Создание службы реагирования на компьютерные инциденты безопасности

Silk Security Workshop 2004
21-24 июня, 2004

Yuri Demchenko, University of Amsterdam
<demch@science.uva.nl>

Содержание

- Основные термины
- Центры реагирования на компьютерные инциденты безопасности
  - Функции, формы и структуры
- Организационные вопросы
  - Подготовка бизнес-плана
  - Создание и становление Центра
- Операционные вопросы
  - Профилактические мероприятия
  - Реагирование на инциденты
- Информационная деятельность Центра
  - Оповещения об уязвимостях и Рекомендации по безопасности

Центры реагирования на компьютерные инциденты безопасности

Computer Emergency Response Team – CERT

- Центр Реагирования на Чрезвычайные Компьютерные Ситуации

Computer Security Incident Response Team - CSIRT

- Центр Реагирования на Компьютерные Инциденты Безопасности – ЦРКИБ

Incident Response Capability – IRC

- Служба реагирования на компьютерные инциденты безопасности

Другие варианты русско-язычного названия

- Центр или Служба реагирования на инциденты безопасности в Информационных и телекоммуникационных системах

Компьютерный инцидент безопасности

- Компьютерный инцидент безопасности
  - Любое реальное или предполагаемое событие, имеющее отношение к безопасности компьютерной системы или компьютерной сети
    - Или согласно более формальной терминологии, информационной или телекоммуникационной системы
- Примеры компьютерных инцидентов
  - Попытка (успешная или неудачная) получения несанкционированного доступа к системе или данным
  - Нежелательное прерывание/нарушение нормальной работы
  - Неавторизированное использование системы для обработки или хранения данных
  - Изменение конфигурации или настроек программного обеспечения без указания, подтвержденного согласия или уведомления пользователя

Организационные структуры ЦРКИБ

Возможные организационные структуры

- Группа безопасности
- Распределенный Центр реагирования на компьютерные инциденты
- Централизованная Служба/Центр
- Комбинированная Служба/Центр
- Координирующий Центр
- Другие формы
  - Аналитический Центр
  - Служба реагирования на уязвимости и компьютерные инциденты безопасности поставщиков оборудования и ПО

Группа безопасности

Использует существующий ИТ-персонал

- Формально не является ЦРКИБ/CSIRT, но отвечает за безопасность сети и компьютерных систем
  - Может быть первым шагом к созданию ЦРКИБ
- Реагирование на КИБ в ограниченном обьеме
  - Действия, относящиеся в основном к работам на собственном оборудовании и касающиеся восстановления и поддержания рабочего состояния сети и компьютерных систем
- Может быть вовлечена в координированное противодействие активным атакам, устранение уязвимостей, или расследование КИБ в составе других ЦРКИБ
- Часто в список задач Группы безопасности входит поддержание безопасности сети, VPN, сетевых экранов, IDS (Intrusion Detection System)
- Проблемы
  - Перечень и уровень услуг зависит от опыта персонала
  - Отсутствие общей политики, возможно дублирование работ разными Группами

Распределенный Центр

(Внутренний) распределенный Центр реагирования состоит из персонала различных подразделений, который может иметь назначенные функции или выполнять определенные функции по очереди

- Может иметь минимальный постоянный состав, например менеджер и технический координатор
  - Менеджер распределенного Центра обычно подчинен высшему менеджеру
- Имеет формализованные процедуры и политику реагирования на КИБ
  - Все заявки об инцидентах должны поступать в центральный офис Центра, который принимает решение о дальнейшей обработке заявок
  - Как правило имеет централизованную систему обработки инцидентов
- Имеет полные полномочия для анализа безопасности в организации и распределенные полномочия реагирования на инциденты
  - Расследование и устранение последствий производятся на местах
- Выпускает рекомендации по безопасности, информационные материалы и вносит предложения по совершенствованию политики безопасности, а также разрабатывает критерии обнаружения вторжений при помощи IDS
- Целевая группа пользователей включает всю или часть организации

Централизованная служба реагирования

Централизованная служба реагирования имеет постоянный состав и несет полную ответственность за реагирование на все виды инцидентов безопасности ИТС, включая анализ, расследование и устранение последствий

- Подченен высшему менеджменту и имеет исключительные полномочия в отношении реагирования на КИБ и соблюдения политики безопасности
- Имеет формализованные процедуры и политику реагирования на КИБ
- Имеет полномочия выпускать рекомендации по улучшению безопасности и реализовывать необходимый комплекс мер по их внедрению
  - Включая установление критерией работы IDS
- Может также производить расследование инцидентов на местах
- Централизованные службы характерны как для малых организаций, так и для больших непроизводственных организаций типа университетов, с однородной организационной структурой

Координирующий центр

Координирующий Центр, как правило, обслуживает распределенные, разнообразные группы пользователей

- Главными задачами координирующего Центра являются координация действий по противодействию широкомасштабным атакам, устранению критических уязвимостей, разработка и внедрение стандартов
  - Имеет формализованные процедуры и политику реагирования на КИБ, а также централизованную Систему отслеживания и обработки инцидентов
  - Часто выступает как независимая сторона в расследовании масштабных инцидентов или проведении скоординированных акций
- Может иметь свои службы расследования инцидентов, тестирования уязвимостей, продуктов безопасности, а также может разрабатывать специальные средства
- Имеет постоянный состав и центральный офис
- Примерами координирующих Центров являются CERT/CC, национальные ЦРКИБ, отраслевые или глобальных сетевых операторов таких как BT, KPN, а также транснациональных корпораций

Другие виды Центров реагирования

- Аналитические центры
  - Могут быть частью услуг предоставляемых производителями средств обеспечения безопасности, как например
    - ISS – Internet Security System – http://xforce.iss.net/xforce/alerts - производитель средств обеспечения безопасности
    - Symantecs - http://securityresponse.symantec.com/ - производитель антивирусного ПО и средств обеспечения безопасности
  - SecurityFocus - http://www.securityfocus.com/incidents
    - Предоставляет широкий набор информационных и аналитических услуг
    - Открытый форум для обмена информацией об инцидентах в реальном времени
- Службы реагирования на уязвимости и компьютерные инциденты безопасности поставщиков оборудования и ПО
  - Cisco PSIRT - http://www.cisco.com/go/psirt
  - Microsoft Security Response - http://www.microsoft.com/security/

Типовые услуги ЦРКИБ

- Реагирование на компьютерные инциденты безопасности
  - Эти услуги инициируются заявкой о случившемся или предполагаемом инциденте, обнаруженной уязвимости, предупреждением о начавшейся атаке, или обнаруженной подозрительной активностью
- Профилактика возможных угроз и уязвимостей
  - Эти услуги включают меры по устранению известных уязвимостей, предупреждению и подготовке к возможным инцидентам с целью уменьшения нежелательных последствий в будущем
- Управление качеством услуг безопасности
  - Эти услуги могут предоставляться ЦРКИБ независимо или совместно с другими службами, основываясь на опыте Центра в работе с реальными инцидентами и обширной информацией по безопасности компьютерных систем

Реагирование на компьютерные инциденты безопасности

- Оповещение и предупреждение об инцидентах, уязвимостях и опасностях
- Работа с инцидентами
  - Анализ инцидентов
  - Непосредственное реагирования на инциденты
  - Поддержка реагирования на инциденты
  - Координация реагирования на инциденты
- Устранение последствий и восстановление системы
- Работа с уликами и извлечение информации об инциденте
- Работа с уязвимостями и потенциальными угрозами
  - Анализ
  - Реагирование
  - Координация

Профилактика возможных угроз и уязвимостей

- Информационные услуги ЦРКИБ
  - Анализ информационных материалов и выработка рекомендаций
  - Распространение внешних информационных материалов
- Аудит безопасности и оценка рисков
- Обслуживание средств поддержания безопасности сети и систем
- Разработка специализированных средств защиты
- Услуги по обнаружению вторжений и выработка критериев для работы автоматизированных систем обнаружения вторжений

Управление качеством услуг безопасности

- Анализ рисков
- Планирование мер по обеспечению непрерывности бизнес-процессов и восстановлению в случае катастроф и других чрезвычайных ситуаций
- Консультации по вопросам безопасности
- Создание обстановки осведомленности в отношении политики безопасности, доступных услуг и процедур реагирования на инциденты, чрезвычайные происшествия
- Образование и тренинг
- Оценка и сертификация оборудования и ПО

Типовый перечень услуг различных ЦРКИБ

- Перечень предоставляемых услуг определяется типом или организационной структурой ЦРКИБ
  - Оптимальное использование персонала
  - Например
    - Обнаружение вторжений - более характерно для Группы безопасности чем для традиционных ЦРКИБ
    - Образование, тренинг и создание обстановки осведомленности – более характерны для координирующих ЦРКИБ и наименее свойственны для Группы безопасности
- Обобщающая Таблица соответствия услуг и типов ЦРКИБ приведена в
  - http://www.sei.cmu.edu/publications/documents/03.reports/03hb001/03hb001app.html

Создания ЦРКИБ: Организационные вопросы

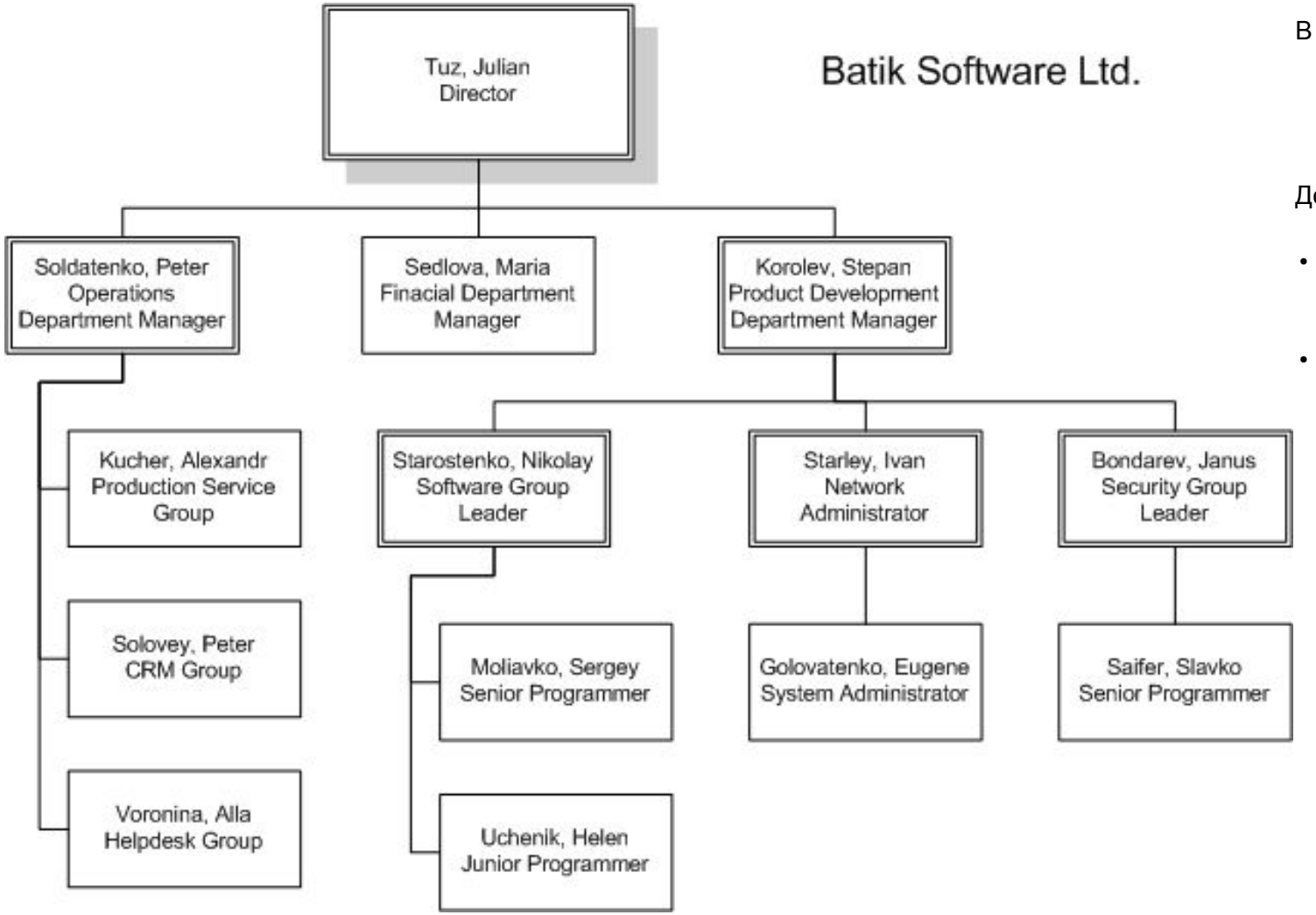
- Начальные этап – представление концепции ЦРКИБ в организации
- Создание ЦРКИБ в организации
- Формирование рабочих связей
- Финансирование ЦРКИБ

Представление концепции ЦРКИБ

Подготовка

- Понять необходимость службы реагирования на компьютерные инциденты безопасности
  - Анализ известных инцидентов
  - Соображения системных администраторов
- Найти место для ЦРКИБ в организации
  - Проанализировать положительные стороны и выгоды
- Разработать план продвижения идеи создания ЦРКИБ
  - Заручиться поддержкой ключевых лиц
  - Проанализировать возможные возражения и препятствия
- Проанализировать возможную финансовую базу ЦРКИБ
  - Этап становления Центра и нормальная работа

Место ЦРКИБ в организации



В чрезвычайной ситуации ЦРКИБ должен действовать независимо и иметь необходимые полномочия

Должна быть поддержка ИТ персонала

- Баланс между независимостью и возможностью привлечения дополнительных специалистов
- Может определяться согласованной Политикой реагирования на инциденты

Подготовка предложения о создании ЦРКИБ

Предложение должно включать

- Важность компьютерной безопасности для организации
  - Почему функции ЦРКИБ не могут быть выполнены существующими подразделениями
  - Анализ слабых/уязвимых мест в организации в отношении компьютерной безопасности
- Известные случаи и возможные сценарии
- Существующая практика и известные положительные случаи работы ЦРКИБ в других организациях
- Выгоды создания ЦРКИБ для организации
  - Проанализировать наличие других аналогичных служб/конкурентов
- Позиционирование нового ЦРКИБ в организации
  - Подчинение и отчетность
- План и предложение о финансировании

Создание ЦРКИБ

- Набор персонала/сотрудников
- Помещение
- Подключение к локальной сети и Интернет
- Разработка Политики безопасности и плана реагирования на инциденты безопасности
  - Должны быть утверждены базовой или вышестоящей организацией
- План информационно-рекламной кампании
- План установления контактов и работы с правоохранительными органами
  - Постоянный контакт для ЦРКИБ
- Разработка Положение о ЦРКИБ (Mission Statement)
  - Что Центр будет делать
  - И что Центр не будет делать

Набор персонала

- Какие специалисты нужны
  - Определяется списком услуг Центра
- Необходимы критические требования к персоналу (в частности, кто не может стать членом ЦРКИБ)
  - Персонал должен быть надежным
- Знание английского языка как международного средства коммуникаций между CSIRT
  - Знание (техническое) английского языка очень желательно
  - Возможность общаться на английском – как минимум один человек
  - ЦРКИБ должен анализировать множественные материалы и публиковать собственные аналитические обзоры и рекомендации
- В случае предоставления услуг 24x7 набрать нужных специалистов

Возможные роли в составе ЦРКИБ

Работа в ЦРКИБ требует энтузиазма и инициативы

- Базовые роли персонала
  - Менеджер или лидер группы/центра
  - Ассистенты и лидеры групп
  - Работники «горячей линии», поддержки пользователей и анализа заявок
  - Работа с собственно инцидентами
  - Проверка уязвимостей и выработка рекомендаций
  - Анализ улик и материалов инцидентов
  - Специалисты по платформам: Windows, UNIX, MacOS
  - Инструктора
  - Информационные аналитики
- Дополнительные роли
  - Системные и сетевые администраторы
  - Программисты и разработчики
  - Веб-мастер(ы)
  - Аудиторы и аналитики рисков, и другие

Формирование контактов

Эффективность работы ЦРКИБ/CSIRT зависит от наличия контактов и взаимного доверия

- Опубликовать информацию о ЦРКИБ
  - Специальная веб-страничка или отдельный веб-сайт
- Известные директории CERT/CSIRT
  - Членство в FIRST
  - Директория и сертификация Trusted Introducer (TI)
- Установить рабочие контакты с организациями и группами публикующими Оповещения (Alert) об инцидентах и угрозах компьютерной безопасности
- Посещение регулярных мероприятий и собраний CSIRT - ВАЖНО
  - TF-CSIRT совещания – 3 раза в год, открыты для членов существующих и планируемых ЦРКИБ, или специалистов, работающих в области компьютерной безопасности
  - FIRST Conference – 1 раз в год, только для членов FIRST или специалистов компьютерной безопасности по приглашению

Финансирование ЦРКИБ

- Финансирование ЦРКИБ должно быть достаточным и включать все затраты на нормальное функционирование Центра
  - Специальная статья на посещение совещаний CSIRT
    - TF-CSIRT – 3 раза в Европе, FIRST – каждый 3-й год в Европе
- Услуги ЦРКИБ могут быть платными или хозрасчетными
  - Плата за фактически предоставляемые услуги
  - Плата по подписке
  - Централизованное финансирование
- Услуги должны быть полными - внутренние и внешние
  - Использование внештатных и внешних специалистов должно учитываться

Дополнительная информация

- Developing an Effective Incident Handling Cost Analysis Mechanism, by David A. Dittrich; SecurityFocus, June 12, 2002 http://online.securityfocus.com/infocus/1592
- Incident Cost and Analysis Model Project http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMP.shtml

Отчетность ЦРКИБ

- Основатели и пользователи (constituency) обычно требуют отчеты
  - Отчеты должны демонстрировать полезность и эффективность
  - Отчеты как инструмент развития и улучшения качества услуг
  - Открытая и позитивная информация может быть помещена на веб
- Некоторые отчеты могут быть платными или по заказу
  - ЦРКИБ должен поддерживать обширную базу как по внетренним вопросам, так и по внешним информационным материалам
- Определенная информация может быть доступна в режиме «реального времени» через веб или по подписке

Следование стандартам

Следование стандартам и общепринятой практике в области компьютерной безопасности и реагирования на компьютерные инциденты безопасности является важным критерием работы и успешного развития Центра

- Существование других провайдеров аналогичных услуг и реальность конкуренции за пользователей
- Сотрудничество с другими Центрами на международном уровне
  - Реагирование на некоторые инциденты может требовать участие Центров из многих стран
- Знание и использование технологий и средств позволяет повысить эффективность работы при меньшем числе персонала
- Как минимум, следовать общепринятой практике для ЦРКИБ/CSIRT
  - Например, RFC 2350 и RFC 2196 и рекомендаций Trusted Introducer

Сертификация/аудит ЦРКИБ

Определенный вид сертификации Центра нужен для приобретения определенного статуса и достижения признания как внутри организации/страны или целевой группы пользователей, так и в международной сети CSIRT

Существующие возможности

- В первую очередь, базовая организация и национальные органы
- Членство в FIRST
  - Необходима рекомендация от действительного члена FIRST, но нет формальной процедуры проверки и контроля деятельности Центра
  - Ежегодные взносы
- Trusted Introducer TF-CSIRT
  - Включение нового Центра в «сеть-доверия» происходит на основании многоступенчатой формальной процедуры проверки/сертификации ЦРКИБ
  - «Сеть доверия» обслуживается и члены периодически контролируются
  - Стоимость обслуживания – 720 EUR

Практические занятие и домашнее задание

Практические занятия будут основаны на информации, подготовленной участниками до начала тренинга

- Описать структуру организации и проанализировать возможное положение ЦРКИБ в структуре организации
- Проанализировать существующую практику реагирования на компьютерные инциденты безопасности, по возможности привлечь реальные примеры
- Описать известные ЦРКИБ или аналогичные службы в поле зрения слушателей

Операционные вопросы работы ЦРКИБ

- Услуги предоставляемые ЦРКИБ
- Помещение
- Средства связи и коммуникации
- Программное обеспечение
- Оборудование
- Процедуры

Услуги предоставляемые ЦРКИБ

Обычный/общепринятый перечень услуг ЦРКИБ

- Координация инцидентов компьютерной безопасности (КИБ)
- Реагирование на КИБ
- Расследование КИБ
- Оповещение об угрозах, уязвимостях, атаках
- Анализ уязвимостях
- Обнаружение случаев вторжения в сеть
- Тренинг и просвещение в вопросах компьютерной безопасности
- Аудит защищенности/безопасности сети, анализ рисков
- Консалтинг по вопросам компьютерной безопасности
- Разработка средств для поддержки внутренних процессов

Потребности организации

- Определить потребности организации
- Определить, какие услуги будет предоставлять создаваемый ЦРКИБ
  - Оценить возможности ЦРКИБ при наличном составе и финансировании
  - Задокументировать в виде отдельного документа, уведомить базовую организацию и сделать его доступным для клиентов
- Предложить решения и/или указать другие организации, которые могут предоставлять дополнительные услуги, решать остальные вопросы
- Определить КАК и в КОГДА будет работать ЦРКИБ
  - Контакт через веб, электронную почту, или по телефону
  - Как предоставляются услуги в рабочее время, вне-рабочее время и есть ли нужда в 24x7x365 регламенте

Структура ЦРКИБ – Общие вопросы

- Должен быть персонал первой, второй и третьей линий поддержки
- Не для всех функций нужен постоянный персонал
  - Другие члены организации могут выполнять определенные функции по совместительству
  - Первые контактные лица должны быть четко определены
  - Нужен четкий учет рабочего времени
- Виртуальный ЦРКИБ может быть создан полностью из уже существующего персонала, работающего на должностях, по своему характеру имеющих дело с аналогичными технологиями, например, специалисты Сетевого операционного центра, системые администраторы, специалисты ИТ

Помещение

ЦРКИБ может иметь дело с конфиденциальной информацией

- Необходимо отдельное помещение со средствами обеспечения физической безопасности
  - Сигнализация, видеокамера
  - Защищенные окна, двери
  - Отдельные помещения для приема посетителей и работы с материалами инцидентов
- Комнаты, шкафы и тумбочки должны иметь замки
- Компьютеры, сеть и архивы должны быть защищены

- Для работы в нерабочие часы
  - Помещение должно иметь гарантированный доступ
  - Помещение должно быть обитаемым (электричество, отопление, вода, т.п.)

Коммуникации и обмен информацией

Электронная почта как основное средство коммуникации

- Должен быть многопользовательский доступ к почтовым ящикам
  - Простейшее решение - использование протокола IMAP
    - Имеет ограниченные возможности для аудита
  - Один человек принимает и сортирует сообщения, другие работают над инцидентами
- Шифрование информации
  - Должны использоваться шифрование и цифровая подпись
  - Поддержка PGP – стандарт-де-факто для CSIRT
  - Персонал ЦРКИБ должен уметь пользоваться технологиями защиты информации

Нахождение контактов

- Регулярные: Директории CSIRTs
  - FIRST
  - Trusted Introducer (TI)
- В ходе расследования инцидентов
  - По IP-адресам
    - RIPE NCC – IR Contact
    - ARIN, APNIC, AfNIC, LatNIC
  - По доменному имени
    - DNS/InterNIC
  - Дополнительно о Центрах, обслуживающих определенные группы
    - FIRST, TI, местные директории
- Должны быть специальные средства для обращения к WHOIS и другим директориям
  - Поддерживать свою базу контактов
- Специальные сайты и списки рассылки
  - Например, SecurityFocus - <incidents@securityfocus.com >

Веб-страничка

Веб-страничка ЦРКИБ должна предоставлять необходимую информацию для пользователей и других центров

- Обслуживаемая группа пользователей (constituency)
- Как контактировать ЦРКИБ (и форма заявки об инциденте, если такая имеется)
- Рекомендации по обеспечению безопасности и источники информации
- Политика безопасности организации или обслуживаемой группы пользователей и другие регламертирующие материалы
- FAQ: Часто задаваемые вопросы
- Веб-сайт ЦРКИБ и информация должны быть защищены
  - Веб-страничка должна быть подписана цифровой подписью PGP и открытый ключ указан

Формы для заявок об инцидентах

- Преимущества
  - Заявители могут ввести необходимые данные для облегчения (автоматической) обработки
    - Обеспечивает полноту и корректность информации
- Возможные проблемы
  - Может обескуражить пользователей сложностью обращения
  - Рекомендация: Должна быть возможность чисто текстовой заявки
- Возможные формы
  - Веб-формы с почтовой отсылкой (mailto:), серверным скриптом (CGI) или JSP
  - Телефонный скрипт или форма для ввода в БД
- Формат данных
  - IODEF (Incident Object Description and Exchange Format)
    - В основном ориентирован на автоматизированные системы, но может использоваться и для форматирования данных от веб-форм

Программные средства

- Операционные системы и базовое/офисное программное обеспечение
- Средства для отслеживания и обработки инцидентов (СООИ)
- Инструментарий для работы по расследованию инцидентов
- Мониторинг сети и делопроизводства

Операционные системы и базовое ПО

- Безопасность Операционой среды определяется уровнем обслуживания
  - Четко отслеживать и применять все обновления и патчи, касающиеся безопасности
  - Использовать версии Windows не менее, чем Windows XP Professional
    - Избегать использования почтовых программ, интегрированных с офисными приложениями, как например MS Outlook
      - Более безопасным является использование Netscape Mail
  - UNIX/Linux среда является потенциально более безопасной

Требования к средствам отслеживания и обработки инцидентов (СООИ)

Incident Handling System (IHS) + Incident Tracking System (ITS) = Система отслеживания и обработки инцидентов (СООИ)

- Должна быть сохранена вся касающаяся инцидента информация
  - Исходная и обнаруженная информация не должна быть потеряна
    - Исходная заявка, контакты, время заявки и инцидента
    - Тип инцидента, тип системы, ее конфигурация, лог-файлы/улики
  - Уникальная идентификация каждого инцидента
- Должна быть возможность записи полной истории каждого инцидента
  - Все коммуникации, исходная информация/улики, извлеченная информация и предпринятые действия
  - Позволять нескольким членам ЦРКИБ работать над инцидентом одновременно
  - Формат и уровень безопасности/целосности хранения данных должен быть достаточным для использования в дисциплинарных или судебных расследованиях

Внедрение СООИ

- Баланс между автоматизацией и ручными процессами
  - Выбор зависит от предполагаемой загрузки
- Простейшее решение – использование почтовых ящиков с множественным доступом на основе протокола IMAP
  - Доступно во всех распространенных почтовых программах
    - Pine, mutt, nmh, Netscape, Eudora, Outlook, Outlook Express, Lotus
- Использование БД упрощает отчетность и анализ трендов
- Использование форм и автоматизация сохраняют время персонала и исключают случайные ошибки
  - Поиск нужной информации и контактов
  - Генерирование стандартных запросов и сообщений
  - Оповещение/напоминание, когда очередной инцидент требует действий
  - Интеграция с системами обнаружения вторжений (IDS – Intrusion Detection System) и использование лог-файлов сетевых экранов

Выбор ПО СООИ

Обычно в арсенале ЦРКИБ используется множество средств

- Собственные БД, средства службы поддержки (helpdesk), средства контроля заявок
- Специальные средства для поддерки расследования инцидентов
- $$$$$ - Интегрированные средства стоят больших денег

Принимать во внимание

- Необходимую квалификацию работников
- Обеспечение безопасности удаленного доступа

Не существует совершенного решения

- Начинать с минимальной конфигурации и интегрировать/ адаптировать новые средства в процессе работы
- Средства могут меняться – форматы и процедуры должны по мере возможности оставаться

Автоматический мониторинг СООИ

Информационные потоки и обработка информации в СООИ должны быть подвержены полному мониторингу

- Лог-мониторинг – syslog, firewall, router
- Сетевой мониторинг – критерии «подозрительной» активности
- Контроль целостности – Tripwire (селективно)
- Мониторинг изменения конфигурации и прав доступа к основным компонентам сети ЦРКИБ
- Периодический контроль/сканирование открытых портов сети

Средства для сбора информации при расследовании инцидентов

Имеются несколько хорошо известных списков и архивов свободно распространяемых средств для сбора информации и востановления системы при расследовании инцидентов

- Архив средств для работы с инцидентами и защиты компьютерных систем - http://www.securityfocus.com/tools
  - Обширнейшая пополняемая коллекция средств с аннотациями и рейтингом
    - Включает коммерческие средства
- CHIHT (Clearinghouse for Incident Handling Tools) – http://chiht.dfn-cert.de/
  - Список обслуживается и содержит краткие аннотации о средствах
    - Сбор улик
    - Исследование улик
    - Восстановление системы
    - Средства отслеживания и обработки инцидентов
    - Безопасный удаленный доступ
    - Профилактические средства

Оборудование

- Сетевое оборудование должно обеспечивать безопасный периметр для внутренней сети ЦРКИБ
  - Удаленный доступ только посредством защищенных туннелей или VPN
  - Удаленное чтение почты только посредством VPN, SSH, или Webmail с HTTPS
- Персональные компьютеры/ноутбуки для персонала
  - Ноутбуки должны иметь апаратные средства авторизации доступа
- Защищенные серверы
  - Для электронной почты, СООИ, веб-сайт
  - Отдельные средства архивирования с шифрованием данных
- Отдельная подсеть для тестирование продуктов, патчей
  - Отключается от основной сети на время тестирования
- Специальное оборудование для судебных (forensic) расследований

Меры безопасности (1)

Сеть и серверы ЦРКИБ должны быть защишены

- Физически: замки, охрана, сигнализация, UPS, кондиционеры
- Операционные системы: инсталяция и обслуживание
  - Периодическое сохранение всей системы (дублирование и архивирование)
  - Возможность быстрого восстановления системы
- Контроль доступа: процедура добавления и исключения пользователей
  - Правила/политика должны быть документированы
  - Сотрудники должны быть ознакомлены под роспись
  - Контроль соответствия действий и привилегий сотрудников и выявление возможных нарушений
  - Удаление логинов сотрудников после их ухода
  - Полезно иметь единую систему контроля доступа

Меры безопасности (2)

- Контроль изменения конфигурации: мониторинг
  - Разработка/доработка – только на отдельной системе
  - Обновление системы должно полностью отражаться в лог-файле и старая система дублироваться
  - Простейшее решение использует RCS/SCSC и ”copy” в Makefile
- Только физический доступ, или возможность удаленного доступа
- Мониторинг
  - Один или несколько центральных syslog-хостов – защищенных и с большим дисковым пространством
  - Использование SNMP и настройка SNMP traps
  - Система периодического оповещения или по-событиям
  - Использование NTP для нотаризации логов и событий
- Аудит: независимая третья сторона

Процедуры

- До возникновения инцидентов
  - Установление системы реагирования и профилактика
  - Информационная деятельность Центра
- Реагирование на инциденты
- Меры после ликвидации инцидентов
- Отчеты и анализ

Политики и планы

Политика безопасности

- Определяет, что требуется, позволено и допустимо
- Определяет характер реагирования и уполномоченные органы

План на случай инцидента (или чрезвычайной ситуации)

- Какая поддержка предоставляется, кому докладывать и кто осуществляет поддержку/реагирование

Политика и план реагирования на инциденты

- Определяет на какие инциденты и как осуществляется реагирование, с каким приоритетом и в какие сроки
- RFC 2350 – пример такого плана/политики в приложении

Политика реагирования на инциденты

- Типы инцидентов и уровень поддержки
  - В форме списка категорий инцидентов в порядке приоритета
- Взаимодействие, сотрудничество и порядок предоставления информации
  - Базируется на Политике безопасности организации(й)
  - Тип информации, ее доступность – кому и в каких случаях
- Коммуникации и аутентификация
  - Какие применяются средства для защиты информации при коммуникациях, включая телефон, электронную почту, обмен файлами, и др.
  - Необходимые и предоставляемые средства удостоверения сторон для различных типов коммуникаций

Типы инцидентов и уровень поддержки

- Угроза человеческой жизни
- Атаки на системы управления сетью или центральными сервисами
- Угроза нормальной работе публичных сервисов
- Угроза разглашения конфиденциальной информации или информации используемой для управления сетью/сервисами
- Угрозы сторонним организациям, аналогичные последним трем, которые исходят от базовой организации ЦРКИБ
- Всевозможные массированные атаки
- Угрозы, вмешательства или другие криминальные действия против индивидуальных пользователей
- Нарушение индивидуального доступа на многопользовательских системах
- Инциденты с персональными системами
- Другие нарушения местной политики безопасности

Профилактические мероприятия

- Аудит – сетей и систем – разовый (начальный) и периодический
- Анализ рисков – рекомендации по улучшению безопасности
- Дублирование ПО и информации – облегчает полное восстановление
- Логирование – политика/профили, анализ, хранение
- Создание безопасного периметра – сетевые экраны, серверы, клиенты, тесты на проникновение
- Регулярные обновления ПО – оценка, тестирование, установка
- Информирование пользователей и системных администраторов

Информация и средства

- Контактные списки
  - Внутренние – администраторы, системные администраторы, пользователи, администраторы основных сервисов и систем, например, сетевых экранов, IDS
  - Внешние – провайдеры верхнего уровня, другие Центры, правохранительные органы
- Список IP-адресов – создание и обслуживание
  - Внутренний – топология сети, распределение адресов, расположение систем
  - Внешний – список IP-регистров, например, RIPE NCC, и средства доступа к ним, например, WHOIS или веб
- Набор средств для сбора информации/улик и восстановления систем
  - Для Windows, UNIX, MacOS, др.

Известность вашего ЦРКИБ

В случае инцидента, ЦРКИБ вынужден будет контактировать и взаимодействовать со своими пользователями, другими Центрами и организациями

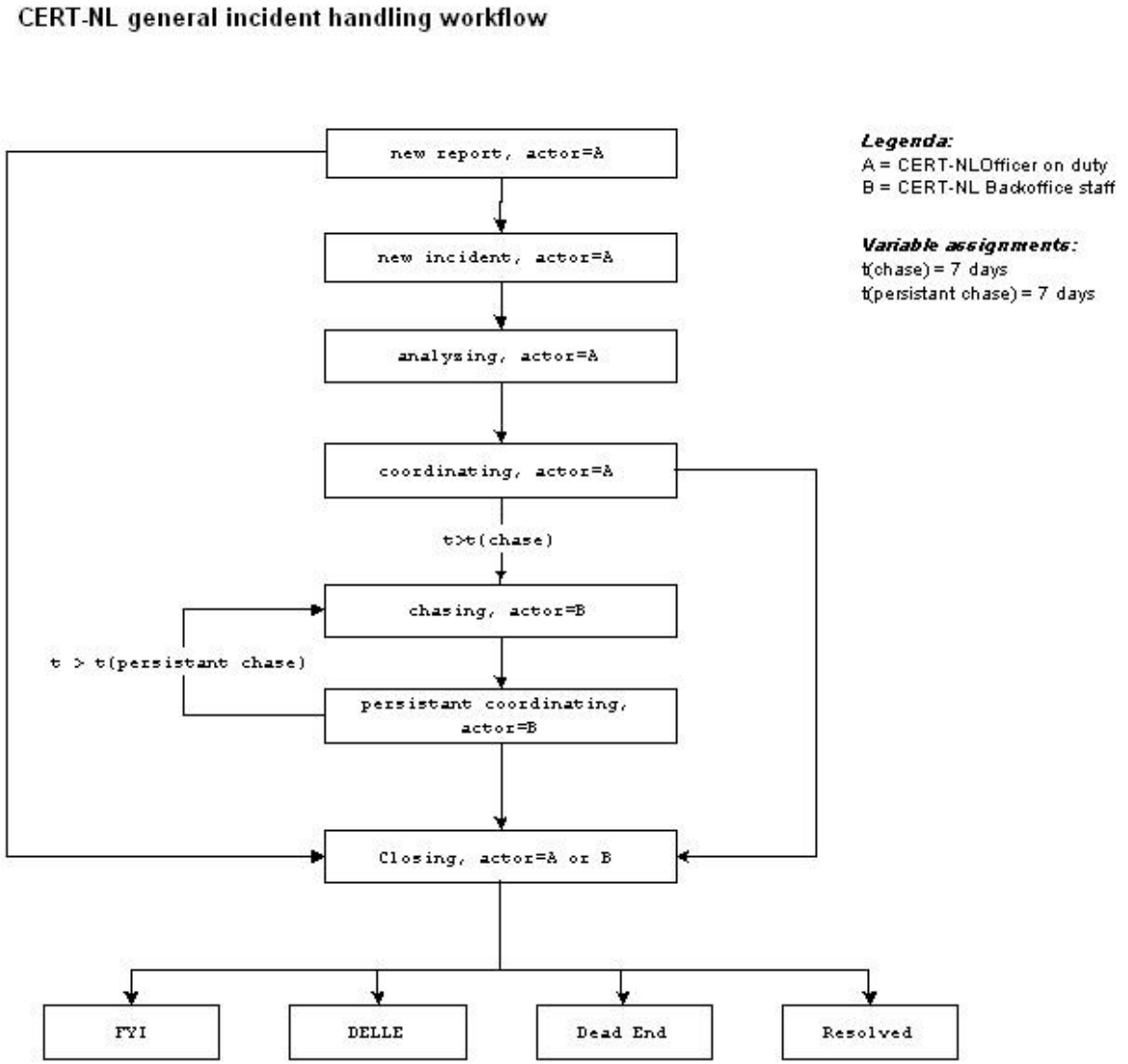
- Они должны знать вас и доверять – основа успешного разрешения инцидентов
- Внутренняя известность – через веб-страничку, политику, оповещения, рекомендации, внутренние бюллетени
- Внешняя известность
  - внешняя веб-страничка
  - списки и личные контакты среди региональных ассоциаций FIRST, TI, TF-CSIRT
  - Директории провайдеров и база данных RIPE NCC

Процедуры реагирования на инциденты

Все стадии реагирования на инциденты должны быть документированы, или по крайней мере, продуманы

1. Прием заявок/жалоб и первичная оценка
   - Assessment and Triage – оценка и сортировка
2. Документирование процесса обработки
3. Сбор исходных данных, идентификация и анализ
4. Уведомление – начальное и по мере расследования
5. Эскалация – в зависмости от категории инцидента или уровня поражения
6. Сдерживание/противодействие
7. Сбор и сохранение улик и других материалов инцидента
8. Устранение последствий и востановление

Типовый алгоритм реагирования



На примере CERT-NL

http://www.surfnetters.nl/meijer/tf-csirt/workflow/workflow.html

Реагирование (1): Прием заявок и оценка

Является ли это проблемой и как срочно требуется разрешение?

- Оценка согласно Политики безопасности и Политики реагирования на инциденты
- Решение принимается в соответствии с предварительно установленными критериями и текущей загрузкой персонала
  - Не все заявки будут соответствовать реальным инцидентам
  - Принятая заявка направляется к соответствующему специалисту или группе
- Эта функция может быть поручена/делегирована дежурному специалисту или службе
  - При достаточной тренировке и поддержке экспертной системой эту функцию может выполнять служба поддержки пользователей организации/сети (helpdesk, call center)

Реагирование (2): Документирование процесса

Задокументировать исходную информацию и быть готовым к документированию всей последующей информации

- Автоматизация процесса документирования позволит не только упростить работу персонала, но и повысить достоверность данных
  - Цифровая подпись и заверение временной квитанцией (timestamping)
- Облегчает обмен информацией об инцидентах
- Позволяет ретроспективно проанализировать процесс расследования и извлечь уроки
- Необходимо для судебного или дисциплинарного расследования
  - Материалы по возможности должны соответствовать требованием, предъявляемым к судебным материалам

Реагирование (3): Сбор исходных данных, идентификация и анализ

Собрать и проанализировать улики/данные об инциденте

- Использовать рекомендации по сбору улик
  RFC 3227 Guidelines for Evidence collection
  - Обрабатывать и сохранять данные в порядке изменчивости
    - registers, cache
    - routing table, arp cache, process table, kernel statistics, memory
    - temporary file systems и disk
    - relevant remote logging and monitoring data
    - physical configuration, network topology
    - archival media
- Избегать возможных потерь данных
  - Не останавливать работу системы и не отключать от сети, в крайнем случае, выдернуть шнур из электрической сети
    - По возможности иметь продуманную процедуру начального сбора данных
- Соблюдать конфиденциальность и приватность данных

Реагирование (4): Уведомление

Быстрое и корректное уведомление соответсвующих лиц и служб

- Согласно существующему Плану реагирования на инциденты
  - Использовать согласованные процедуры и формы уведомления
  - Все ответственные лица должны быть уведомлены
- Раннее уведомление позволяет получить больше поддержки от команды и сотрудничающих служб/организаций
- Последующие уведомления
  - Продумано и уравновешено,без элементов паники
  - В некоторых случаях подготовить заявление для прессы

Реагирование (5): Эскалация

В случае необходимости привлечение внешних и дополнительных ресурсов

- Информировать менеджмент для привлечение внутренних ресурсов
- Другие Центры для помощи в прекращении атаки и разрешении инцидента

- Согласно существующему Плану реагирования на инциденты
  - Уменьшает влияние стрессовой ситуации на действия персонала
- Ответственные лица должны быть информированы в случае усугубления последствий инцидента

Реагирование (6): Противодействие

Ограничить дальнейший ущерб вследствии (продолжающегося) инцидента

- Действия должны быть согласованы/оговорены для типовых инцидентов
  - Позволяет быстрое реагирование
  - Особо важно для внеурочных ситуаций
- Иметь четкое представление о ключевых точках для претотвращения нежелательной активности
  - Внутри сети – для изоляции пораженных систем
  - Внутри сети – для предотвращения исходящих атак, например, сетевой экран или входной маршрутизатор, почтовый сервер
  - Вне сети – для предотвращения внешних атак, например, шлюз провайдера

Реагирование (7): Сбор и сохранение улик

В случае предполагаемых дисциплинарных или судебных наказаний обеспечить сбор и сохранение улик и других данных об инциденте

- Список возможных наказаний для различных категорий инцидентов или атак должен быть подготовлен заранее
- Средства для сбора улик и данных должны быть в наличии
  - Отдельный компьютер или загружаемый CD
- Руководство и инструкции для пользователей и/или пострадавших должны быть готовы для типовых категорий инцидентов
- Действовать в соответствии с RFC 3227 Evidence collection
  - Сохранять данные в порядке изменчивости
- Все собранные данные должны быть помечены в порядке сбора и во времени

Реагирование (8): Устранение последствий и восстановление

После сбора данных последствия инцидента должны быть устранены и нормальная работа должна быть восстановлена

- Должны быть подготовлены и быть в наличии
  - Средства для контроля целостности файловой системы и данных
    - Tripwire
  - Дубли/архивы системы и данных – проконтролированы при аудите
  - Инсталяционные носители – проконтролированы при аудите
  - Средства востановления как компонент средств анализа
    - Средства восстановления должны защищены от возможных последствия «закладок» и rootkits
  - Любая система может быть восстановлена
    - Подготовка определяет успех и минимальные потери

Действия после инцидента

- Дисциплинарные воздействия и наказания
  - Злоумышленник/инициатор атаки должен быть определен
  - Наказание и возмещение ущерба в соответствии с существующими правилами и законодательством
- Дополнительные меры, чтобы предотвратить подобные инциденты
- Извлечь уроки и при необходимости пересмотреть Политику безопасности
- Информировать пользователей и просветить пострадавших

Отчеты и анализ

- Задокументировать положительный опыт
  - Отчеты и статистика может быть полезна как собственному персоналу, так и другим Центрам
  - Некоторая информация может иметь ограниченное распространение
    - Злоумышленники и хакеры также учаться
- Предоставление формального отчета об инциденте может быть обязанностью Центра
  - Как часть соглашения с учредителями или SLA (Service Level Agreement), а также как часть соглашение о сотрудничестве с другими центрами
- Пересмотреть существующую Политику безопасности
  - В случае необходимости провести аудит системы и/или сети

Информационная деятельность Центра (1)

В зависмости от типа ЦРКИБ, может составлять большую или меньшую часть предоставляемых услуг

- Существуют множественные источники регулярной информации об уязвимостях компьютерных систем и соответствующих рекомендаций
  - Службы производителей и поставщиков: Microsoft, Cisco, Sun, RedHat
  - Фирмы и организации в области безопасности: ISS, BugTraq, CA, SANS
  - Центры реагирования и обмена информацией: CERT/CC, SecurityFocus, eCSIRT, национальные Центры
- Получение определенной информации может потребовать подписания соглашения о неразглашении (NDA – Non-Disclosure Agreement)
  - ЦРКИБ должен поддерживать доверительные отношения с поставщиками и другими Центрами

Информационная деятельность Центра (2)

- ЦРКИБ должен отслеживать, оценивать и отбирать информацию, актуальную для своих пользователей
  - Информация часто должна быть адаптирована к нуждам пользователей
  - Краткая аннотация или полный перевод исходных материалов может быть необходим
    - Какие системы уязвимы
    - Возможный ущерб, например, отказ в обслуживании, потеря информации
    - Оценка опасности (реальная, теоретическая, ...)
    - Как избежать опасности и устранить уязвимость (обновления системы, патчи)
    - Возможные последствия применения «быстрых» патчей или чрезвычайных мер

Информационная деятельность Центра (3)

- ЦРКИБ может выпускать свои собственные рекомендации
  - На основе компиляции получаемых материалов или собственных исследований
  - Рекомендации и опыт ликвидации прошедших инцидентов
- Информация должна быть доступна по подписке и через веб
  - Достоверность информации должна подтверждаться цифровой подписью Центра
    - Пользователя должны иметь возможность проверить достоверность и целостность получаемой информации

Заключение

- Центр реагирования на компьютерные инциденты безопасности – важный компонент обеспечения безопасности сети и компьютерных систем
- Существуют сильное сообщество сотрудничающих ЦРКИБ, которое заинтересовано и готово помочь новым Центрам
- Существуют обширные информационные материалы в помощь новым ЦРКИБ
  - Специально для Silk Security Workshop http://www.uazone.org/znews/security/

Вопросы и комментарии?