

Essential tasks of CERT AM

Насущные цели и задачи CERT AM

CERT/CSIRT уже основаны и существуют.

Общий круг задач определен с 2005 года.

“CERT-AM занимается сбором и анализом фактов компьютерных инцидентов выступает также в качестве контактной стороны для пользователей, которым необходимо содействие в обращении к Интернет-провайдерам и официальным структурам Армении, отвечающим за расследование компьютерных преступлений”

Однако, за все годы существования, несмотря на усилия как членов Интернет Сообщества, так и просто активистов – среди которых были и признанные профессионалы в области аудита безопасности информационных систем, эта структура пока что остается практически пассивной.

Что же мешало CERT-у начать активную деятельность?

Ответив на этот вопрос, мы сможем перейти от общих концепций к определению действительно необходимых и реализуемых – насущных целей и задач центра информационной безопасности CERT AM.

Что говорят эксперты о прошлом опыте:

“A country needs a critical mass of people who understand and care about a particular subject. without that mass it is very difficult if not impossible to do anything”

“Чтобы CERT.AM “сработал” нужен интерес коммерческих и не коммерческих партнеров, нужны пользователи, которые умеют читать и понимать, что им говорят и зачем, и, конечно, нужен staff, который будет на все это тратить время”

“it's not going to be easy - and not because you are not doing enough but because you need others for this thing to work. Without support of partners and understanding of users CERT won't be.”

Подобные замечания и оценки указывают на **отсутствие** в прошлом при создании CERT -а таких основополагающих факторов как

- потребность в кооперации между потенциальными клиентами / партнерами в решении проблем безопасности IT служб
- осознание возможных преимуществ существования CERT- а как со стороны государственных структур, так и частных лиц
- понимание, что вопрос безопасности информационной системы не может решаться эпизодически и требует постоянного внимания, времени, специализации, а также программных и технических средств

Современные проблемы:

Ситуация, которую мы наблюдаем сегодня, изменилась, сформулированы даже детальные планы на ближайший год, однако достаточно ли этих изменений, чтобы с уверенностью сказать – CERT становится действующей структурой ?

Думаю, что положительный ответ на этот вопрос зависит теперь уже от

1. принципов формирования команды CERT-AM,
2. среды функционирования,
3. возможности контроля за качеством предоставляемых сервисов,
4. степени участия государства и, в связи с этим, доверия клиентов

Что может сегодня обеспечить CERT-AM и как это согласуется с ожиданиями потенциальных

клиентов?

Кто является потенциальным клиентом и каковы условия предоставления услуг ?

Как предполагается (и предполагается ли вообще) вовлечение CERT-AM в создание и подготовку специалистов для внутренних CERT-ов формирующихся в организациях и компаниях ?

Ответы на эти и подобные вопросы – принципиальны, так как от них зависит будет ли CERT-AM выполнять общепринятые задачи CERT или это скорее WARP

<http://www.warp.gov.uk/Index/indexintroduction.htm>

Большую помощь в успешной реализации планов по активизации деятельности CERT-AM может оказать рекомендованный **Европейским Агентством по Сетевой и Информационной Безопасности (ENISA)** документ *“Пошаговое руководство по созданию CSIRT”*

Однако, следует учесть, что этот документ может не учитывать специфичных для Армении отношений и возможно не все цели и методы приведенные в данном руководстве могут быть приемлемы для нашего государства.

Будущее CERT-AM

Эффективным стимулом для развития CERT-AM может также стать привлечение молодежи (студентов и возможно старшеклассников).

Почему бы вместе с группой экспертов не привлекать к решению каких-то задач и студентов, специализирующихся в IT и CS ?

Это поможет им быстрее интегрироваться в профессиональную среду после окончания университета, а CERT-AM -у развиваться