – разработка бизнес-плана.

Результат анализа дает хорошее представление о потребностях и (предполагаемых) слабых сторонах клиентов, поэтому он используется на входе для следующего шага.

6.1 Определение финансовой модели

По результатам анализа была выбрана пара основных сервисов, с которых следует начать. Следующий этап – подумать о финансовой модели - какие характеристики услуги подходят клиентам и будут ими оплачены.

В совершенном мире финансирование было бы адаптировано под нужды клиентов, но в реальности набор оказываемых услуг должен быть адаптирован под определенный бюджет. Поэтому более реалистично начать планирование с финансовых вопросов.

6.1.1 Модель затрат

Двумя основными факторами, влияющими на затраты, являются установление рабочих часов и количество (а также качество) нанимаемого персонала. Есть ли потребность в 24x7 оказании сервиса реагирования на инциденты и технической поддержки? Или эти сервисы будут предоставляться в течение рабочего времени?

В зависимости от желаемой доступности услуги, а также от необходимого оборудования (например, возможно ли работать из дома?), может быть выгодным работать с графиком «по вызову» или же с повременным графиком.

Возможным сценарием является оказание профилактических услуг и услуг реагирования во время рабочего времени. Вне рабочего времени будут предоставляться только ограниченные услуги, например, оказание услуг персоналом с графиком работы «по вызову» в случае наступления серьезных аварий и инцидентов.

Другая альтернатива – поискать международное сотрудничество с другими CSIRT группами. Уже есть примеры существующего сотрудничества «Вслед за Солнцем». Например, сотрудничество между Европейскими и Американскими группами оказалось выгодным, и оно обеспечивает хороший способ обмена ресурсами друг с другом. Например, Группа Реагирования на Инциденты Компьютерной Безопасности компании Sun Microsystems, которая имеет многочисленные подразделения в разных временных зонах по всему миру, оказывает сервис 24x7 посменным дежурством команд по всему миру (но все подразделения в разных временных зонах являются членами одной группы CSIRT).

Это сокращает затраты, потому что команды работают всегда только во время своего рабочего времени, но в это время также оказывают сервис «спящей части» мира.

Анализ потребности клиентов в сервисе 24x7 - хорошая практика. Сигналы тревоги и предупреждения, поданные в ночное время, не имеют особого смысла, когда получатель этого сервиса прочитает их только на следующее утро. Между «нужным сервисом» и «желаемым сервисом» очень тонкая линия, но рабочие часы являются важным фактором, определяющим количество персонала и оборудования, и оказывающим основное влияние на модель затрат.

6.1.2 Модель доходов

После определения расходов следующий шаг – подумать о возможных моделях доходов – как запланированные сервисы будут финансироваться. Вот некоторые возможные сценарии:

Использование существующих ресурсов

Всегда выгодно оценивать существующие ресурсы в других подразделениях компании. Есть ли среди нанятого персонала подходящий для CSIRT с нужным опытом и квалификацией (например, в отделе информационных технологий)? Можно совместно с руководством можно найти вариант их привлечения по совместительству в CSIRT на начальной стадии. Или, как вариант, оказание ими поддержки CSIRT на специальных условиях.

Членские взносы

Другой вариант – оказывать услуги клиентам за ежегодные/ежеквартальные членские взносы. Дополнительные сервисы могут оплачиваться на основе «в случае использования», например, консультационные услуги или анализ системы безопасности.

Другой вероятный сценарий - услуги (внутренним) клиентам оказываются бесплатно, но услуги, оказываемые внешним заказчикам, могут быть платными. Другая идея – публиковать рекомендации и информационные бюллетени на общественных веб сайтах и иметь раздел «Только для Членов» с более детальной специализированной информацией.

Было доказано на практике, что «Подписка по услуге CSIRT» не обеспечивает достаточного финансирования, особенно на начальной стадии. Существуют, например, фиксированные основные затраты на команду и оборудование, которые должны быть оплачены заранее. Финансирование этих затрат продажей услуг CSIRT затруднено и требует очень детального финансового анализа для определения точки безубыточности.

Субсидия

Другой возможностью, достойной рассмотрения, может быть – подать заявку на субсидирование проекта за счет средств правительства или правительственной организации, т.к. в настоящее время большинство стран имеет в наличии фонды на проекты области ИТ безопасности. Хорошим началом могло бы быть - связаться с Министерством Внутренних Дел.

Комбинация различных моделей, конечно, возможна.

6.2 Определение организационной структуры

Подходящая организационная структура CSIRT сильно зависит от существующей структуры компании-владельца и клиентов. Она также зависит от доступности квалифицированных экспертов, нанимаемых на постоянной основе или для конкретной задачи.

Типичная Группа Реагирования на Инциденты Компьютерной Безопасности выделяет следующие роли внутри группы:

Руководство

- Главный менеджер

Персонал

- Офис-менеджер
- Бухгалтер
- Консультант по коммуникациям
- Юридический консультант

Оперативная техническая группа

- Руководитель технической группы
- Техники CSIRT, оказывающие CSIRT-сервисы
- Исследователи

Внешние консультанты

- Нанимаются, когда требуются

Чрезвычайно полезно иметь в штате юридического специалиста, особенно во время начальной фазы CSIRT. Это увеличит затраты, но в конечном итоге вы сэкономите время и избежите правовых проблем.

В зависимости от уровня и разнообразия квалификации внутри группы клиентов, а также когда CSIRT имеет хороший медиа-профиль, оказалось очень полезным иметь в группе эксперта по коммуникациям. Такой эксперт может сосредоточиться на переводе сложных технических вопросов в более понятные сообщения для клиентов или медиа-партнеров. Эксперт по коммуникациям также будет обеспечивать обратную связь от клиентов к техническим экспертам, так он может служить «переводчиком» и «посредником» между этими двумя группами.

Ниже приведено несколько примеров организационных моделей, используемых действующими CSIRT.

6.2.1 Независимая бизнес модель

CSIRT создается и действует как независимая организация со своим менеджментом и работниками.

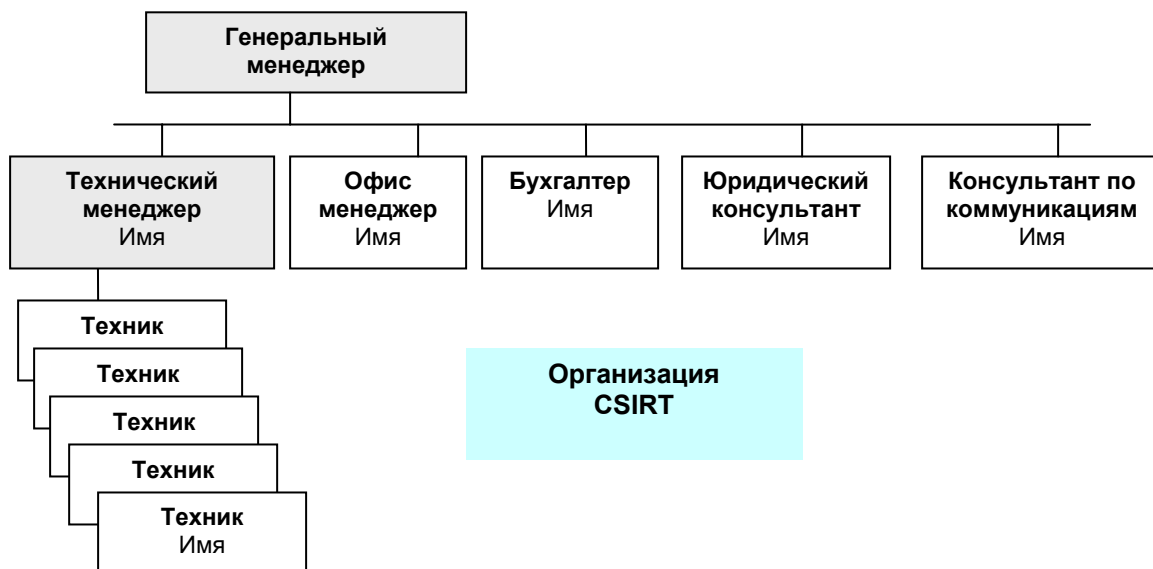


Рис. 5 Независимая бизнес модель

6.2.2 Встроенная модель

Эта модель может быть использована, если CSIRT основана в рамках существующей организации, используя существующий IT отдел, например. CSIRT возглавляет лидер группы, который отвечает за деятельность CSIRT. Лидер группы собирает необходимых техников на время устранения инцидентов или для работы над задачами CSIRT. Он может попросить помощи в пределах существующей организации.

Эта модель может быть также адаптирована под конкретные ситуации по мере их возникновения. В этом случае команда имеет определенное количество эквивалентов полной занятости. Служба жалоб Интернет Сервис Провайдера, например, определенно является работой с полной занятостью на один или (в большинстве случаев) больше, чем один эквивалент занятости.

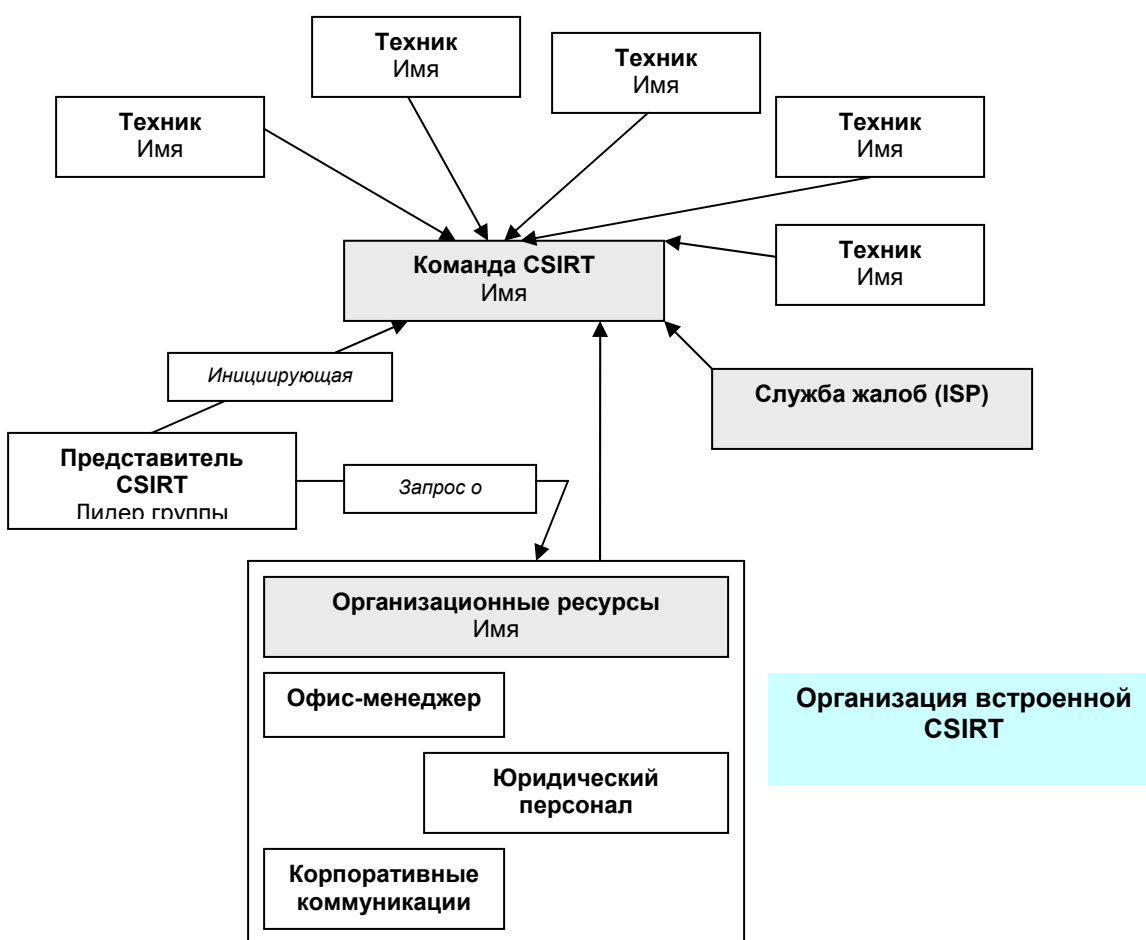


Рис. 6 Встроенная организационная модель

6.2.3 Модель кампуса

Модель кампуса, как подсказывает имя, главным образом используется образовательными и исследовательскими CSIRT. Большинство академических и исследовательских организаций состоят из различных университетов и кампусных инфраструктур в разных местах, распределенных по региону или даже всей стране (как в случае NREN, Национальных Исследовательских Сетей). Обычно эти организации независимы друг от друга и имеют свою собственную CSIRT. Эти CSIRT-группы обычно организованы под зонтиком «материнской», или центральной CSIRT. Центральная CSIRT занимается координированием и является единственным контактом для внешнего мира. В большинстве случаев центральная CSIRT тоже предоставляет основные CSIRT-сервисы, а также распространяет информацию об инцидентах CSIRT соответствующего кампуса.

Некоторые CSIRT распространяют свои основные CSIRT-сервисы другим кампусным CSIRT, что в результате приводит к уменьшению перегрузки центральной CSIRT.

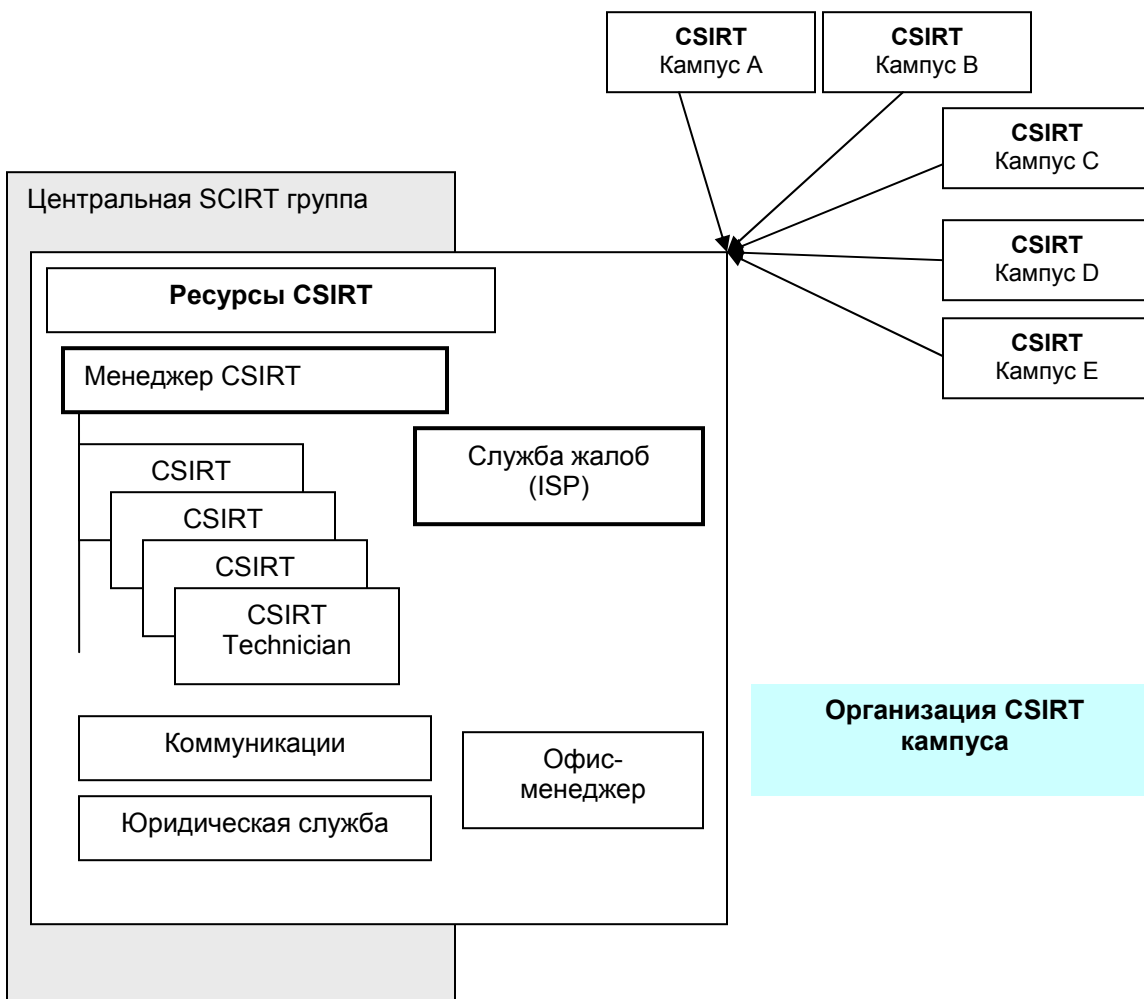


Рис. 7 Модель кампуса

6.2.4 Добровольная модель

Эта организационная модель описывает группу людей (специалистов), которые объединяются для обмена советами и оказания поддержки друг другу (и третьим лицам) на добровольной основе. Это свободное общество, сильно зависимое от мотивации участников.

Эта модель, например, принята обществом WARP¹³.

6.3 Наем нужного персонала

Решив, какие сервисы и какой уровень поддержки оказывать, а также выбрав организационную модель, следующий шаг – найти нужное количество квалифицированного персонала.

Почти невозможно дать точные цифры о количестве требуемого технического персонала, но следующие значения оказались на практике хорошим подходом:

- Для оказания двух основных сервисов – распространения консультационных бюллетеней и обработки инцидентов: минимум **4** эквивалента полной занятости.
- Для полного спектра сервиса CSIRT в рабочие часы и обслуживания систем: минимум **6 – 8** эквивалентов полной занятости.
- Для полностью укомплектованных смен с сервисом 24x7 (2 смены во вне рабочее время): минимум около **12** эквивалентов полной занятости.

Эти цифры также включают резерв на случаи болезней, праздников и т.д. Также необходимо проверить местные коллективные трудовые договоры. Если персонал будет работать в нерабочие часы, это может привести к дополнительным расходам в связи с надбавками к заработной плате за внеурочное время, которые должны выплачиваться.

¹³ Инициатива WARP http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

Ниже приведен краткий обзор ключевых сфер компетентности технических экспертов Групп Оперативного Реагирования на Компьютерные Инциденты (CSIRT).

Общее описание технического персонала:

Личные способности

- Гибкость, креативность и хороший командный дух
- Сильные аналитические навыки
- Способность объяснить сложные технические вопросы простыми словами
- Хорошее отношение к конфиденциальности и методической работе
- Хорошие организационные способности
- Стрессоустойчивость;
- Хорошие разговорные и письменные навыки
- Восприимчивость ума и желание учиться

Технические навыки

- Хорошие знания Интернет-технологий и протоколов
- Знание Linux и Unix систем (в зависимости от оборудования клиентов)
- Знание Windows систем (в зависимости от оборудования клиентов)
- Знание сетевого оборудования (маршрутизаторы, коммутаторы, DNS, Proxy, Mail и т.д.)
- Знание Интернет приложений ((SMTP, HTTP(s), FTP, telnet, SSH и т.д.)
- Знание Угроз безопасности (DDoS, фишинг, атаки Deface, сниффинг и т.д.)
- Знание оценки рисков и практических применений

Дополнительные способности

- Желание работать в режиме 24x7 или в режиме «по вызовам» (в зависимости от модели сервиса)
- Максимальное время на дорогу, доступность (в случае аварии доступность в офисе; максимальное время, нужное на дорогу к месту аварии)
- Уровень образования
- Опыт работы в сфере компьютерной безопасности

Условная CSIRT (шаг 4)

Составление Бизнес Плана

Финансовая модель

Благодаря тому, что компания ведет 24x7 электронный бизнес, а также имеет IT отдел, работающий 24x7, было решено оказывать полный сервис во время рабочих часов и поддержку по телефону в нерабочее время. Сервис будет предоставляться клиентам на платной основе, но эта возможность оказывать сервис внешним клиентам будет оценена во время пилотной и оценочной стадии.

Модель доходов

Во время стартовой и пилотной фазы CSIRT будет финансироваться через компанию-владельца. Во время пилотной и оценочной стадии будет обсуждено дополнительное финансирование, включая возможность продажи сервиса внешним клиентам.

Организационная модель

Компания-владелец – маленькая компания, поэтому выбрана встроенная модель. Во время рабочего времени персонал из трех человек будет оказывать основные сервисы (распространение консультационных бюллетеней и обработка инцидентов). IT отдел компании уже имеет людей с подходящими навыками. Договор с отделом составлен таким образом, что новая CSIRT может, когда нужно, просить помощи на

специальной основе.

Также может быть организована вторая линия из техников компании, отвечающих на запросы по телефону. Таким образом, будет главная CSIRT команда из четырех членов с полной занятостью и пять дополнительных членов группы CSIRT. Один из них также будет доступен для циркулирующих смен.

Персонал

Лидер группы CSIRT имеет опыт работы в IT безопасности и оказании поддержки 1-го и 2-го уровня. Также он имеет опыт работы в сфере управления устойчивыми кризисами. Остальные 3 члена группы – специалисты по безопасности. Члены группы CSIRT с частичной занятостью из IT отдела компании – специалисты по инфраструктуре компании.

6.4 Использование офиса и оборудования

Оборудование, использование офисного пространства и физическая охрана помещения – очень широкие темы, поэтому в этом документе не дается их исчерпывающего описания.

Больше информации об охране помещения можно найти здесь:

http://en.wikipedia.org/wiki/Physical_security

http://www.sans.org/reading_room/whitepapers/phycial/

<http://www.infosyssec.net/infosyssec/physfac1.htm>

“Укрепление здания”

Так как CSIRT обычно работает с очень важной информацией, то было бы хорошо подготовить команду к заботе о физической безопасности офиса. Это очень сильно зависит от существующих условий и инфраструктуры, а также от существующей политики информационной безопасности компании-владельца.

Правительства, например, работают со схемами классификации и очень строго следят за обращением с конфиденциальной информацией. Рекомендуем проверить в вашей организации установленные правила и политику.

Обычно новая группа CSIRT вынуждена зависеть от организации-владельца, чтобы научиться принятым правилам, политике и другим вещам.

Исчерпывающее описание всего необходимого оборудования и методов измерения безопасности не включено в этот документ. Тем не менее, ниже вы найдете короткий список основных средств для вашей CSIRT.

Главные правила для выбора здания

- Использование средств контроля доступа
- Доступ в офис CSIRT только для персонала CSIRT
- Мониторинг офиса и входов с помощью камер
- Хранение конфиденциальной информации в запирающихся шкафах или в сейфе
- Использование защищенных IT систем

Главные правила для IT оборудования

- Использование такого оборудования, которое может быть обслужено персоналом
- Усиление всех систем
- Устанавливание патчей и обновление системы перед подключением ее к Интернет
- Использование программного обеспечения по компьютерной безопасности (Firewalls, антивирусные сканеры, anti-spyware и т.д.)

Обслуживание коммуникационных каналов

- Общественный веб сайт
- Закрытая область пользователей на веб сайте
- Веб-формы для сообщений об инцидентах
- Email (с поддержкой PGP / GPG / S/MIME)
- Софт почтовых списков
- Выделенный телефонный номер, доступный клиентам:
 - Телефон
 - Факс
 - SMS

Системы отслеживания записей

- База данных контактов с детальной информацией о членах команды, других командах и т.д.
- Средства управления взаимодействием с клиентами (CRM)
- Система билетов по обработке инцидентов

Использование с самого начала «корпоративного стиля» для:

- электронных сообщений и информационных бюллетеней
- писем на бумажных носителях
- ежемесячных и годовых отчетов
- форм отчета об инцидентах

Другие вопросы

- Предусмотреть резервные каналы коммуникации на случай атаки
- Предусмотреть избыточность Интернет канала

Больше информации об инструментарии CSIRT можно найти в главе 8.5 «Инструментарий CSIRT».

6.5 Разработка политики информационной безопасности

Политика информационной безопасности будет зависеть от типа вашей CSIRT. Кроме описания желаемых операционных и административных процессов и процедур, политика должна соответствовать законодательству и стандартам, особенно в отношении ответственности SCIRT. Обычно CSIRT ограничена национальными законами и нормами, которые часто выполнены в соответствии с Европейским законодательством (обычно Директивами ЕС) и международными соглашениями. Стандарты не обязательно применяются напрямую, они могут быть рекомендованы законами или инструкциями.

Ниже следует список возможных законов и методик:

Национальные

- Различные законы об информационных технологиях, телекоммуникациях, медиа
- Законы о защите данных и конфиденциальности
- Законы и нормы о сохранности данных
- Законодательство о финансах, бухгалтерском учете и корпоративном менеджменте
- Кодексы поведения для корпоративного управления и IT управления

Европейские

- Директивы об электронной подписи (1993/93/EC)
- Директивы о защите данных (1995/46/EC) и конфиденциальности в электронных коммуникациях (2002/58/EC)
- Директивы о телекоммуникационных сетях и сервисах (2002/19/EC – 2002/22/EC)
- Директивы о Корпоративном Законодательстве (например, 8-ая Директива о корпоративном законодательстве)

Международные

- Базельское Соглашение II (особенно в отношении управления операционными рисками)
- Конвенция Совета Европы по Киберпреступности
- Конвенция Совета Европы по правам человека (статья 8 о конфиденциальности)
- Международные стандарты финансовой отчетности (МСФО, они в какой-то мере относятся к контролю над IT)

Стандарты

- Британский стандарт BS 7799 (Информационная безопасность)
- Международные стандарты ISO2700x (Системы управления информационной безопасностью)
- Немецкий IT-Grundschutzbuch, Французский EBIOS и другие национальные вариации

Чтобы определить, действует ли ваша CSIRT в соответствии с национальным и международным законодательством, воспользуйтесь юридической консультацией.

Основные вопросы, на которые нужно ответить в вашей политике обработки информации:

- Как входящая информация «маркируется» или «классифицируется»?
- Как обрабатывается информация, особенно эксклюзивного характера?
- Какие принципы приняты для раскрытия информации, особенно если информация, связанная с инцидентом, передается другим командам?
- Есть ли правовые принципы, которые должны учитываться при обработке информации?

- Есть ли у вас политика по использованию криптографии для защиты эксклюзивности и целостности в архивах и/или в передаче данных, особенно по e-mail?
- Включает ли эта политика правовые граничные условия, такие как исковая сила дешифрования в случае судебных разбирательств?

Условная CSIRT (шаг 5)**Оборудование и местоположение офиса**

Благодаря тому, что компания-владелец уже имеет эффективную физическую охрану помещения, новая CSIRT хорошо в этом отношении организована. Так называемая «военная комната» предоставляется для осуществления координирования в случае возникновения инцидента. Куплен сейф для хранения материалов шифрования и важных документов. Организована отдельная телефонная линия с коммутатором для организации горячей линии во время рабочих часов, и мобильный телефон с тем же номером для реагирования «по запросу» вне рабочего времени.

Также могут использоваться существующее оборудование и корпоративный веб-сайт для объявления информации, связанной с CSIRT. Списки E-mail рассылки создаются и обслуживаются с разграничением коммуникаций между членами команды и с другими командами. Вся контактная информация персонала хранится в базе данных, распечатанная версия хранится в сейфе.

Правила

Так как CSIRT встроена в компанию с существующей политикой информационной безопасности, соответствующая политика для CSIRT установлена с помощью правового консультанта компании.

6.6 Поиск сотрудничества с другими CSIRT и возможными национальными инициативами

Существование других CSIRT-инициатив и большая потребность в их сотрудничестве уже была несколько раз упомянута в этом документе. Хорошая практика – как можно скорее познакомиться с другими командами CSIRT, чтобы получить необходимый контакт с сообществом CSIRT. Обычно команды CSIRT очень открыты к тому, чтобы помочь начать деятельность.

*Инструментарий работы CERT в Европе*¹⁴ от ENISA – хорошая отправная точка для поиска других CSIRT в стране или для поиска национального сотрудничества между CSIRT.

Чтобы получить помощь в поиске подходящего источника информации о CSIRT, свяжитесь с CSIRT экспертами ENISA:

CERT-Relations@enisa.europa.eu

¹⁴ Реестр ENISAs: http://www.enisa.europa.eu/cert_inventory/



Ниже приводится обзор активности сообщества CSIRT. Пожалуйста, обратитесь к *Инструментария* за более подробным описанием и дополнительной информацией.

Европейская CSIRT-инициатива

TF-CSIRT (Оперативная группа CSIRT)¹⁵

Оперативная группа CSIRT продвигает сотрудничество между Группами Реагирования на Инциденты Компьютерной Безопасности (CSIRT) в Европе. Основными целями оперативной группы являются организация форума для обмена опытом и знаниями, запуск пилотных сервисов для европейского сообщества CSIRT и помощь в создании новых CSIRT.

Основными задачами оперативной группы являются:

- организация форума для обмена опытом и знаниями;
- пилотный запуск сервисов для европейского сообщества CSIRT;
- продвижение общих стандартов и процедур для реагирования на инциденты компьютерной безопасности;
- помощь в создании новых CSIRT и обучении персонала CSIRT.
- Деятельность оперативной группы сфокусированы на Европе и соседних странах в соответствии с Кругом Обязанностей, утвержденных Технической Комиссией TERENCE 15 сентября 2004 г.

Глобальная CSIRT-инициатива

FIRST¹⁶

FIRST - это первая организация – признанный глобальный лидер в реагировании на инциденты компьютерной безопасности. Членство в FIRST позволяет командам реагирования на инциденты более эффективно отвечать на инциденты по безопасности, – как активно в виде реагирования, так и профилактически.

FIRST сводит друг с другом разнообразные команды CSIRT из государственных, коммерческих и образовательных организаций. Целями FIRST являются поощрение сотрудничества и координации по предупреждению инцидентов, стимулирование быстрой реакции на инциденты и продвижение обмена информации среди членов сообщества в целом.

Кроме доверительной сети, которую FIRST формирует среди сообщества реагирования на инциденты, он также создает дополнительные сервисы.

Условная CSIRT (шаг 6)

Поиск сотрудничества

Используя инструмент ENISA, быстро удалось найти несколько CSIRT в одной стране и связаться с ними. Для недавно нанятого лидера группы была организована поездка в одну из этих CSIRT, из встречи он узнал о национальной деятельности CSIRT. Эта встреча была более чем полезна для получения информации о примерах методов работы получения поддержки пары других команд.

¹⁵ TF-CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

¹⁶ FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

7 Продвижение Бизнес Плана

Были проделаны следующие шаги:

1. Понимание что такое CSIRT и возможности, которые он предоставляет.
2. Какому сектору новая команда CSIRT будет предоставлять свои сервисы
3. Какого типа сервисы может предоставить CSIRT своим клиентам.
4. Анализ окружающего сообщества и потенциальной клиентуры.
5. Определение основных целей и положений
6. Разработка бизнес плана.
 - a. Определение финансовой модели.
 - b. Определение организационной структуры,
 - c. Первоначальный подбор кадров.
 - d. Подбор и оборудование офиса.
 - e. Разработка политики информационной безопасности
 - f. Поиск потенциальных партнеров.

>> Следующий шаг – учесть все вышесказанное в плане проекта и начинать!

Хорошее начало для определения вашего проекта начать с бизнес-идеи. Бизнес-идея будет использоваться в качестве основы для плана проекта, а также для обращения за поддержкой у руководства и получения бюджета или других ресурсов.

Доказано практикой, что полезно постоянно отчитываться перед руководством, чтобы сохранить хорошую осведомленность о проблемах безопасности, что обеспечит постоянную поддержку CSIRT.

Бизнес-идея начинается с анализа проблем и возможностей, используя аналитическую модель, описанную в главе 5.3 Анализ клиентов, а также с поиска тесного контакта с потенциальными клиентами.

Как было описано ранее, есть многое, над чем надо подумать при запуске CSIRT. Лучше всего корректировать вышеуказанные документы под нужды CSIRT по мере их развития.

Хорошо при докладе руководству представлять свою бизнес-идею как можно более отвечающей современным требованиям, используя свежие статьи из газет или Интернета для объяснения, почему CSIRT-сервис и внутренняя координация инцидентов важна для защиты бизнес активов. Также важно дать понять, что только непрерывная поддержка в вопросах IT безопасности ведет к стабильному бизнесу, особенно это важно для компании или организации, зависящей от информационных технологий.

(Знаменитая фраза Брюса Шнейера подводит к позиции: *“Безопасность – это не продукт, а процесс”¹⁷!*)

Нижеследующий график – известное средство для изображения проблем безопасности, предоставленное CERT/CC:

¹⁷ Bruce Schneier: <http://www.schneier.com/>

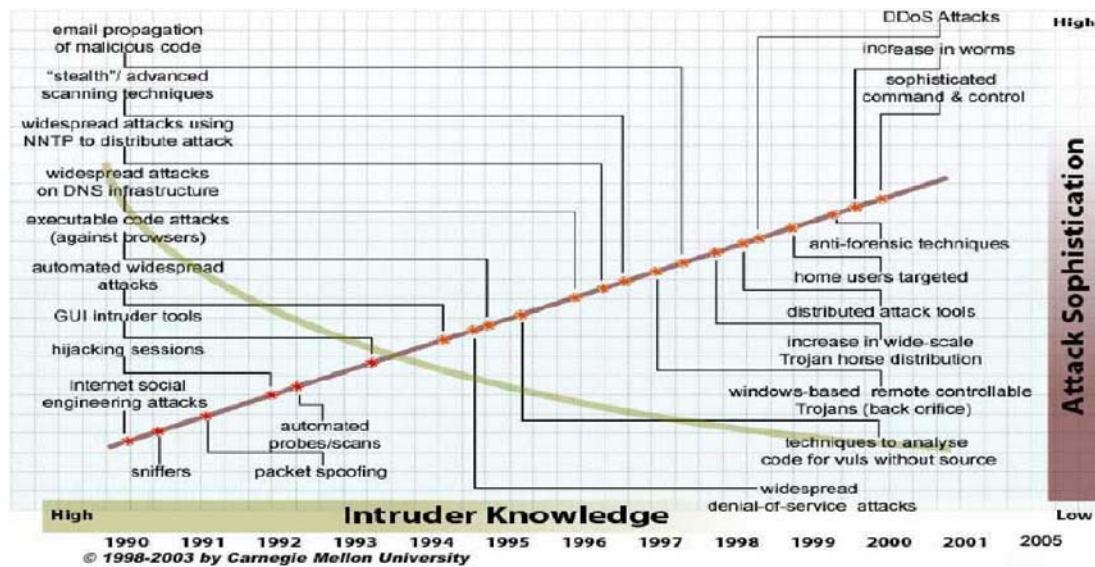


Рис. 8 Знания злоумышленника по отношению к сложности атаки (источник - CERT-CC¹⁸)

Она показывает направление ИТ безопасности, особенно в снижении необходимого уровня знаний для выполнения более сложных атак.

Нужно также отметить постоянно сокращающееся время между доступностью обновлений для софта и началом атак против них:

Заплата -> Эксплойт

Nimda:	11 месяцев
Slammer:	6 месяцев
Nachi:	5 месяцев
Blaster:	3 недели
Witty:	1 день (!)

Скорость распространения

Code red:	Дни
Nimda:	Часы
Slammer:	Минуты

Собранные данные об инцидентах, потенциальное усовершенствование и извлеченные уроки дают хороший материал для презентации.

¹⁸ <http://www.cert.org/archive/pdf/info-sec-ip.pdf>

7.1 Описание бизнес планов и управленческих механизмов

Одна только презентация для руководства, включая продвижение CSIRT, не составляет бизнес идею, но если она выполнена должным образом, то в большинстве случаев приведет к поддержке CSIRT руководством. С другой стороны бизнес идея не должна быть лишь упражнением для менеджмента, она также должна быть использована для коммуникаций между командой и клиентами. Термин «бизнес-идея», может быть, звучит очень по-коммерчески и кажется далеким от ежедневной практики CSIRT, но он дает хороший фокус и направление при запуске CSIRT.

Чтобы оформить хорошую бизнес-идею, можно использовать ответы на следующие вопросы (приведенные примеры гипотетические и использованы исключительно для иллюстрации, реальные ответы очень сильно зависят от реальных обстоятельств):

- В чем проблема?
- Какие цели должны быть достигнуты в работе со своими клиентами?
- Что произойдет, если вы ничего не сделаете?
- Что произойдет, если вы начнете действовать?
- Сколько это будет стоить?
- Какая может быть выгода?
- Когда вы начали и когда закончили?

В чем проблема?

В большинстве случаев идея создать CSIRT возникает, когда IT безопасность становится необходимой частью основного бизнеса компании или организации, и когда инциденты IT безопасности становятся бизнес риском, делая обеспечение безопасности нормальной бизнес-деятельностью.

Большинство компаний или учреждений имеют отдел постоянной поддержки или службу технической поддержки (Helpdesk), но в большинстве случаев инциденты, связанные с безопасностью, обрабатываются неудовлетворительно. В большинстве случаев работа по обработке инцидента безопасности требует особых навыков и внимания. Более структурированный подход также желателен, он смягчит бизнес риски и ущерб компании.

Проблема в большинстве случаев в том, что не хватает координации, а существующие знания не используются для обработки инцидентов, а это предотвратило бы от их повторения в будущем, а также удалось бы предотвратить возможные финансовые потери и/или вред репутации организации.

Какие цели должны быть достигнуты в работе со своими клиентами?

Как было описано ранее, ваша CSIRT будет обслуживать своих клиентов и помогать им в решении проблем и инцидентов IT-безопасности. Дополнительными целями являются повышение уровня знаний об IT-безопасности и развитие культуры знаний о безопасности.

Эта культура отражает активные и превентивные меры, предпринимаемые с самого начала и сокращающие операционные расходы.

Представление этой культуры сотрудничества и помощи компании или учреждению может в большинстве случаев увеличить эффективность в целом.

Что произойдет, если вы ничего не сделаете?

Неструктурированный метод работы с IT-безопасностью может привести к дальнейшему вреду и не только репутации организации. Другими последствиями могут стать финансовые убытки и юридические последствия.

Что произойдет, если вы начнете действовать?

Повышается осведомленность о происшествии, связанном с проблемами безопасности. Это поможет их устранению более эффективно и предотвращению будущих убытков.

Сколько это будет стоить?

В зависимости от организационной модели это будет стоить зарплата членов CSIRT команды и организации, оборудования, инструментария и софта.

Какая может быть выгода?

В зависимости от бизнеса и убытков в прошлом, выгода организации будет в большей прозрачности процедур и инструкциях по безопасности, следовательно, в защите главных бизнес активов.

Когда вы начали и когда закончили? (Сколько это заняло времени?)

Смотрите главу 12 «Описание плана проекта», посвященную описанию примера плана проекта.

Примеры существующих бизнес идей и целей

Вот примеры некоторых бизнес идей CSIRT, которые стоит изучить:

- http://www.cert.org/csirts/AFI_case-study.html
Создание финансового института CSIRT: Учебный пример.

Целью этого документа является передача опыта финансовой организации (в этом документе - AFI) о том, как она выполнила как план по поднятию интереса к безопасности, так и создание Группы Реагирования на Инциденты Компьютерной Безопасности (CSIRT).

- <http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf>
Краткое описание бизнес идеи польской CERT (слайды в формате PDF).
- <http://www.auscert.org.au/render.html?it=2252>
Работа по формированию Группы Реагирования на Инциденты (IRT) в 1990-ых могла ужасать. Многие люди, формирующие Группу реагирования на Инциденты, не имеют в этом опыта. Этот документ рассматривает роль, которую IRT может играть в обществе, а также вопросы, которые должны быть рассмотрены как во время формирования IRT, так и вначале ее деятельности. Он может оказаться полезным для существующих групп реагирования на инциденты, т.к. может увеличить осведомленность в ранее не затронутых вопросах.
- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
Case Изучение Информационной безопасности, обеспечение информационной безопасности компании Роджера Бентона.

Этот практикум – бизнес-идея перехода страховой компании к системе безопасности масштаба предприятия. Смысл практикума – показать путь, которым нужно следовать при создании или переходе к системе безопасности. В начале система безопасности Online была единственным механизмом контроля доступа к корпоративным данным. Незащищенность была высокой – не было проверки целостности за пределами Online среды. Любой, кто имел фундаментальные навыки программирования, мог изменить и/или удалить производственные данные.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
Стратегия электронной безопасности компании Marriott: сотрудничество бизнес – IT.

Опыт Криса Золадза из компании «Marriott International Inc.» показывает, что безопасность электронного бизнеса – это процесс, а не проект. Такое заявление Золадз сделал на недавней конференции по электронной безопасности и выставке в Бостоне, спонсором которых выступала «Intermedia Group». Как вице-президент по защите информации компании Золадз делал доклад от имени юридического департамента, хотя он сам не является юристом. Его функция – определять, где хранится самая ценная информация компании Marriott и как она движется внутри компании и за ее пределами. В Marriott есть отдельная ответственность по поддержанию безопасности технической инфраструктуры, возложенная на архитектора по IT безопасности.

Условная CSIRT (шаг 7)

Продвижение бизнес-плана

Решено собирать факты и цифры из истории компании. Это более, чем полезно для статистического обзора ситуации IT безопасности. Этот сбор должен осуществляться с самого запуска CSIRT, и его следует постоянно обновлять.

Был проведен опрос о бизнес-идеях других национальных CSIRT. Они оказали помощь в сборе информации о недавних IT-инцидентах и стоимости этих инцидентов.

В этом примере условной CSIRT не было острой нужды убеждать руководство в важности IT-бизнеса, поэтому было не сложно получить одобрение на запуск. Были подготовлены бизнес идея и план проекта, также была проведена оценка расходов на запуск CSIRT и операционных расходов.

8 Примеры операционных и технических процедур (рабочих потоков)

Были проделаны следующие шаги:

1. Понимание что такое CSIRT и возможности, которые он предоставляет.
2. Какому сектору новая команда CSIRT будет предоставлять свои сервисы
3. Какого типа сервисы может предоставить CSIRT своим клиентам.
4. Анализ окружающего сообщества и потенциальной клиентуры.
5. Определение основных целей и положений
6. Разработка бизнес плана.
 - a. Определение финансовой модели.
 - b. Определение организационной структуры,
 - c. Первоначальный подбор кадров.
 - d. Подбор и оборудование офиса.
 - e. Разработка политики информационной безопасности
 - f. Поиск потенциальных партнеров.
7. Продвижение бизнес плана.
 - a. Наличие утверждённого бизнес плана
 - b. Занесение вышеперечисленного в план проекта

>> Следующий шаг: начать работу CSIRT

Хорошо определенные рабочие потоки повысят качество и снизят затраты времени на обработку инцидента или проблемы уязвимости.

Как описано в примерах, условная CSIRT будет предоставлять базовые сервисы CSIRT:

- Предупреждения
- Обработка инцидентов
- Объявления

Эта глава предоставляет примеры рабочих потоков, которые описывают основные сервисы CSIRT. Также эта глава содержит информацию о сборе информации из различных источников, проверке ее на соответствие и аутентичность и передаче ее клиентам. И, наконец, эта глава содержит примеры большинства базовых процедур и специфического инструментария CSIRT.

8.1 Оценка установочной базы клиента

Первый шаг – это сбор общей информации, какие IT-системы установлены у Вашего клиента. Благодаря этому CSIRT может оценивать важность входящей информации и фильтровать перед распространением, так что клиенты не будут перегружены информацией, которая практически бесполезна для них.

Рекомендуется начинать с простого, например, используя лист Excel такого вида:

Категория	Приложение	ПО	Версия	ОС	Версия ОС	Клиент
ПК	Офис	Excel	x-x-x	Microsoft	XP-проф	А
ПК	Браузер	IE	x-x-	Microsoft	XP-проф	А
Сеть	Маршрутизатор	Cisco	x-x-x	CISCO	x-x-x	А
Сервер	Сервер	Linux	x-x-x	L-distro	x-x-x	Б
Сервисы	Веб сервер	Apache		Unix	x-x-x	Б

Используя функцию фильтра в Excel, будет очень просто выбирать необходимое ПО и смотреть, какой клиент использует определенный тип ПО.

8.2 Создание сигналов тревоги, предупреждений и объявлений

Создание сигналов тревоги, предупреждений и объявлений идет по одной схеме:

- Сбор информации
- Проверка важности и источника информации
- Оценка риска на основе собранной информации
- Распространение информации

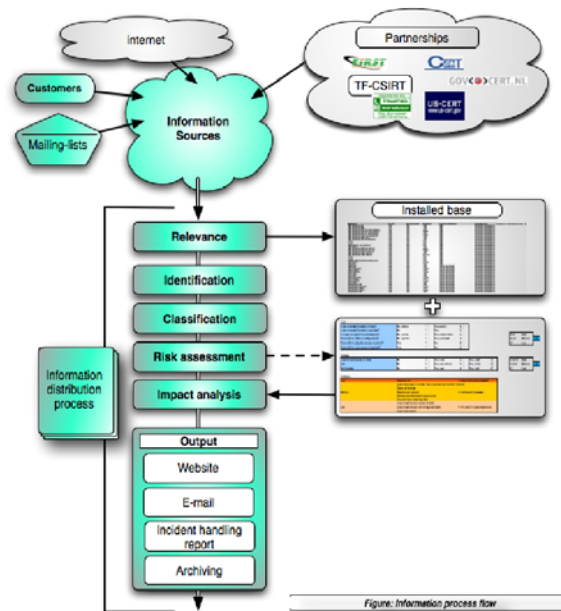
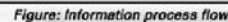


Рис. 9: процесс обработки информации

В следующих параграфах эта схема работы будет описана более детально.



Шаг 1: Сбор информации об уязвимости.

Обычно существует два основных типа источников информации, которые предоставляют входную информацию для сервисов:

- Информация об уязвимости (Вашей) IT-системы
- Отчеты об инцидентах

В зависимости от вида деятельности и ИТ-инфраструктуры, существует много публичных и закрытых источников информации об уязвимостях:

- Публичные и закрытые списки почтовой рассылки
- Информация об уязвимостях от производителей
- Веб-сайты
- Информация в Интернет (Google и другие)
- Публичные и личные контакты, которые предоставляют информацию об уязвимостях (FIRST, TFC SIRT, CERT-CC, US-CERT....)

Вся эта информация поднимает уровень знаний о специфических уязвимостях IT-систем.

Как говорилось раньше, в Интернете есть много источников хорошей и легкодоступной информации о безопасности. Специальная рабочая группа ENISA «CERT сервисы» в 2006 году, в момент написания этой книги, создавала более полный список, который должен появиться к концу 2006 года¹⁹.

Шаг 2: Проверка информации и оценка риска

Этот шаг приведет к анализу последствий специфической уязвимости на IT-инфраструктуру клиента.

Идентификация

Источник входящей информации об уязвимости всегда должен идентифицироваться и всегда необходимо определять, можно ли доверять источнику, перед отправкой любой информации клиенту. В противном случае, люди могут быть встревожены по ошибке, что может привести к ненужным беспокойствам в бизнес-процессах и, в конечном итоге, нанести урон репутации CSIRT.

¹⁹ Сервисы специальной рабочей группы CERT:
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Следующая процедура является примером проверки подлинности сообщения:

Процедура проверки подлинности сообщения и источника

Перечень основных вопросов

- 1 Источник известен и зарегистрирован как таковой?
- 2 Информация поступила по обычному каналу?
- 3 Есть ли там «странная» информация, которая «кажется» ошибочной?
- 4 Следуйте своим чувствам, если есть сомнение в информации, не спешите реагировать на нее, а проверьте еще раз!

E-mail источники

- 1 Адрес отправителя известен организации и известен списку источников?
- 2 Верна ли PGP-подпись?
- 3 В случае сомнений проверьте полные заголовки сообщения.
- 4 В случае сомнений, используйте “nslookup” или “dig”, чтобы уточнить домен отправителя²⁰.

WWW - источники

- 1 Проверьте сертификаты браузера, когда подключаетесь к защищенным сайтам (https://).
- 2 Проверьте источник содержания и правильность (техническую).
- 3 Если сомневаетесь, не нажимайте ни на какие ссылки и не скачивайте никаких программ.
- 4 Если сомневаетесь, проверьте домен с помощью “lookup” и “dig” и сделайте “traceroute”.

Телефон

- 1 Внимательно слушайте Имя и Фамилию.
- 2 Вы узнали голос?
- 3 Если сомневаетесь, спросите телефонный номер и перезвоните сами.

Рис. 10. Пример процедуры идентификации информации

Актуальность

Обзор установленного оборудования и программного обеспечения, сделанный ранее, может использоваться для определения актуальности входящей информации об уязвимостях, с целью найти ответ на вопросы: «Клиент использует данное программное обеспечение?», «Актуальна ли эта информация для клиента?»

Классификация

Некоторая полученная информация может быть классифицирована или помечена как для служебного пользования (например, входящие отчеты об инцидентах от других команд). Вся информация должна обрабатываться в соответствии с требованиями отправителя и собственной политикой информационной безопасности. Есть хорошее базовое правило: *«Не распространяйте информацию, если не уверены, что она предназначена для этого, а если сомневаетесь, спросите у отправителя разрешение не распространение».*

²⁰ Инструменты для проверки подлинности CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Оценка рисков и анализ последствий

Существует несколько методов определения риска и последствий (возможной) уязвимости.

Риск определяют как потенциальную возможность того, что уязвимость может быть использована. Перечислим несколько важных факторов (среди остальных):

- Уязвимость широко известна?
- Уязвимость распространена?
- Легко ли воспользоваться уязвимостью?
- Можно ли воспользоваться уязвимостью удаленно?

Все эти вопросы помогают понять серьезность уязвимости.

Следующая формула является простым подходом к оценке риска:

Последствия = Риск X Потенциальные повреждения

Потенциальными повреждениями могут быть:

- Несанкционированный доступ к данным
- Отказ в сервисе (DOS)
- Получение или расширение прав доступа

(Расширенные классификационные схемы смотрите в конце этой главы).

Ответив на эти вопросы, можно добавить общий рейтинг в бюллетень, информирующий о потенциальном риске и повреждениях. Часто используются простые термины НИЗКИЙ, СРЕДНИЙ и ВЫСОКИЙ.

Другие, более сложные схемы оценки риска:

Схема GOVCERT.NL²¹

Голландский правительственный CSIRT GOVCERT.NL разработал матрицу для оценки риска, которая была создана, когда Govcert.nl только начинал работать и сейчас он обновляется в соответствии с последними вениями.

РИСК					
Уязвимость хорошо известна?	Нет, ограниченно	1	Да, публична	2	
Уязвимость распространена?	Нет	1	Да	2	
Легко ли воспользоваться уязвимостью?	Нет, хакер	1	Да, любитель	2	
Precondition: default configuration?	Нет, особенная	1	Да, стандартная	2	
Предусловия: необходим ли физический доступ?	Да	1	Нет	2	
Предусловия: необходима ли учетная запись?	Да	1	Нет	2	
Повреждения					
Несанкционированный доступ к данным	Нет	0	Да, чтение	2	Да, чтение+ 4
DoS	Нет	0	Да, некритический	1	Да, критический 5
Права доступа	Нет	0	Да, пользователь	4	Да, администратор 6
Общее					
Высокий	Удаленное администрирование Локальный взлом администратора (атакующий имеет учетную запись на машине) Отказ в обслуживании Удаленный взлом пользователя Несанкционированный удаленный доступ к данным Несанкционированное получение информации Несанкционированный локальный доступ к данным Несанкционированное локальное получение прав Взлом локального пользователя				
Средний	>> Небходима срочная реакция! >> Решить в течение недели				
Низкий	>> Включить в генеральный список				

Рис. 11 Схема рейтингов The GOVCERT.NL

Описание общего формата бюллетеня EISPP²²

Европейская программа по продвижению информационной безопасности (EISPP) – это проект, финансируемый Европейским Сообществом в рамках Пятой рамочной программы. Проект EISPP направлен на развитие Европейской структуры не только для развития знаний о безопасности, но и для определения содержания и направления распространения информации о безопасности малому бизнесу. Предоставляя европейским малым предприятиям необходимые сервисы по IT-безопасности, осуществляется их поддержка в увеличении доверия и использования электронной коммерции, что приведет к увеличению и улучшению возможностей для нового бизнеса. EISPP – пионер в видении Европейской Комиссии по формированию Европейской сети экспертизы в Европейском союзе.

DAF – Немецкий формат бюллетеня²³

DAF – инициатива Германского CERT-Verbund и ключевой компонент инфраструктуры по созданию и обмену бюллетенями безопасности между разными командами. DAF стандарт, созданный специально для нужд немецких CERT-ов, который совершенствуется и поддерживается такими командами как CERT-Bund, DFN-CERT, PRESECURE и Siemens-CERT.

²¹ Матрица уязвимостей: <http://www.govcert.nl/download.html?f=33>

²² EISPP: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#03

²³ DAF: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#02

3

Шаг 3: Распространение информации

CSIRT может выбрать один из нескольких методов распространения, в зависимости от пожеланий клиентов и Вашей коммуникационной стратегии.

- Веб-сайт
- Электронная почта
- Отчеты
- Архивирование и исследования

Бюллетени безопасности, распространяемые CSIRT, всегда должны иметь одинаковую структуру. Это увеличит читабельность, и читатель сможет быстро найти всю важную информацию.

Бюллетень должен содержать как минимум следующую информацию:

Название бюллетеня	
Номер	
Пораженные системы - -	
ОС и ее версия	
Риск	(Высокий-Средний-Низкий)
Последствия/потенциальный повреждения	(Высокий-Средний-Низкий)
Внешние ID:	(CVE, Vulnerability bulletin ID's)
Обзор уязвимости	
Последствия	
Решение	
Описание (детали)	
Приложение	

Рис. 12 Пример схемы бюллетеня



Смотрите главу 10. Упражнение для получения полного примера бюллетеня безопасности.

8.3 Процесс обработки инцидентов

Как упомянуто в введении этой главы, процессы обработки информации во время обработки инцидента и во время создания сигналов тревоги, предупреждений и объявлений очень похожи. Но обычно часть сбора информации отличается, так как обычно информацию, касающуюся инцидента, получают посредством отчетов об инцидентах от клиентов или других команд или отзывов от вовлеченных сторон во время обработки инцидента. Информация обычно поступает через (зашифрованный) e-mail, иногда посредством телефона или факса.

При получении информации по телефону рекомендуется сразу отметить каждую деталь используя программу по обработке/отчету об инцидентах или просто сделав заметку. Это необходимо для того, чтобы незамедлительно (до конца телефонного разговора) сгенерировать номер инцидента (если его не создали до сих пор) и передать его звонящему (или в итоговом электронном письме после разговора) как ссылку для дальнейшего общения.

Оставшаяся часть этой главы описывает базовый процесс обработки инцидента. Очень подробный анализ полного процесса работы с инцидентами и всех сопутствующих рабочих потоков и субпотоков можно найти в документации CERT/CC Defining Incident Management processes for CSIRTs²⁴.

²⁴ Defining Incident Management Processes: <http://www.cert.org/archive/pdf/04tr015.pdf>

В основном, обработка инцидентов соответствует следующему рабочему потоку:

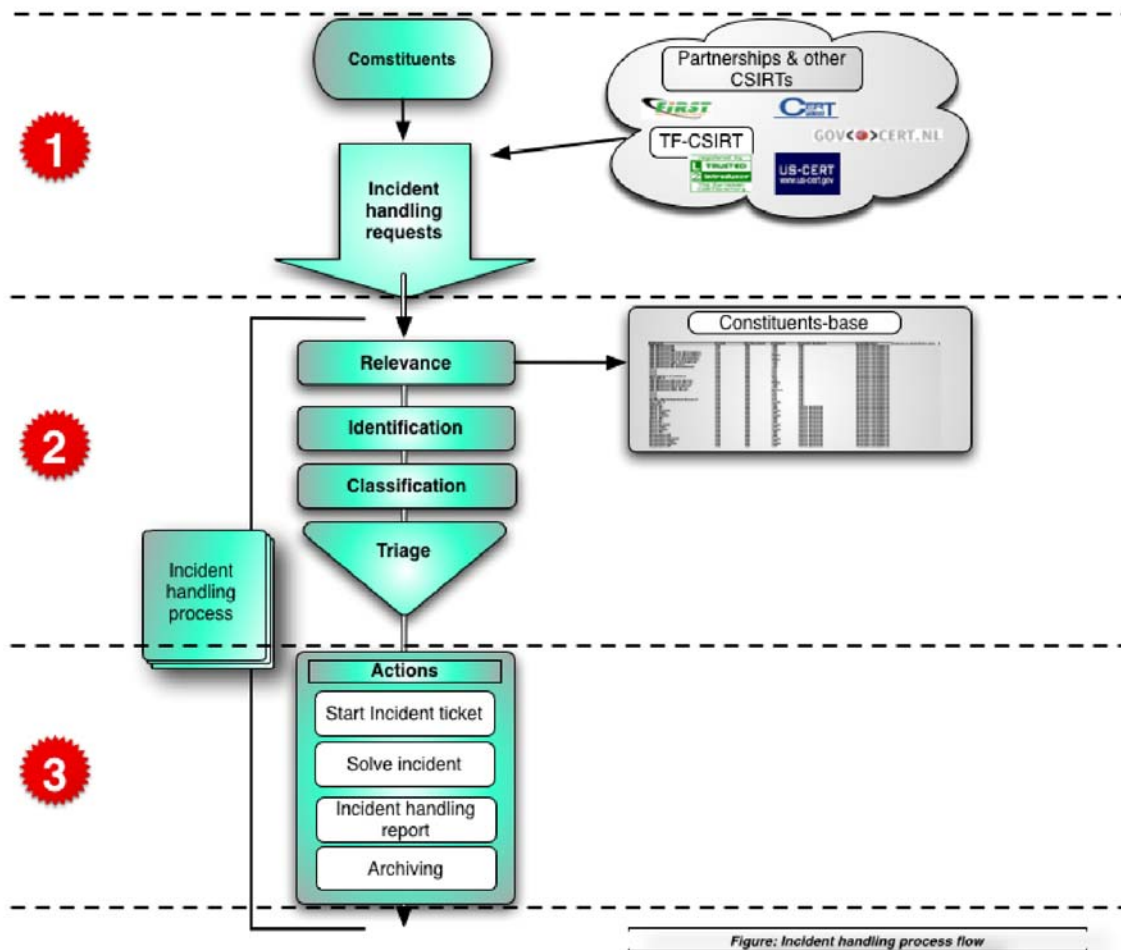


Рис. 13 Поток обработки инцидента

**Шаг 1: Получение отчетов об инцидентах**

Как ранее говорилось, отчеты об инцидентах поступают в CSIRT по нескольким каналам, главным образом, по e-mail, но также по телефону и факсу.

Как говорилось ранее, рекомендуется записывать все детали в фиксированном формате во время получения отчета об инциденте. Благодаря этому можно быть уверенными, что никакая важная информация не упущена. Ниже приведен образец схемы:

ФОРМА ОТЧЕТА ОБ ИНЦИДЕНТЕ	
<i>Пожалуйста, заполните эту форму и отправьте по факсу или email: Строки, помеченные *, обязательны для заполнения.</i>	
<i>Имя и организация</i>	
1.	Имя*:
2.	Название организации*:
3.	Сектор:
4.	Страна*:
5.	Город:
6.	E-Mail адрес*:
7.	Номер телефона*:
8.	Другое:
<i>Пораженный компьютер(ы)</i>	
9.	Количество компьютеров:
10.	Hostname и IP*:
11.	Функции компьютера*:
12.	Часовой пояс:
13.	Оборудование (конфигурация):
14.	Операционная система:
15.	Поврежденное ПО:
16.	Поврежденные файлы:
17.	Безопасность:
18.	Hostname и IP:
19.	Протокол/порт:
<i>Инцидент</i>	
20.	Номер инцидента #:
21.	Тип инцидента:
22.	Время начала инцидента:
23.	Это постоянный инцидент: ДА НЕТ
24.	Время и метод обнаружения:
25.	Известные уязвимости:
26.	Подозрительные файлы:
27.	Противомеры:
28.	Детальное описание*:

Рис. 14 Содержание отчета об инциденте

2

Шаг 2: Проверка инцидента

На этом шаге проверяются аутентичность и важность инцидента, а также инцидент классифицируется.

Идентификация

Для предотвращения ненужных действий рекомендуется всегда проверять отправителя, является ли он благонадежным и является ли он одним из Ваших или дружественных Вам CSIRT-клиентов. Действуют те же правила, что описаны в пункте 8.2 *Создание сигналов тревоги*.

Актуальность

На этом шаге Вы проверяете, пришел ли запрос на обработку инцидента от клиента CSIRT или касается ли инцидент IT-систем Вашего клиента. Если ни одно из условий не выполняется, обычно инцидент перенаправляется в подходящую CSIRT²⁵.

Классификация

На этом шаге подготавливается сортировка путем классификации опасности инцидента. Детали классификации инцидента находятся за рамками данного документа. Рекомендуем начать с использования схемы Классификации дел CSIRT (образец для Корпоративной CSIRT):

Incident Categories

All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	DOS or DDOS attack.
Forensics	S1	Any forensic work to be done by CSIRT.
Compromised Information	S1	Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	- Sharing offensive material, sharing/possession of copyright material. - Deliberate violation of Infosec policy. - Inappropriate use of corporate asset such as computer, network, or application. - Unauthorized escalation of privileges or deliberate attempt to subvert access controls.

* - Sensitivity will vary depending on circumstances. Guidelines are provided.

Рис. 15 Схема классификации инцидентов (источник: FIRST)²⁶

²⁵ Инструменты для проверки подлинности в CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

²⁶ Классификация дел CSIRT http://www.first.org/resources/guides/csirt_case_classification.html

Сортировка

Сортировка (Triage) – это система, которая используется медицинскими или аварийными службами для распределения ограниченных ресурсов, когда количество раненых, нуждающихся в заботе, превышает доступные ресурсы, таким образом, чтобы помочь максимальному числу больных²⁷.

CERT/CC дает следующее описание:

Сортировка – это важнейший элемент возможности управления инцидентом, особенно для любого сложившейся CSIRT. Сортировка находится на важнейшем пути понимания, какая информация распространяется по организации. Она служит как автомобиль, на котором вся информация поступает в одну точку контакта, позволяя предприятию видеть текущую активность и полную взаимосвязь всей поступившей информации. Она также предоставляет стартовую площадку для документирования и ввода информации отчета или запроса, если это не было сделано в процессе Распознавания.

Функция сортировки предоставляет возможность сделать мгновенный снимок статуса всех процессов, о которых сообщено, – какие отчеты открыты или закрыты, какие действия предстоит сделать, и сколько отчетов каждого типа было получено. Этот процесс может помочь выявить возможные проблемы безопасности и распределить приоритет рабочей нагрузки. Информация, собранная в процессе сортировки, также может использоваться для генерации трендов об уязвимостях и инцидентах, а также статистики для высшего менеджмента²⁸.

Сортировка может выполняться только наиболее опытными членами команды, потому что она требует глубокого понимания потенциального ущерба от инцидентов на специфические части клиента и возможности принимать решение, какой участник команды лучше справится с инцидентом.

²⁷ В Wikipedia: <http://en.wikipedia.org/wiki/Triage>

²⁸ Определение процессов управления инцидентами: <http://www.cert.org/archive/pdf/04tr015.pdf>

Шаг 3: Действия

Обычно отсортированные элементы поступают в очередь запросов программы обработки инцидентов, которая используется одним или более обработчиками инцидентов, которые следуют этим путем.

Ярлык начала инцидента

Номер ярлыка инцидента уже мог быть создан на предыдущем шаге (например, когда об инциденте сообщили по телефону). Если нет, то первым шагом является создание такого номера, который будет использоваться в дальнейших обсуждениях этого инцидента.

Жизненный цикл инцидента

Обработка инцидента не следует линии шагов, которые в конце приводят к решению, а скорее следует кругу шагов, которые повторяются, пока инцидент не решится и все вовлеченные стороны не получат всей необходимой информации. Этот круг, также называемый «Жизненным циклом инцидента», содержит следующие процессы:

<i>Анализ:</i>	Все детали полученного инцидента анализируются
<i>Получение контактной информации:</i>	чтобы иметь возможность в дальнейшем сообщить информацию об инциденте вовлеченным сторонам, например, другим CSIRT, жертвам и возможным владельцам систем, которые могли быть использованы для атаки.
<i>Предоставление технической помощи:</i>	Помогите жертвам быстро восстановиться от последствий инцидента и собрать больше информации об атаке.
<i>Координация:</i>	Проинформируйте другие вовлеченные стороны, например, CSIRT, ответственная за IT-систему, с которой производились атаки, или другие жертвы.

Эта структура называется жизненным циклом, один шаг ведет к другому и последний, координация, может вести к новому анализу и цикл начинается снова. Процесс заканчивается, когда все вовлеченные стороны получили и предоставили всю необходимую информацию.

Обратитесь к книге «CERT/CC CSIRT handbook» за более детальным описанием жизненного цикла инцидента²⁹.

Отчет об обработке инцидента

Подготовьтесь к вопросам от руководства об инцидентах, составив отчет. Также рекомендуется написать документ (для внутреннего пользования) о «полученных уроках» для обучения персонала и для избежания ошибок в будущем при обработке инцидентов.

Архивирование

Правила архивирования описаны ранее в главе 6.6 *Разработка политики информационной безопасности*.

Обратитесь к Приложению А.1 за более подробной информацией по управлению инцидентами и жизненным циклам инцидентов.

²⁹ Учебник CSIRT: <http://www.cert.org/archive/pdf/csirt-handbook.pdf>

8.4 Образец графика реагирования

Часто забывают об определении времени реагирования, но оно должно быть частью каждого хорошо разработанного соглашения сервисного уровня (SLA) между CSIRT и клиентом. Предоставление своевременного ответа клиентам в процессе обработки инцидента чрезвычайно важно, как для собственных обязательств клиента, так и для репутации команды.

Время реагирования должно быть четко оговорено с клиентом, чтобы избежать неправильных ожиданий. Следующий очень простой график может использоваться как начальная точка для более детального SLA с клиентом CSIRT.

Вот образец практического графика ответа с момента поступления запроса на помощь:

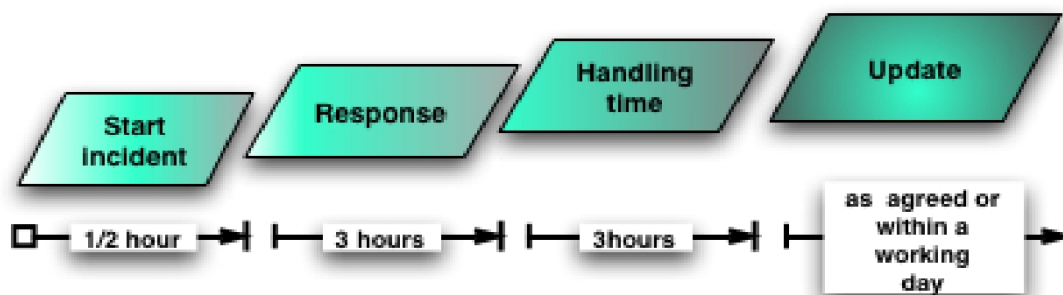


Рис. 16 Образец графика реагирования

Также рекомендуется проинструктировать клиента об их собственном времени реагирования, особенно при контакте с CSIRT в случае происшествия. В большинстве случаев связываться со своей CSIRT на ранней стадии и рекомендуется поощрять клиентов делать это при возникновении сомнений.

8.5 Доступные инструменты для работы CSIRT

Эта глава предоставляет ссылки на широко распространенные инструменты, используемые CSIRT-ами. Здесь представлены только примеры, большее количество ссылок может быть найдено в Clearinghouse of Incident Handling Tools³⁰ (CHIHT).

Программное обеспечение для шифрования email и сообщений

- GNUPG <http://www.gnupg.org/>
GnuPG – это полностью бесплатная реализация проектом GNU стандарта OpenPGP, который описан в RFC2440. GnuPG позволяет кодировать и подписывать Вашу информацию и переговоры.

- PGP <http://www.pgp.com/>
Коммерческий вариант.

Инструменты по обработке инцидентов

Администрирование инцидентов и их завершение, протоколирование действий.

- RTIR <http://www.bestpractical.com/rtir/>
RTIR – бесплатная open source система по обработке инцидентов, разработанная под потребности команд CERT и других команд реагирования на инциденты.

CRM инструменты

Когда у Вас есть много различных клиентов и необходимо вести записи всех встреч и деталей, база данных CRM очень полезна. Существует много вариаций, мы приведем два образца:

- SugarCRM <http://www.sugarcrm.com/crm/>
- Sugarforce (бесплатная open source версия) <http://www.sugarforge.org/>

Проверка информации

- Website watcher <http://www.aignes.com/index.htm>
Эта программа следит за изменениями и изменениями web-сайтов

- Watch that page <http://www.watchthatpage.com/>
Этот сервис посылает информацию об изменениях в web-сайтах по e-mail (бесплатная и коммерческая версии)

³⁰ CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Поиск контактной информации

Поиск правильной контактной информации для сообщения об инцидентах – непростая задача. Существует несколько информационных источников, которыми можно пользоваться:

- RIPE³¹
- IRT-object³²
- TI³³

Дополнительно CHINT предлагает некоторые инструменты для поиска контактной информации³⁴.

Условная CSIRT (шаг 8)**Наладка потоков процесс и операционных и технических процедур**

Условная CSIRT фокусируется на предоставлении ключевых CSIRT-сервисов:

- Сигналы тревоги и предупреждения
- Объявления
- Обработка инцидентов

Команда разработала процедуры которые хорошо работают и понятны каждому члену команды. Условная CSIRT также нанял юриста, чтобы решать вопросы обязательств и политики информационной безопасности. Команда выбрала некоторые полезные инструменты и нашла полезную информацию о рабочих вопросах благодаря обсуждению с другими CSIRT.

Был создан фиксированный шаблон для бюллетеней безопасности и отчетах об инцидентах. Команда использует RTIR для обработки инцидентов.

³¹ RIPE whois: <http://www.ripe.net/whois>

³² IRT-object in the RIPE database: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

³³ Trusted Introducer: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

³⁴ Инструменты для проверки подлинности в CHINT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 CSIRT-тренинг

Были проделаны следующие шаги:

1. Понимание что такое CSIRT и возможности, которые он предоставляет.
2. Какому сектору новая команда CSIRT будет предоставлять свои сервисы
3. Какого типа сервисы может предоставить CSIRT своим клиентам.
4. Анализ окружающего сообщества и потенциальной клиентуры.
5. Определение основных целей и положений
6. Разработка бизнес плана.
 - a. Определение финансовой модели.
 - b. Определение организационной структуры,
 - c. Первоначальный подбор кадров.
 - d. Подбор и оборудование офиса.
 - e. Разработка политики информационной безопасности
 - f. Поиск потенциальных партнеров.
7. Продвижение бизнес плана.
 - a. Наличие утверждённого бизнес плана
 - b. Занесение вышеперечисленного в план проекта
8. Создание действующего CSIRT.
 - a. Создание делопроизводства
 - b. Внедрение утилит CSIRT

>>Следующий шаг: обучение персонала

Данная глава включает 2 основных источника посвященных CSIRT-тренингу: TRANSITS и курсы CERT/CC.

9.1 TRANSITS

TRANSITS был разработан как европейский проект для ускорения создания Групп Реагирования на Инциденты Компьютерной Безопасности (CSIRT) и увеличения эффективности существующих CSIRT, с целью решения проблемы нехватки опытного CSIRT-персонала. Эта цель была достигнута внедрением специальных обучающих курсов, для того чтобы обучить персонал (новых) CSIRT организационным, операционным, техническим, маркетинговым и юридическим задачам, связанным с внедрением CSIRT-сервисов.

В частности, TRANSITS включает

- разработанный, обновлённый и регулярно исправляемый состоящий из модулей материал для обучающих курсов
- организацию обучающих семинаров, где читаются материалы курсов
- возможность участия персонала (новых) CSIRT в данных обучающих семинарах, особенно участие персонала из Стран, вступивших в Европейский Союз.
- Распространение материалов обучающих курсов и гарантия их использования³⁵.

³⁵ TRANSITS: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#11



ENISA содействует и поддерживает TRANSITS курсы. Если вы хотите узнать, как пройти данные курсы, а также требования и цены, пожалуйста, обращайтесь к экспертам ENISA CSIRT:

CERT-Relations@enisa.europa.eu

Примеры приведены в приложении к этому документу!

9.2 CERT/CC

Сложность компьютерной и сетевой инфраструктуры, а также требования администрации затрудняют правильное управление сетевой безопасностью. Сетевые и системные администраторы не располагают достаточным количеством персонала и опытом в обеспечении безопасности для защиты от атак и минимизации повреждений. Как результат увеличение количества инцидентов нарушения компьютерной безопасности. Когда возникают инциденты взлома компьютерной безопасности, организаторы должны отреагировать быстро и эффективно. Чем быстрее организация распознает, проанализирует и отреагирует на инцидент тем быстрее сократится количество повреждений и тем меньше будут затраты на восстановление. Формирование CSIRT это наилучший путь обеспечения быстрого реагирования, а также помощи в предотвращении будущих инцидентов.

CERT-CC предоставляют курсы для менеджеров и технического персонала в таких областях как: создание и управление CSIRT-ами, реагирование на инциденты и их анализ, и улучшение безопасности сетей. Если в иных случаях отмечено что, все курсы проводятся в Питсбурге. РА члены, из наших сотрудников, также проходят обучающие курсы по безопасности в Университете Carnegie Mellon.

Доступные курсы³⁶ CERT/CC посвященные CSIRTs

Создание CSIRT

Менеджмент CSIRT

Основы обработки инцидентов

Дополнительная обработка инцидентов для технического персонала

Примеры приведены в приложении к этому документу!

Условная CSIRT (шаг 9)

Тренинг персонала

Условная CSIRT решила послать весь свой технический персонал на следующие доступные курсы TRANSITS. Руководитель команды дополнительно проходит курс от CERT/CC «Менеджмента CSIRT».

³⁶ Курсы CERT/CC: <http://www.sei.cmu.edu/products/courses>

10 Пример: создание рекомендаций

Были проделаны следующие шаги:

1. Понимание что такое CSIRT и возможности, которые он предоставляет.
2. Какому сектору новая команда CSIRT будет предоставлять свои сервисы
3. Какого типа сервисы может предоставить CSIRT своим клиентам.
4. Анализ окружающего сообщества и потенциальной клиентуры.
5. Определение основных целей и положений
6. Разработка бизнес плана.
 - a. Определение финансовой модели.
 - b. Определение организационной структуры,
 - c. Первоначальный подбор кадров.
 - d. Подбор и оборудование офиса.
 - e. Разработка политики информационной безопасности
 - f. Поиск потенциальных партнеров.
7. Продвижение бизнес плана.
 - a. Наличие утверждённого бизнес плана
 - b. Занесение вышеперечисленного в план проекта
8. Создание действующего CSIRT.
 - a. Создание делопроизводства
 - b. Внедрение утилит CSIRT
9. Обучение персонала

» Следующий шаг это упражнение и подготовка к реальной работе!

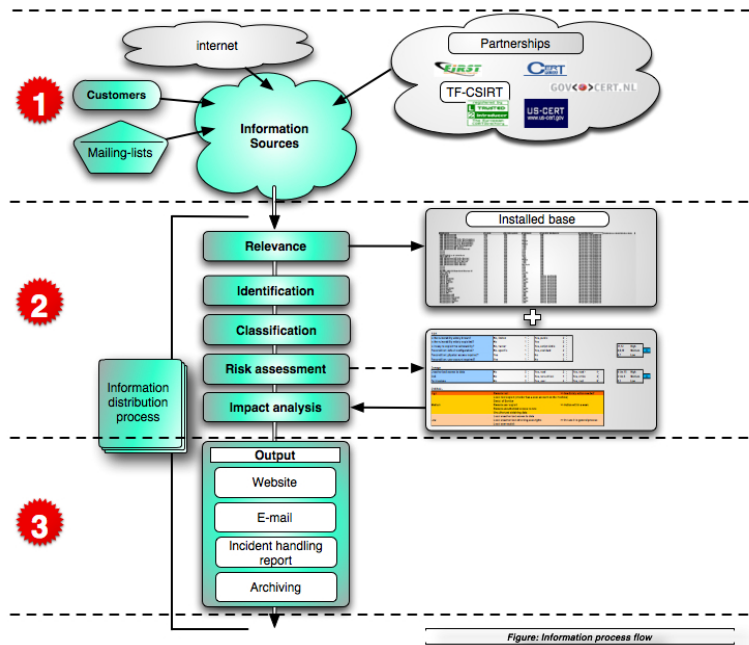
Для наглядной иллюстрации данная глава описывает пример обыкновенного каждодневного задания для CSIRT: создание советов по безопасности.

Первоначальным источником является совет по безопасности, присланный Microsoft:

Идентификатор сообщения	Сообщение безопасности Microsoft MS06- 042
Заголовок сообщения	Сборное обновление системы безопасности для Internet Explorer (918899)
Административное резюме	Данное обновление устраняет некоторые уязвимости в Internet Explorer, которые позволяли Удаленное исполнение кода.
Уровень опасности	Критический
Воздействие уязвимости	Удаленное исполнение кода
Поражённое программное обеспечение	Windows, Internet Explorer. Для более полной информации, просмотрите пораженное программное обеспечение, загрузив определённую секцию.

Это сообщение разработчика относится к ранее найденной уязвимости в Internet Explorer. Разработчик опубликовал различные исправления для этого программного продукта для различных версий Microsoft Windows.

Условная CSIRT, после получения информации о данной уязвимости посредством рассылки, начал с последовательности действий описанной в главе 8.2 *Генерация оповещений, предупреждений и объявлений*



1

Шаг 1: Сбор информации об уязвимости.

Первый шаг это просмотр web сайта разработчика. Условная CSIRT проверяет достоверность информации и собирает дополнительные детали об уязвимостях и повреждённых информационных системах.



Шаг 2: Оценка информации и определение рисков

Оповещение

Теперь информация об уязвимости проверена из нескольких источников: по содержанию сообщения полученного по электронной почте и тексту с web сайта разработчика.

Важность

Условная CSIRT сверяет список повреждённых систем, найденных на сайте, со списком систем используемых клиентами. Было выяснено, что как минимум один из клиентов использует Internet Explorer, таким образом, уязвимость признана важной.

Категория	Приложение	Продукт ПО	Версия	ОС	Версия ОС	Клиент
Настольное приложение	Browser	IE	x-x-	Microsoft	XP-prof	A

Классификация

Информация общедоступна, поэтому открыта для использования и распространения.

Определение рисков и анализ повреждений (воздействий)

Ответ на вопрос указывает, что риск и уровень влияния высокий (оценён как критичный Майкрософтом).

РИСКИ

Является ли уязвимость известной?	Да
Является ли уязвимость широко распространённой?	Да
Легко ли использовать уязвимость?	Да
Возможно ли удалённое использование уязвимости?	Да

ПОРАЖЕНИЕ

Возможное воздействие: удалённый контроль и потенциальная возможность удаленного выполнения кода. Данная уязвимость состоит из множества проблем, делающие риск поражения высоким.



Шаг 3: Распространение

Условная CSIRT является внутренней CSIRT. Есть следующие доступные каналы связи: электронная почта, телефон и внутренний web сайт. CSIRT создаёт рекомендации, полученные из шаблонов главы 8.2 *Генерация оповещений, предупреждений и объявлений*.

Заголовок рекомендации Множественные уязвимости были найдены в «Internet explorer»	
Ссылка номер: 082006-1	
Пораженные системы Все настольные приложения, работающие под Microsoft	
Связанные ОС + версия Microsoft Windows 2000 Service Pack 4 Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2 Microsoft Windows XP Professional x64 Edition Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1 Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems Microsoft Windows Server 2003 x64 Edition	
Риск (Высокий-Средний-Низкий) Высокий	
Влияние/возможное повреждение (Высокое –Среднее - Низкое) Высокое	
Внешний(е) Идентификатор(ы): (CVE, Идентификатор бюллетеня уязвимости) MS-06-42	
Обзор уязвимости Майкрософт нашёл несколько критических уязвимостей в «Internet Explorer», которые могут привести к удалённому выполнению кода.	
Влияние Взломщик может получить полный контроль над системой: устанавливать программы, добавлять пользователей и просматривать, изменять или удалять данные. Смягчающим фактором является то, что всё вышеперечисленное может произойти, только если пользователь вошёл в систему с правами администратора. Пользователь, вошедший в систему с ограниченными правами, имеет меньше влияния на систему.	
Решение Немедленная установка заплатки для IE	
Описание (детали) Дополнительная информация ms06-042.mspk	
Приложение Дополнительная информация ms06-042.mspk	



Теперь данная рекомендация готова для распространения. Так как это критический бюллетень, рекомендуется по возможности оповестить клиентов.

Условная CSIRT (шаг 10)**Испытание**

В течении нескольких первых недель функционирования, Условный CSIRT использовал несколько выдуманных ситуаций, (которые они взяли как пример от других CSIRTs) которые они использовали как упражнения. Более того, они выпустили несколько рекомендации по безопасности основанных на реальной информации об уязвимости распространённой разработчиками программного обеспечения и оборудования, которую они уточнили и сделали пригодной к требованиям клиентов.

11 Заключение

На данном этапе руководство заканчивается. Данный документ предназначен для получения очень краткого обзора разнообразных процессов необходимых для создания CSIRT. Он не является всеобъемлющим документом, а также не вдаётся в специфические детали. Смотрите приложение A. 1. Список дополнительной литературы, в данном разделе описаны статьи с дополнительной информацией.

Следующие важные шаги для условной CSIRT:

- Получение отзывов от клиентов для уточнения предоставленных сервисов
- Создание установленного порядка ежедневных действий
- Проработка внештатных ситуаций, требующих быстрого реагирования
- Находится в тесном контакте с различными CSIRT сообществами с целью добровольного содействия

12 Описания плана проекта

Замечание: План проекта это первый подсчёт необходимого времени. В зависимости от доступных ресурсов варьируются реальные сроки проекта.

План проекта доступен в различных форматах на CD и на электронной странице ENISA. Он полностью охватывает все процессы, описанные в данном документе.

Основным форматом будет являться «Microsoft Project», поэтому он может быть непосредственно использован как инструмент управления данного проекта.

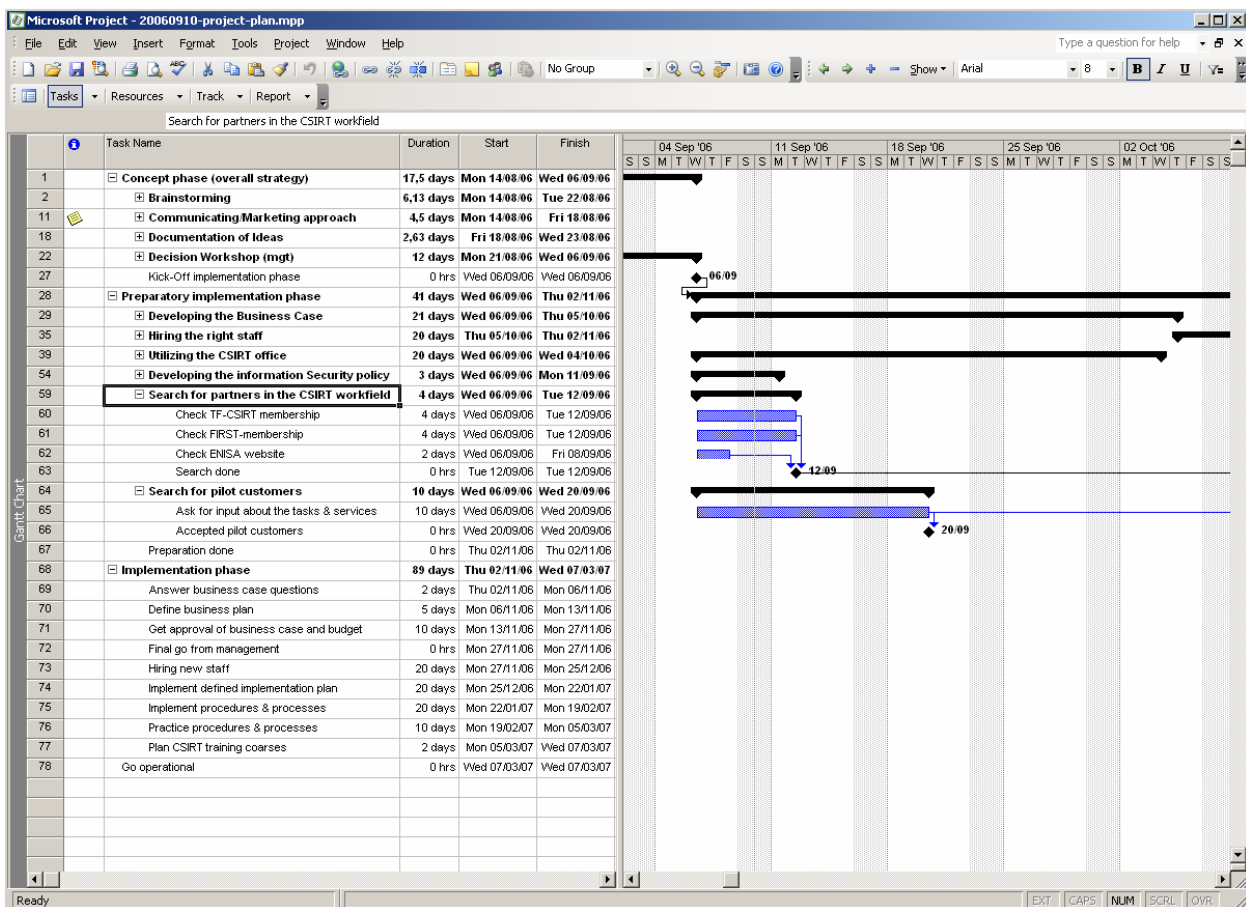


Рис. 17 План проекта

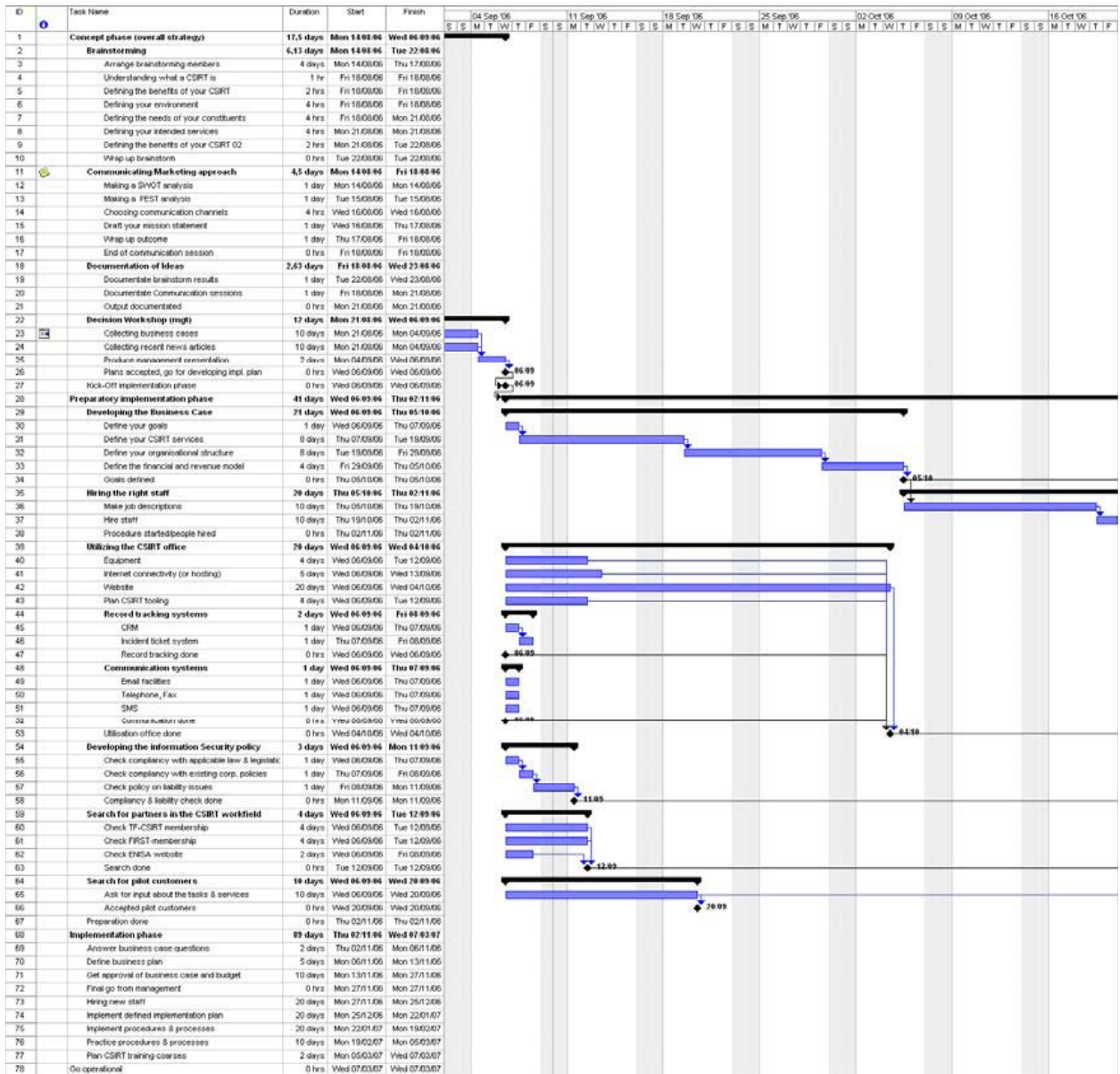


Рис. 18 План проекта со всеми заданиями и частью Gantt chart

План также доступен в CVS и XML форматах. Дальнейшая модернизация может быть запрошена у экспертов CSIRT из ENISA:

CERT-Relations@enisa.europa.eu

ПРИЛОЖЕНИЕ

A.1 Дополнительная литература

Настольная книга для CSIRT (CERT/CC)

Весьма обширное дополнение ко всем главам относящимся к работе CSIRT.

Источник: <http://www.cert.org/archive/pdf/csirt-handbook.pdf>

Определение процессов управления инцидентами CSIRTs: Работа в процессе

Глубокий анализ управления инцидентами.

Источник: <http://www.cert.org/archive/pdf/04tr015.pdf>

Практика для Групп Реагирования на Инциденты Компьютерной Безопасности (CSIRTs)

Обширный анализ актуальных ситуаций, принимая во внимание всемирную дислокацию CSIRT, включая историю, статистику и многое другое.

Источник: <http://www.cert.org/archive/pdf/03tr001.pdf>

CERT-in-a-box

Подробное описание уроков полученных при создании GOVCERT.NL и 'De Waarschuwingdienst', Датский национальный сервис оповещения.

Источник: <http://www.govcert.nl/render.html?it=69>

RFC 2350: Ожидаемый результат от Реагирования на Инциденты Компьютерной Безопасности

Источник: <http://www.ietf.org/rfc/rfc2350.txt>

NIST³⁷ Руководство по обработке Инцидентов Компьютерной Безопасности

Источник: <http://www.securityunit.com/publications/sp800-61.pdf>

Список ENISA CERT мероприятий в Европе

Дополнительный список информации о работе CSIRT в Европе и их разнообразной деятельности

Источник: http://www.enisa.europa.eu/cert_inventory/

³⁷ NIST: Национальный институт стандартов и технологий

A.2 Сервисы CSIRT

Специальная благодарность CERT/CC, которые предоставили данный список

Сервисы реагирования	Профилактические сервисы	Обработка артефактов
- Оповещение и предупреждение - Обработка инцидентов - Анализ инцидентов - Реакция на инциденты - Координация реагирования на инциденты - Реакция на инциденты на месте - Обработка уязвимостей - Анализ уязвимостей - Реакция на уязвимости - Координация реагирования на уязвимости	- Объявления - Слежение за развитием технологий - Анализ и оценка систем безопасности - Конфигурирование и поддержка систем безопасности - Разработка средств обеспечения безопасности - Обнаружение вторжения - Распространение информации о системах безопасности	- Анализ артефактов - Реакция на артефакт - Координация реагирования на артефакты
		Управление качеством систем безопасности - Анализ рисков - Непрерывность рабочего процесса и восстановление при аварийных ситуациях - Консультирование по вопросам безопасности - Повышение осведомлённости - Обучение / Тренинги - Оценка продукта и Сертификация

Рис. 19 Список сервисов CSIRT от CERT/CC

Описание сервисов

Сервисы реагирования

Сервисы реагирования разработаны для ответов на запросы о помощи, создания отчётов об инцидентах клиентов CSIRT и реагирования на любые угрозы атаки на системы CSIRT. Некоторые сервисы могут быть реализованы оповещением при помощи третьей стороны или просмотром результатов мониторинга или логов и предупреждений IDS.

Оповещение и предупреждение

Данный сервис включает в себя распространение информации описывающей атаки злоумышленников, уязвимости безопасности, попытки вторжения, компьютерные вирусы, или hoax, и предоставление любых кратких рекомендованных наборов действий для решения проблемы. Оповещение, предупреждение, или рекомендация отсылаются, как реакция на конкретную проблему, чтобы оповестить клиентов о данной деятельности и предоставить инструкции по защите их систем или восстановлению всех пораженных систем. Информация может быть составлена CSIRT или распространена непосредственно производителями ПО, а также другим CSIRT или экспертом в области безопасности, или из любого другого клиентского источника.

Обработка инцидентов

Обработка инцидентов включает в себя получение, сортировку и определение приоритетов, реагирование на запросы и отчёты, а также анализ инцидентов и событий. Подробный набор действий для реагирования включают:

- Принятие мер для защиты систем и сетей, поражённых действиями злоумышленников или находящихся под угрозой поражения
- Предоставление решения и стратегии уменьшения риска поражения из соответствующих рекомендаций или оповещений
- Поиск деятельности злоумышленников в других частях сети

- Фильтрация сетевого трафика
- Восстановление функциональности систем
- Исправление или восстановление систем
- Разработка других откликов или усовершенствование стратегий

После того как различными средствами и при помощи различных типов CSIRT имплементированы действия по обработке инцидента, данный сервис категоризируется по типу вредоносной деятельности и типу оказанной помощи следующим образом:

Анализ инцидентов

Существует множество уровней анализа инцидента, а также множество подуровней. По существу, анализ инцидента это оценка всей доступной информации и вспомогательных доказательств или артефактов, связанных с данным инцидентом или событием. Цель анализа идентифицировать масштаб инцидента, объём причиненного по вине инцидента ущерба, природу инцидента, а также доступные стратегии отклика или отладки. CSIRT может использовать результаты анализа уязвимости или артефакта (описанного выше), для того чтобы понять и предоставить наиболее полный и своевременный анализ, произошедшего на определённой системе. CSIRT сравнивает действия инцидентов и их активность для определения любых взаимосвязей, тенденций, шаблонов, или следов злоумышленника. Два подуровня, которые могут быть выполнены как часть анализа инцидента в зависимости от задачи, цели, и действий CSIRT это:

Сбор юридической информации

Сбор юридической информации это - сбор, сохранение, документирование, и анализ фактов о подверженных риску компьютерных системах для определение изменений системы и для содействия в реконструкции событий приведших к оптимальному решению. Данный сбор информации и фактов должен быть проведён таким образом, чтобы задокументировать цепочку доказательств сохранности информации, чтобы она являлась допустимой в законе суде по всем юридическим правилам представления доказательств. Задачи, связанные со сбором юридических доказательств, включают в себя (но не ограничиваются этим) создание побитовой копии жёсткого диска пораженной системы; сопоставления изменений системы таких как: новые программы, файлы, сервисы, и пользователи; просмотр запущенных процессов и открытых портов; а также проверку на наличие «троянов» и других вредоносных программ. Персонал CSIRT, исполняя данную функцию, должен быть также подготовлен к выступлению в судебном процессе в качестве экспертов

Отслеживание или трассировка

Отслеживание источника проникновения злоумышленника или определение систем, к которым он имеет доступ. Данная деятельность включает отслеживание или трассировку путей проникновения злоумышленника в поражённую систему и относящуюся к ней сеть, какие системы были использованы для получения данного доступа, источник возникновения атаки, а также определение других сетей и систем которые через которые доступен данный доступ. Это может также включать попытку установления личности злоумышленника. Даная работа должна быть проделана самостоятельно, но обычно включает взаимодействие с правоохранительными органами, Интернет провайдерами и другими вовлеченными в данную деятельность организациями.

Отклик на инциденты на стороне клиента

CSIRT предоставляет непосредственную поддержку на стороне клиента для помощи в восстановлении клиентов после инцидента. CSIRT самостоятельно физически анализирует поражённые системы и руководит восстановлением и исправлением системы, взамен предоставления отклика на инцидент по телефону или через электронные письма (см. ниже). Данный сервис включает полный комплекс мероприятий на локальном уровне, которые необходимы, если инцидент произошёл или предполагается. Если CSIRT не может исправить поражение локально, то члены группы отправляются к непосредственно клиенту, чтобы произвести отклик. В противном случае

должна существовать группа на стороне клиента, частью повседневной деятельности которой, является отклик на локальные инциденты. Это в особенности актуально, если обработка инцидента является частью нормального функционирования системы, сети или безопасного администрирования в месте, где расположена CSIRT.

Поддержка отклика на инциденты

CSIRT ассистирует и руководит действиями потерпевших от атак по восстановлению после инцидента посредством: телефона, электронной почты, факса, или документации. Это также может включать техническую поддержку в виде сбора данных, предоставления контактной информации или руководств со стратегиями уменьшения атак и восстановления системы. Это не включает непосредственных действий на стороне клиента описанных выше. Вместо этого CSIRT предоставляет инструкции удалённо, при помощи которых персонал на стороне клиента мог бы произвести восстановление самостоятельно.

Обработка артефактов

Здесь «артефакт» - это любой файл или объект найденный в системе, который мог быть вовлечён в исследование или атаку системы и сети или использовался для аннулирования средств безопасности. Артефакты могут содержать, но не ограничиваются, компьютерными вирусами, «троянскими» программами, «червями», эксплойт-скриптами, и прочим инструментарием злоумышленника.

Обработка артефактов включает получение информации о копиях артефактов, которые использовались в атаке злоумышленником, зондировании, и другой неавторизованной или разрушительной деятельности. Будучи однажды полученным, артефакт становится частью базы известных артефактов. Это включает анализ природы, механизма, версии, и использования артефакта; и разработку (или рекомендацию) стратегии отклика для определения, устранения и защиты от данного типа артефактов. Будучи однажды реализованной различными способами различными типами CSIRT обработка артефакта в дальнейшем распределяется по следующим категориям, основываясь на производимом типе деятельности и типе содействия:

Анализ артефактов

CSIRT производит техническое исследование и анализ любых артефактов найденных в системе. Произведенный анализ должен включать идентификацию типа файла и структуры артефакта, сравнивая новый артефакт с существующими или с другими версиями таких же артефактов на схожесть и отличия, реинженеринг или дизассемблирование для определения назначения и функции артефакта.

Отклик на артефакт

Данный сервис включает определение подходящих действий для установления присутствия и удаления артефакта из системы, для предупреждения его установки в систему. Это может включать создание описания характерных черт, которые могут быть добавлены в антивирусное программное обеспечение или IDS.

Координация отклика на артефакты

Данный сервис включает в себя распространение и синтез результатов анализа и стратегий отклика, присущих артефакту полученных от различных исследователей, CSIRT, разработчиков и других экспертов по безопасности. Деятельность включает оповещение остальных сторон и синтез технического анализа от различных источников. Деятельность также может включать поддержку открытого или частично открытого (только для клиентов данной CSIRT) архива известных артефактов, их воздействия и соответствующих стратегий отклика

Профилактические сервисы

Профилактические сервисы призваны улучшить состояние инфраструктуры клиентов и процессов, обеспечивающих их безопасность прежде, чем произойдет или будет зафиксирован инцидент или любое другое событие. Главной целью профилактических

сервисов является избежание инцидентов и снижение их последствий, а также – отслеживание факта их происшествия.

Объявления

Включают, но не ограничиваются следующим: оповещениями о вторжениях, предупреждениями об уязвимостях и рекомендациями по безопасности. Объявления информируют клиентов о новых событиях, имеющих средний и длительный срок влияния, например, о недавно обнаруженных уязвимостях или инструментах злоумышленников. Объявления помогают клиентам защитить свои системы и сети от недавно обнаруженных проблем, связанных с безопасностью, прежде чем те будут использованы для взлома.

Слежение за развитием технологий

Для того, чтоб легче было идентифицировать угрозы, CSIRT отслеживает появление и наблюдает за развитием новых технических средств, деятельностью злоумышленников и за новыми тенденциями в области безопасности. Список отслеживаемых источников информации может быть расширен. Они могут включать судебные постановления и законодательные акты, информацию о социальных или политических угрозах, новейших технологиях. Работа этой службы заключается также в чтении информации, публикуемой на сайтах и в списках рассылки, посвященных безопасности, а также чтении свежих новостей и статей в журналах по науке, различным технологиям, политике, системы государственной власти с целью извлечения информации, имеющей отношение к системам безопасности и сетям клиентов. Для того, чтоб получить наиболее точную информацию и ее трактовку, данная деятельность может включать взаимодействие с полномочными органами перечисленных областей науки и знаний. Результатом деятельности службы являются объявления, руководства или рекомендации по проблемам безопасности, носящие средне- и долгосрочный характер.

Анализ или оценка систем безопасности

Эта служба проводит подробную оценку и анализ инфраструктуры безопасности какой-либо организации, основываясь на требованиях, определенных в политике данной организации, или определенных в стандартах, действующих в данной отрасли. Деятельность службы может включать оценку организационной политики безопасности. Существует множество типов оценки и анализа, среди них:

Анализ инфраструктуры

Собственноручная проверка настроек ПО и оборудования, маршрутизаторов, сетевых экранов, серверов и рабочих станций на соответствие требованиям организационной политики безопасности или лучшим ее образцам и стандартам в отрасли

Анализ на соответствие лучшим образцам

Опрос персонала, системных и сетевых администраторов с целью выяснения, соответствуют ли применяемые для организации безопасности методы ее политике безопасности или стандартам конкретной отрасли

Сканирование

Использование сканера уязвимостей или вирус-сканера для определения уязвимых систем и участков сети

Испытание на проникновение

Тестирование безопасности узла путем целенаправленной атаки на его системы и сетевые сегменты. Для выполнения подобного рода оценки или аудита необходимо получить санкции руководителей высшего звена. Некоторые из таких методов могут быть запрещены организационной политикой безопасности. В рамках данных услуг может быть разработан набор критериев, по которым проводятся тесты или оценка, а также определены

квалификация и сертификаты, которым должен обладать персонал, производящий тестирование, анализ, оценку или аудит. Проведение этих мероприятий может быть поручено другой контрактной стороне или провайдеру услуг безопасности с необходимой квалификацией для проведения аудита и оценки

Настройка и сопровождение инструментария, приложений, инфраструктуры и сервисов для обеспечения безопасности

Этот сервис устанавливает или дает рекомендации о том, как с точки зрения безопасности лучше настроить и поддерживать функциональность инструментария, приложений и всей информационной инфраструктуры, используемой клиентами CSIRT или самим CSIRT. Кроме выдачи рекомендаций, CSIRT может проводить обновление настроек и поддержку следующих инструментов и сервисов, обеспечивающих безопасность: системы обнаружения вторжений (IDS), систем сканирования и мониторинга, фильтров, вращающихся (wgarrers), сетевых экранов, виртуальных частных сетей (VPN) и систем аутентификации.

Разработка средств обеспечения безопасности

Этот сервис подразумевает разработку новых, специфичных для конкретной области деятельности, инструментов, требуемых (желаемых) клиентом или самой CSIRT. Эта деятельность может, например, включать разработку заплаток на модифицированное по заказу ПО, используемое клиентами; разработку пакетов ПО, которые могут быть использованы для восстановления работы скомпрометированных узлов; разработку модулей или скриптов, которые смогли бы расширить функциональность существующих инструментов, например, новых модулей для сканеров уязвимостей или сетевых сканеров; скриптов, способствующих использованию технологий шифрования; автоматизированных систем распространения заплаток.

Сервисы обнаружения вторжений

Группы CSIRT, предоставляющие эту услугу, анализируют существующие журналы систем обнаружения вторжений, оценивают и применяют ответные действия, на события, произошедшие в результате срабатывания этих систем, распространяют оповещения в соответствии с составленным заранее Соглашением об Уровне Оказываемого Сервиса (SLA) или политикой обострения статуса ситуации. Обнаружение вторжений и анализ связанных с ними журналов может быть очень трудоемкой задачей, т.к. заключается не только в определении места размещения сенсоров, но и сборе и последующем анализе больших объемов собранных данных. Для того, чтоб обнаружить ложные срабатывания системы, атаки, идентифицировать прочие происшествия, предотвратить их в будущем и минимизировать их влияние, во многих случаях требуется специальный инструментарий и высокая квалификация при обобщении и интерпретации полученной информации. Некоторые организации поручают проведение этих мероприятий другой контрактной стороне с надлежащей квалификацией и опытом, таким как провайдеры услуг безопасности.

Распространение информации, связанной с безопасностью

Этот сервис предоставляет клиентам всеобъемлющий набор полезной информации, способствующей повышению уровня безопасности. Эта информация может включать:

- Рекомендации по созданию отчетов и контактную информацию о группе CSIRT
- Архив оповещений, предупреждений и объявлений
- Документация о лучших методах организации безопасности
- Общие рекомендации по обеспечению компьютерной безопасности
- Описания политик, процедур и контрольные перечни дел
- Информация о разработке и распространении заплат
- Ссылки на поставщиков и разработчиков
- Глобальная статистика и тенденции в реагировании на инциденты
- Прочая информация, которая может способствовать практическому улучшению уровня безопасности

Эта информация может быть подготовлена и опубликована как самой группой CSIRT, так и другим отделом конкретной организации (ИТ, отделом кадров, отделом по связи со СМИ)

Сервис управления качеством систем безопасности

Сервисы, попадающие в эту категорию, не являются характерными только для обработки инцидентов или групп CSIRT. Это широко известные, общепризнанные сервисы, предназначенные для улучшения безопасности организации в целом. Используя опыт, полученный при предоставлении сервисов реагирования и профилактических сервисов, описанных выше, группа CSIRT может создать хорошую почву для развития сервисов управления качеством, которые иначе были бы недоступны. Эти сервисы должны включать организацию обратной связи, должны учитывать знания, полученные в результате реагирования на инциденты, уязвимости и атаки. Наполнение этим опытом общеизвестных традиционных сервисов (описанные ниже), являющееся частью процесса управления качеством систем безопасности, позволит улучшить долгосрочные мероприятия по обеспечению безопасности организации. В зависимости от организационной структуры и полномочий, группа CSIRT может предоставлять эти сервисы сама или быть частью команды, участвующей в мероприятиях по обеспечению безопасности.

Следующие понятия объясняют, как опыт и квалификация группы CSIRT может помочь в реализации каждого из сервисов управления качеством систем безопасности.

Анализ рисков

CSIRT может способствовать совершенствованию процесса анализа и оценки рисков. Это может, в свою очередь, повысить способность организации по оценке реальных угроз, максимально точно давать качественную и количественную оценку рискам информационных активов, разработать стратегии реагирования и защиты. CSIRT, выполняющая данную роль, смог бы сам осуществлять или помогать при анализе рисков информационной безопасности для внедряемых систем и бизнес процессов, а также оценивать степень опасности угроз и атак по отношению к системам и активам клиентов.

Непрерывность рабочего процесса и планирование восстановления при аварийных ситуациях

Принимая во внимание произошедшие инциденты и предсказываемый в будущем ущерб от появляющихся инцидентов и угроз безопасности, можно сделать вывод о том, что все большее количество инцидентов будут наносить урон бизнес процессу. Таким образом, процесс планирования должен происходить с учетом опыта и рекомендаций группы CSIRT по определению лучших способов реагирования на подобные инциденты и обеспечения непрерывности рабочего процесса. Группы CSIRT, предоставляющие данный сервис, автоматически включаются в планирование непрерывности рабочего процесса и процедур восстановления при аварийных ситуациях, связанных с атаками и угрозами компьютерной безопасности.

Консультирование по вопросам безопасности

В обязанности CSIRT может входить выдача рекомендаций по внедрению в бизнес процессы клиентов лучших методов обеспечения безопасности. Группа CSIRT, выполняющая данную работу, готовит рекомендации, определяет требования, которые должны выполняться при покупке, установке и в процессе обеспечения безопасности новых систем, сетевых устройств, программного обеспечения или внедрению бизнес процессов масштаба предприятия. Этот сервис также подразумевает рекомендации и помощь в разработке политики безопасности отдельной организации или группы клиентов, советы и дачу показаний в законодательных и других правительственных органах.

Повышение осведомлённости

CSIRT может определить, по каким предметам клиентам нужно предоставить больше сведений, и дать рекомендации для того, чтоб полностью соответствовать общепринятым нормам безопасности и организационной политике безопасности. Повышение общей осведомленности клиентов о безопасности не только расширяет их знания, но и помогает им выполнять ежедневные операции более безопасным способом. Это приведет к снижению количества успешных атак, увеличит вероятность того, что клиенты обнаружат атаку и сообщат о ней. Это поможет сократить время восстановления и предотвратить или свести к минимуму убытки. Группы CSIRT, предоставляющие данный тип сервиса, способствуют увеличению осведомленности о безопасности, выпуская статьи, плакаты, информационные бюллетени, создавая веб-сайты и другие информационные ресурсы, которые рассказывают о лучших методах внедрения безопасности и советуют, какие принять меры предосторожности. Деятельность также может включать встречи и семинары для того, чтоб рассказать клиентам о мероприятиях, проводимых для улучшения безопасности, и потенциальных угрозах различным системам организации.

Обучение и подготовка

Этот сервис подразумевает предоставление клиентам информации по проблемам компьютерной безопасности на семинарах, конференциях специалистов, курсах и практических занятиях. На них могут быть затронуты темы: рекомендации по тому, как сообщить об инцидентах, надлежащих способах реагирования на них, средствах реагирования, методах предотвращения инцидентов и другие темы, необходимые для защиты, обнаружения, сообщения и реагирования на инциденты, связанные с компьютерной безопасностью.

Оценка или сертификация конечного продукта

Предоставляя этот сервис, группа CSIRT может проводить оценку средств, приложений и других услуг для обеспечения необходимого уровня безопасности продукции и ее соответствия организационным меркам безопасности, или установленным CSIRT. Оцениваемые средства или приложения могут быть как программным обеспечением с открытым кодом, так и коммерческим продуктом. Сервис может представлять собой процесс оценки или сертификации, в зависимости от стандартов и норм, применяемых в организации или рекомендуемых группой CSIRT.

А.3 Примеры

Условная CSIRT
Шаг 0. Осознание того, что такое CSIRT Наш образец CSIRT будет служить учреждению среднего размера, персонал которого состоит из 200 работников. В составе учреждения есть отдел информационных технологий (ИТ) и два филиала, находящиеся в пределах этой же страны. Отдел ИТ. играет ключевую роль в бизнес процессе компании, т.к. обеспечивает ее средствами внутренней связи, сетью передачи данных и непрерывность ее электронного бизнеса. ----- Шаг 1: Начальный этап На начальных этапах новая CSIRT планируется как внутренняя группа CSIRT, предоставляющая услуги отделу ИТ компании-владельца и остальному персоналу. Она также поддерживает и координирует меры по обработке компьютерных инцидентов в филиалах. ----- Шаг 2: Определение списка предоставляемых сервисов На начальном этапе было решено, что новая группа CSIRT будет предоставлять работникам учреждения лишь некоторые из основных сервисов. После пилотного запуска может быть рассмотрена возможность расширения списка предоставляемых услуг. Могут быть добавлены Сервисы Управления Безопасностью. Решение будет вынесено на основании отзывов от клиентов пилотного запуска и в тесном сотрудничестве с Отдел Контроля Качества. ----- Шаг 3: Проведение анализа клиентов и информационных каналов. В результате мозгового штурма, проведенного совместно с руководителями высшего звена и клиентами, было получено достаточно информации для SWOT-анализа. Это привело к выводу, что требуется внедрение следующих основных сервисов: • Оповещений и предупреждений • Обработки инцидентов (анализ, оказание поддержки при реагировании и координация мероприятий, выполняемых в рамках данной процедуры) • Оповещений Для того, чтоб информация достигла как можно более широкого круга клиентов, нужно должным образом организовать ее распространение. Было принято решение, что оповещения, предупреждения и объявления будут публиковаться в форме рекомендаций по безопасности на выделенном для этой цели веб-сайте, а также посредством списка рассылки. Создание универсальной веб-формы запланировано на следующем шаге.

Шаг 4: Заявление о намерениях

Руководство условной CSIRT сформировало следующее заявление о намерениях:
«Условная CSIRT предоставляет информацию и оказывает содействие персоналу компании-владельца с целью снижения рисков инцидентов, связанных с компьютерной безопасностью, а также с целью реагирования на произошедшие инциденты»
Этим условная CSIRT заявляет, что это внутренняя CSIRT и что ее главная обязанность – заниматься вопросами, связанными с информационной безопасностью.

Шаг 5: Составление Бизнес Плана**Финансовая Модель**

Вследствие того, что электронный бизнес компании должен работать круглосуточно, и того что в ее структуре круглосуточно функционирует отдел ИТ, постановили, что в рабочие часы CSIRT будет предоставлять услуги в полном объеме, а в нерабочее время услуги будут предоставляться по требованию. Услуги клиентам будут предоставляться бесплатно, а возможность предоставления услуг внешним потребителям будет рассмотрена в течение пилотного и оценочного этапов.

Модель Доходов

С самого начала и во время пилотного этапа CSIRT будет финансироваться из бюджета компании-владельца. С пилотного этапа по оценочный будет рассмотрен вопрос привлечения дополнительного финансирования, включая возможность продажи услуг внешним потребителям.

Организационная модель

Компания-владелец – небольшая компания, поэтому выбрана вложенная модель. В рабочее время персонал из трех человек будет предоставлять основные сервисы (распространение рекомендаций по безопасности и обработку инцидентов). В отделе ИТ есть люди, обладающие необходимой квалификацией. С отделом ИТ заключено соглашение, в рамках которого созданная группа CSIRT может запросить поддержку в специальных случаях. Также для нужд CSIRT может быть использована вторая телефонная линия отдела ИТ. Группа CSIRT будет состоять из четырех специалистов с полной занятостью и пяти дополнительных членов CSIRT. Один из них будет работать в «плавающую» смену.

Штат сотрудников

Начальник группы CSIRT имеет образование, связанное с обеспечением безопасности, и имеет опыт по предоставлению тех. поддержки 1го и 2го уровня, а также обладает гибкостью при принятии решений во время кризисных ситуаций. Остальные три члена группы являются специалистами по безопасности. Члены команды с неполной рабочей занятостью из отдела ИТ являются знатоками определенной части инфраструктуры компании.

Шаг 6: Использование офисной и информационной политики безопасности**Офисное оборудование и его размещение**

Благодаря тому, что в компании-владельце уже внедрена физическая защита, созданная группа CSIRT тоже является ее объектом. Построена так называемая «военная комната» для координации действий в случае чрезвычайного положения. Для шифрованных материалов и ценных документов был приобретен сейф. Была проведена отдельная телефонная линия, которую оборудовали коммутационной панелью для организации «горячей линии» в рабочие часы и установлен мобильный телефон с тем же номером для работы по требованию в нерабочее время.

Существующее оборудование и корпоративный веб-сайт могут быть использованы для размещения информации, связанной с деятельностью CSIRT. Установлено и введено в эксплуатацию ПО для организации списков рассылки. В нем есть закрытый для общего доступа раздел, позволяющий членам команды общаться между собой и с другими командами. Вся контактная информация персонала хранится в базе данных, распечатка хранится в сейфе.

Правила и нормативы

Поскольку CSIRT является частью организационной структуры компании с существующей политикой информационной безопасности, данные политики были применены и в группе CSIRT при содействии юрисконсульта компании.

Шаг 7: В поисках сотрудничества

С помощью Реестра Европейского Агентства Сетевой и Информационной Безопасности (ENISA) были найдены группы CSIRT в той же стране и налажены с ними контакты. Для руководителя нашей группы был организован визит на узел одной из групп-партнеров. Он узнал там о деятельности национальной CSIRT и посетил одну из деловых встреч. Встреча была более чем плодотворной благодаря сбору информации о работающих методах и получению поддержки других групп.

Шаг 8: Создание бизнес-плана

Было принято решение собрать факты и численные показатели деятельности компании. Это будет полезно для статистического анализа состояния информационной безопасности. Сбор должен быть продолжен для поддержания актуальности статистики, когда CSIRT будет запущена в эксплуатацию. Были опрошены некоторые национальные группы CSIRT о том, как организованы их бизнес процессы. Они помогли тем, что предоставили несколько слайдов со свежей информацией по эволюции инцидентов, связанных с компьютерной безопасностью, и их издержках. В данном примере создания условной CSIRT не было необходимости убеждать руководство в важности ИТ бизнеса и было сразу получен зеленый сигнал на то, чтоб предпринять первые шаги по созданию группы. Было подготовлено экономическое обоснование и план проекта, а также расчет затрат на наладочные работы и расчет эксплуатационных расходов.

Шаг 9 Определение последовательности технологических процессов, порядка действий и технических процедур.

Условная группа CSIRT обеспечивает предоставление следующих основных сервисов CSIRT:

Оповещения и предупреждения

Объявления

Обработка инцидентов

Команда разработала нормально функционирующие процедуры, которые понятны всем ее членам. Условная группа CSIRT наняла юриста для работы, связанной с юридической ответственностью и политикой информационной безопасности. Команда также приняла в пользование несколько полезных утилит и почерпнула полезную информацию об особенностях функционирования CSIRT во время общения с членами других групп. Был создан шаблон для рекомендаций по безопасности и отчетов об инцидентах. Команда использует систему RTIR для обработки инцидентов.

Шаг 10 Обучение персонала

Условная группа CSIRT решила послать весь свой технический персонал на ближайшие по времени курсы, организуемые в рамках проекта TRANSITS. Руководитель группы дополнительно проходит курс «Управление группой CSIRT», организованной CERT/CC.

Шаг 11: Практические занятия

В течение первой недели существования условной CSIRT работала на практических занятиях над несколькими воображаемыми инцидентами (реальные случаи, зафиксированы другими CSIRT). Также были созданы несколько рекомендаций по безопасности разработанных на основе реальной, распространенной производителями ПО и оборудования информации об уязвимостях, которую специалисты CSIRT отредактировали и адаптировали к нуждам клиентов.

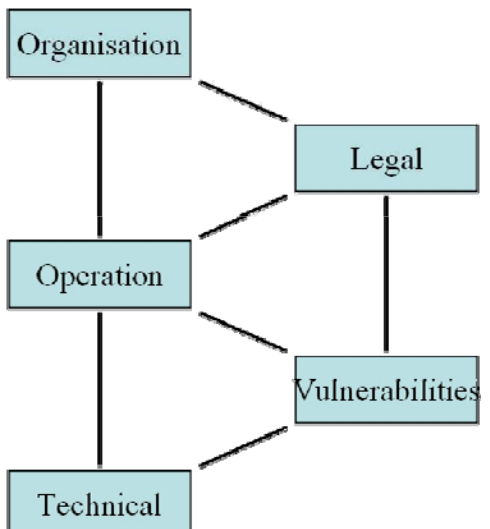
A.4 Пример материалов из курсов CSIRT

TRANSITS (с любезного разрешения TERENA <http://www.terena.nl>)

Course structure



- **Five modules**
- **Independent, but linked**
- **12-14 hours work in 2 days**
- **Practical exercises include**
 - Analyse incidents
 - Organisational plan
 - Incident response plan



```
graph TD; Organisation --- Operation; Organisation --- Legal; Operation --- Technical; Operation --- Legal; Operation --- Vulnerabilities; Technical --- Vulnerabilities; Legal --- Vulnerabilities
```

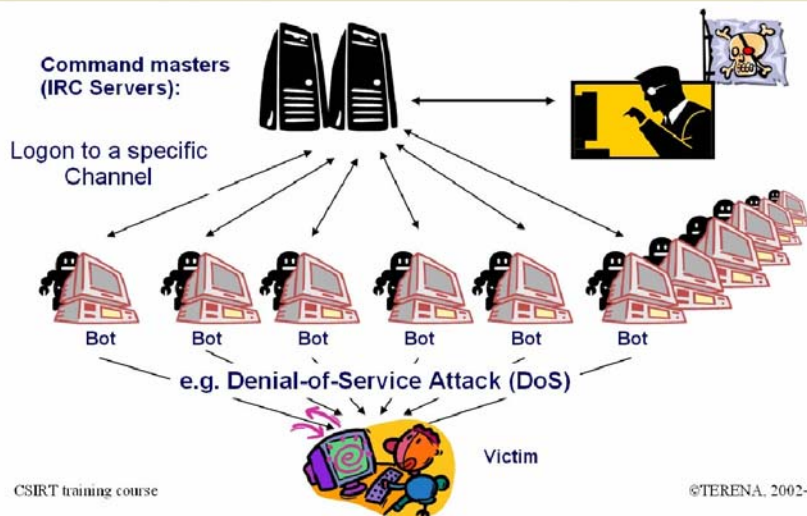
CSIRT training course

TERENA, 2002-6

Обзор: структура курса

Malicious Code

Malicious IRC Bots - A botnet in action

Из модуля о технологиях: описание сети зараженных компьютеров Botnet

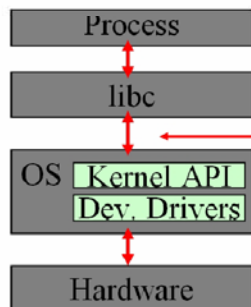
Malicious Code

Rootkits - Basic design



- Replacing binaries is easily detected (tripwire et al).
- A more elegant approach would deliver false data to **all** processes -> Modify kernel

```
fd = open(...);
movl $0x5,%eax
int 0x80
call $sect1+%eax
|
```



Intercept this communication

CSIRT training course

©TERENA, 2002-6

Из модуля о технологиях: Разработка простейшего руткита

Who is the Biggest Threat?

Employees?

- Secure h/w & s/w?
- Firewalls?
- Anti-virus s/w?



Customers/Students?

Viruses/Worms

LoveBug, CodeRed, Nimda, Slammer, ...

Cost \$1T worldwide

Need user help to spread:

- Unexpected attachments
- Unneeded programs

Unwary users get caught



Suppliers/Partners?

Do you know?
DTI* data indicates:

- 68% suffered a malicious incident
- Two thirds have no info security policy
- 57% have no contingency plan for incidents



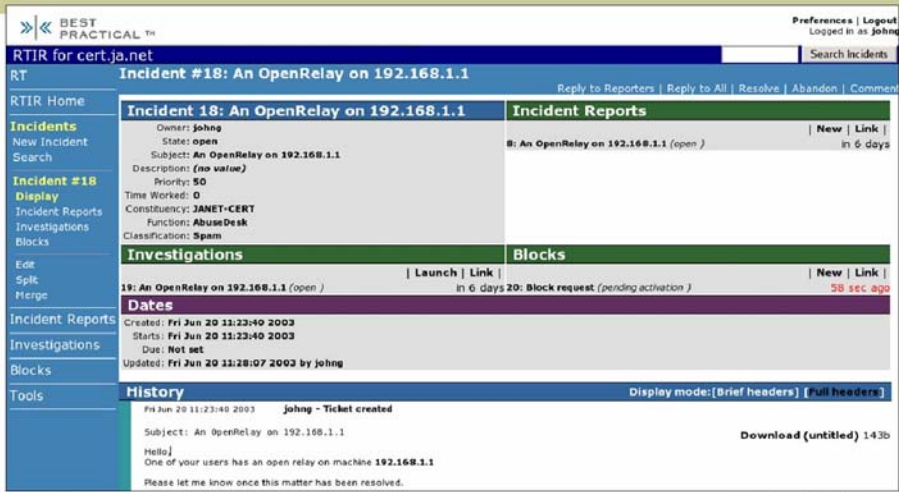
CSIRT training course

* UK Department for Trade & Industry Information Security Breaches survey 2004

©TERENA, 2002-6

Из Организационного модуля: от кого исходит большая угроза – от своих, или чужих?

e.g. RTIR incident page



CSIRT training course

©TERENA, 2002-6

Из модуля *Operational track*: Request Tracker for Incident Response (RTIR)

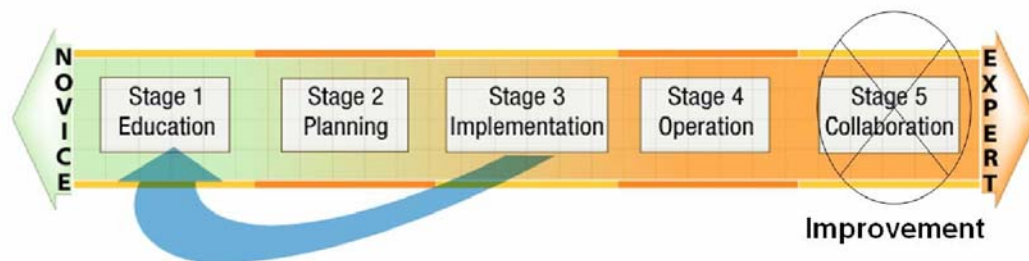


«Создание CSIRT» (с любезного разрешения CERT/CC, <http://www.cert.org>)

ENISA с удовольствием благодарит команду по развитию CSIRT из программы CERT за разрешение на использование информации из их учебных курсов!

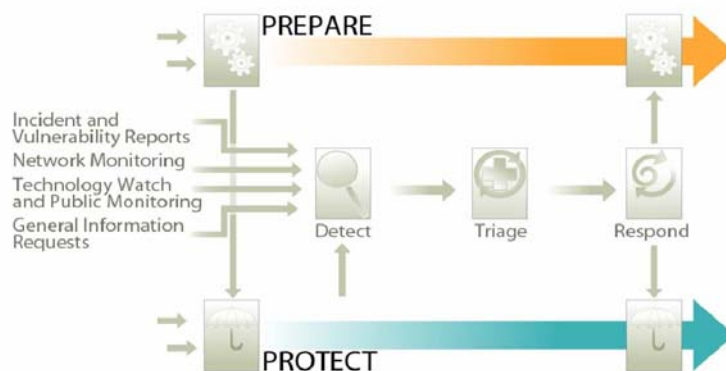
Stages of CSIRT Development

- Stage 1 Educating the organization
- Stage 2 Planning effort
- Stage 3 Initial implementation
- Stage 4 Operational phase
- Stage 5 Peer collaboration— Improvement of the CSIRT



Из обучающего курса CERT/CC: Этапы создания CSIRT

Incident Management Best Practice Model



© 2006 Carnegie Mellon University

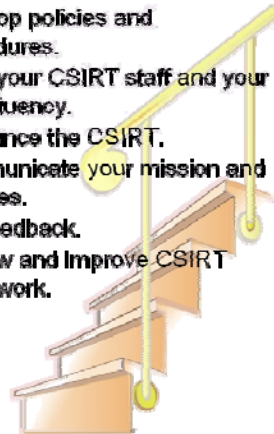
3

CERT

Из обучающего курса CERT/CC: Лучшие методы организации обработки инцидентов

Basic Implementation Steps

- Gather information.
- Identify the CSIRT constituency.
- Determine the CSIRT mission.
- Secure funding for CSIRT operations.
- Determine CSIRT range and levels of service.
- Determine CSIRT reporting structure, authority and organizational model.
- Identify interactions with key parts of the constituency.
- Define roles and responsibilities for interactions.
- Create a plan, obtain feedback on the plan.
- Identify and procure personnel, equipment and infrastructure resources.
- Develop policies and procedures.
- Train your CSIRT staff and your constituency.
- Announce the CSIRT.
- Communicate your mission and services.
- Get feedback.
- Review and Improve CSIRT framework.



© 2006 Carnegie Mellon University

4

CERT

Из обучающего курса CERT/CC: Шаги, выполняемые при создании CSIRT

Range of CSIRT Services



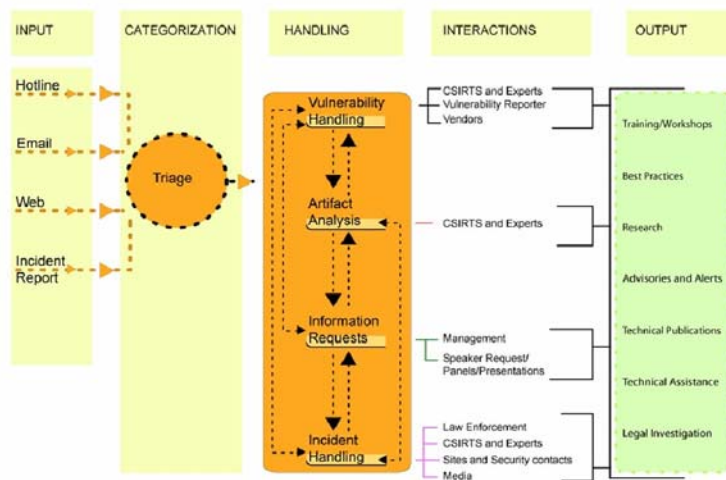
© 2006 Carnegie Mellon University

5



Из обучающего курса CERT/CC: сервисы, которые может предоставлять CSIRT

Service Integration

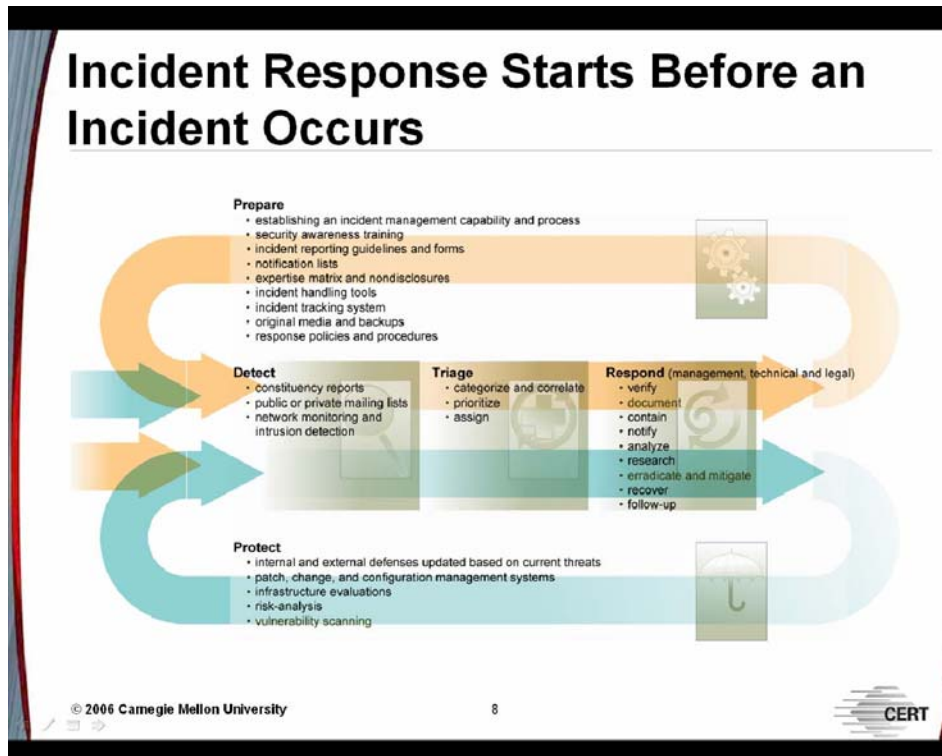


© 2006 Carnegie Mellon University

6



Из обучающего курса CERT/CC: Технологический процесс обработки инцидента

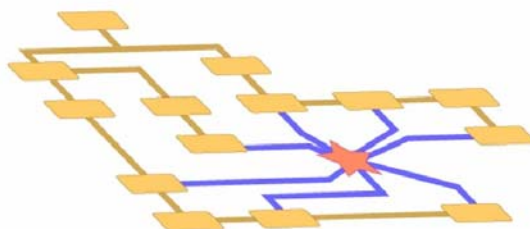


Из обучающего курса CERT/CC: реагирование на инцидент

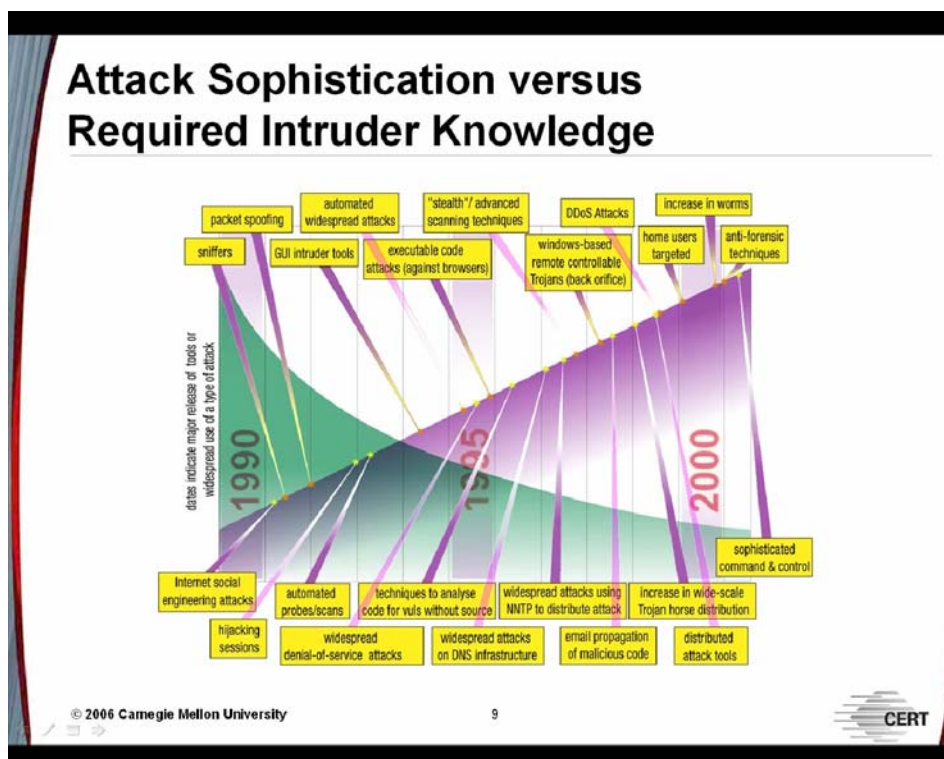
Organizational Models

When designing the vision of your CSIRT, you need to think about how the CSIRT will operate and interact with the organization and constituency.

You need to envision a model that can be implemented.



Из обучающего курса CERT/CC: Как организовать CSIRT?



Из обучающего курса CERT/CC: меньше известно – больше вреда