CERT AM services
Сервисы CERT AM

I.Mkrtumyan imkrumyan@isoc.am
Internet Society - Armenia

Задачи центра информационной безопасности

Центр информационной безопасности страны призван помочь Интернет сообществу, а вместе с ним и всей стране, предотвратить паралич информационной инфраструктуры и преодолеть последствия атак на нее.

- *Недавние события в Эстонии, когда Интернет инфраструктура страны в течение нескольких недель была парализована из-за массовых атак, в основном DDOS, говорит о том, что этот сценарий, кастати уже названный кибервойной, может повторится в любой стране.*

- *В Интернете полно инструментов для спаммеров и хакеров. Для того, чтобы стать хакеров не нужно ни глубоких знаний в программировании, ни в принципах работы сети. Для хакеров разработан очень дружественный софт. Примеры приведены на следующих слайдах.*

495,00 руб. SPAM-DVD - этот диск предназначен, прежде всего, людям, которые имеют свой бизнес, владельцам сайтов различных тематик, людям, которые хотят заработать хорошие деньги. Диск включает в себя полностью проработанный софт, как для рассылок и обработки огромных e-mail баз, так и для качественного их сбора: по ключевым словам, по странам, по конкретному региону; большую базу объемом 100 млн. e-mail адресов, активно использующихся по всему миру.

345,00 руб.
HACKER-CD - НАДЕЖНЫЙ И МОЩНЫЙ ИНСТРУМЕНТ ХАКЕРА!

HACKER-CD - это полный программный комплекс Хакера. В комплект поставки комплекса входят сотни программ и утилит, предназначенных для взлома любого софта: взлом icq, взлом паролей, взлом сайтов, взлом почты, взлом архивов, взлом сети и многого другого софта. Весь комплекс программ является уникальным. Данная информация предоставляется только для ознакомления на Вашем персональном компьютере, для восстановления своих паролей и файлов, и не должна использоваться в сети Интернет, либо другой сети в противоправных целях. Информация может использоваться Вами только в том случае, если Вы понимаете, какие последствия могут возникнуть в результате неправильного использования.

Стандарты по информационной безопасности

- ***27 April 2007 – Семинар Офиса ОБСЕ Методы управления информационной безопасностью в соответствии с международно-признанными стандартам.***
- ***Основная цель стандарта ISO 17799 – общая методология создания, внедрения и оценки системы управления информационной безопасностью, применимой к коммерческим, государственным и не-государственным структурам. Этот стандарт является частью обязательств по Европейской Конвенции по Кибербезопасности, ратифицированной Арменией в 2006 г.***
- ***В идеале каждая организация должна стремиться к внедрению этого стандарта.***
- ***В Армении есть специалисты по международным стандартам и при необходимости мы будем обращаться к ним.***

Сервисы центра информационной безопасности

Мы предлагаем, чтобы Центр предоставлял следующие сервисы:

- ***Оповещение***
  Распространение информации, описывающей атаку взломщика, предупреждение о возможном проникновении, вирусах, с предоставлением кратких рекомендаций по борьбе с этими явлениями. Эта информация рассылается сообществу во время возникновения реальных проблем вместе с кратким руководством по блокировке атаки и восстановлению системы. Конечно, сисадмины, в основном, подписаны на конференции, где рассылаются извещения о проблемах безопасности в программном обеспечении. (Я, например, подписан на security-bulletins@us-cert.gov , который рассылает очень качественную информацию) CERT AM будет рассылать членам сообщества пользователям важную информацию по безопасности, предупреждения и другую необходимую информацию.

- ***Мы просим участников сообщества регистрировать инциденты на сайте CERT AM. Мы просим Вас посылать информацию о проблемах безопасности на наш форум и на адрес мейлинг листа infosec@cert.am. Эта информация будет проверена модератором и распространена по сети. Все это позволит обобщить статистику и принимать превентивные меры.***

- ***Между Центром и членами сообщества должен быть подписан меморандум о взаимопонимании.***

- ***Следует отметить, что центр – это не некая бюрократическая контора, которая что-то требует и что-то распеделяет, это не кто-то, обладающий абслютными знаниями в этой области, а мы с вами, т.е. совокупный интеллект сообщества. Центр это всего лишь орган, который позволит обединить специалистов и направить их знания и усилия в нужном направлении для всеобщего блага. Эта миссия должна будет выполняться как за счет финансовой поддержки, так и добровольного содействия волонтеров. Естественно, волонтеры будут вознаграждаться путем бесплатного обучения, в том числе и на зарубежных курсах, а также другими поощрениями.***

- **Обработка инцидента**

Включает получение данных, их сортировку, классификацию и приоритетизацию, анализ инцидента, а также ответные акции. Последние включают:
- действия по защите систем и сетей, подвергшихся атаке
- предоставление решений по восстановлению
- отслеживание активности взломщиков в других частях сети
- восстановление системы
- установление патчей или ремонт системы

- *Анализ инцидента*
  Включает изучение всех доступных данных, вещественных доказательств и следов взломщика. Целью анализа является определение масштаба повреждений, суть инцидента, и возможные ответные действия. Анализ включает:
  - сбор доказательств, их сохранение, документирование для реконструкции событий атаки. Он должен обеспечить доказательную цепочку событий, которая может понадобиться при юридическом рассмотрении вопроса о взломе.

- *отслеживание источника атаки. В этот процесс могут быть вовлечены несколько сетей, таких как университетскя сеть, сеть сервис провайдера, dial-up провайдеры, телефоны юзеров, интернет кафе и т.д. В этом процессе возможно также потребуется разрешение органов госбезопасности.*
- *Помощь в обработке инцидента может быть следующей:*
  - Помощь по телефону, факсу, эл.почте
  - Выезд на место происшествия для анализа инцидента на месте. Центр может обеспечить непосредственную помощь на месте инцидента, выполнить анализ инцидента и помочь в восстановлении системы.

- ***Аудит или оценка информационной безопасности системы***

  Центр может обеспечить детальный анализ инфраструктуры информационной безопасности:
  - на наличие корпоративной политики (правил и процедур) по информационной безопасности;
  - проверку конфигурации аппаратуры и программного обеспечения, маршрутизаторов, брандмауэров, серверов, рабочих станций на соответствие общепринятым рекомедациям;
  - интервью с сотрудниками организации, ответственными за информационную безопасность, для определения уровня знаний в этой области;
  - выявление уязвимостей корпоративной системы;
  - тестирование системы моделированием реальных атак;
  - на соответствие мировым стандартам по информационной безопасности.

  Мы планируем подготовку одного-двух специалистов сообщества на получение сертификата по мировым стандатам в области информационной безопасности (OCTAVE, CRAMM, FIRM, CASP, COBIT).

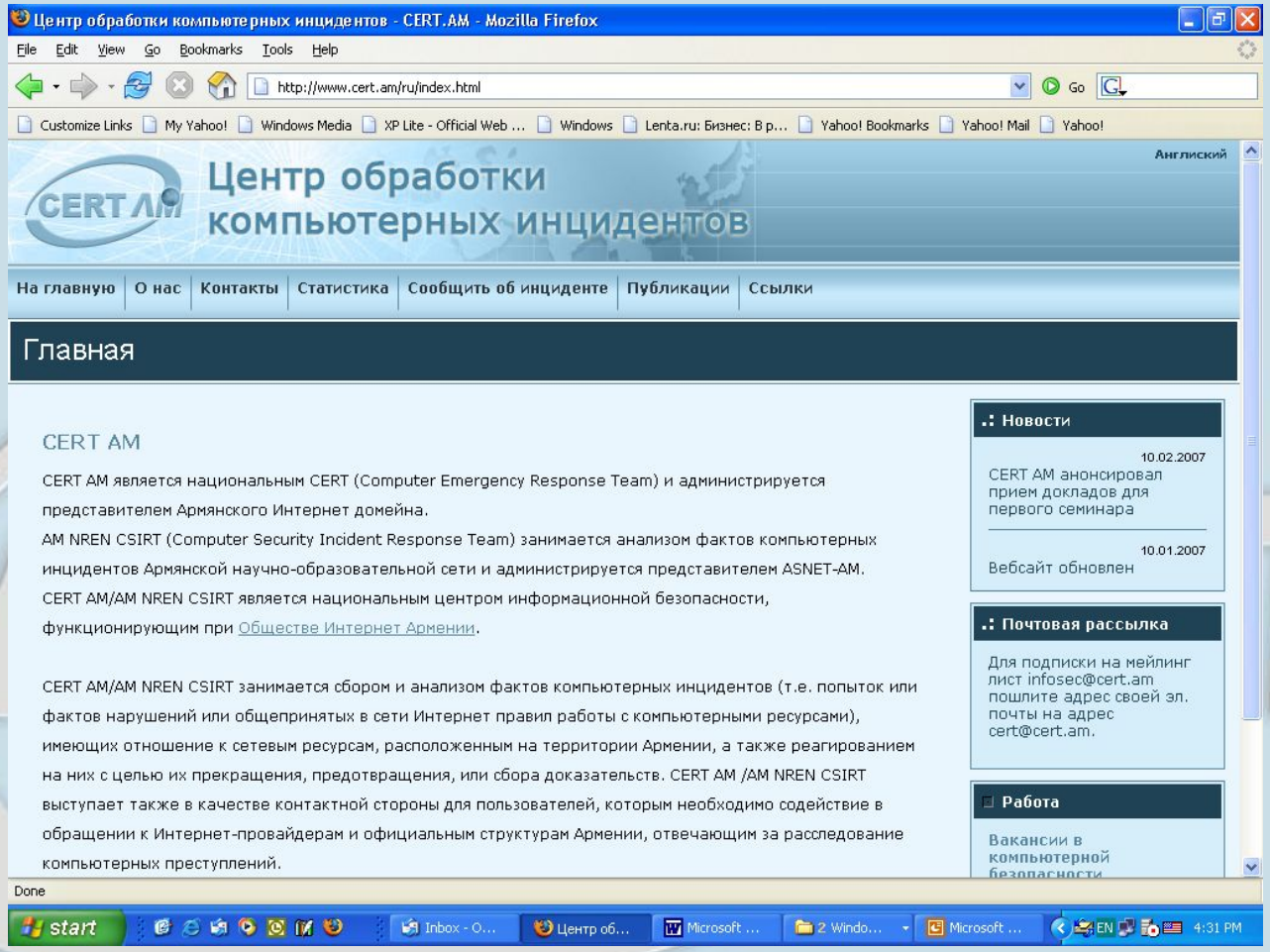
- ***Разработка рекомендаций по наилучшей практике информационной безопасности и их распространение***
- ***Планирование восстановления при катастрофах***
- ***Консультации по информационной безопасности***
- ***Обучение***
- ***Сертификация специалистов по информационной безопасности (Cisco security)***

- **Меморандум о взаимопонимании (МоВ)**

- *Центр обязуется:*
- - организовать и управлять мейлинг листом и дискуссионным форумом сообщества специалистов по инфромационной безопасности (ССИБ),
- - пересылать членам сообщества информацию об угрозах, предупреждения, рекомендации, а также наиболее важную информацию от других CERT-в,
- - оказывать помощь членам сообщества по анализу инцидента, восстановлению систем, отслеживанию места возникновения атаки, а также другие услуги, обявленные Центром,
- - организовать обучение и трейнинг для членов ССИБ.

- *Члены сообщества специалистов по инфромационной безопасности обязуются:*
  - извещать Центр об инцидентах,
- - принимать к сведению предупреждения об угрозах и предпринимать необходимые действия следующего характера:
- а) подтвердить прием оповещения
- б) предпринять необходимые меры
- в) доложить в Центр о принятых мерах
- - предоставлять Центру информацию (в результате анализа логов) об источнике атаки, если последняя возникла из их сети, а также предпринять меры по нахождению злоумышленника,
  - принимать активное участие в деятельности Центра, распространении информациии о деятельности Центра и привлечении в ССИБ специалистов по информационной безопасности.

Web site: www.cert.am
Mailing list: infosec@cert.am



June 22, 2007, Yerevan

"CERT AM Workshop"

Приглашаю к дискуссии

Благодарю за внимание