РЕАЛЬНЫЕ РИСКИ В ВИРТУАЛЬНОМ ПРОСТРАНСТВЕ

K. Nuthall and A. Osborn Real risks in virtual space.-
Nuclear engineering international, 2009, March, vol. 54, № 656, p. 38

Безопасность АЭС зависит от надежности компьютерных сетей. Киберпреступники могут использовать слабость системы защиты информации, чтобы ее повредить. Правительства реагируют на это новыми программами.

В марте 2008 г. одна из американских АЭС в штате Georgia была аварийно остановлена из-за сбоя в программном обеспечении компьютерной сети. Инцидент был вызван тем, что компьютеры данной серии были объединены в эксплуатационную систему, управляемую с АЭС Hatch в городе Baxley, и когда специалисты вводили в рабочую схему новые данные, неожиданно прошла недостоверная информация, что уровень воды в резервуаре охлаждения топливных стержней упал до критического значения. Аварийная компьютерная система выдала команду на отключение станции.

Официальные лица позже заявляли, что исследованию подвергалась кибернетическая уязвимость объекта; при этом было установлено, что системы взаимосвязаны так, что не было возможности предпринять корректирующие действия раньше срабатывания автоматики. С тех пор инженерами станции заменены все соединительные линии между серверами. Эксперты по безопасности Интернета заявили, что рассматривают инцидент в качестве примера поведения взаимосвязанных систем вплоть до того момента, когда с помощью Интернета еще можно диагностировать реальную уязвимость.

Конечно, в данном случае останов был начальным событием, но злоумышленники пытаются (и успешно) нарушить электрические цепи АЭС. В январе 2008 г. ведущий специалист по кибернетической безопасности Tom Donahue обнаружил, что действующие в Интернете хакеры атаковали компьютерные системы предприятий, находясь вне Соединенных Штатов, и вызвали по крайней мере одно отключение из нескольких. Неизвестно, кто и почему предпринял эти атаки, но все эти незаконные проникновения осуществлялись через Интернет; мы предполагаем, что некоторые злоумышленники извлекали из этого выгоду.

В мае 2008 г. в отчете специального органа правительства США – US Government Accountability Office – отмечалось, что крупнейшая энергетическая компания Tennessee Valley Authority, снабжающая 8,7 миллионов потребителей, весьма уязвима для кибернетических атак, причем это относится ко всем ключевым элементам ее инфраструктуры.

Возможные решения

Требуется всеобъемлющий подход к проблеме. Прежде всего – участие межправительственных агентств. NATO образовало специальное ведомство по управлению кибернетической безопасностью – Cyber Defence Management Authority (CDMA), располагающееся в Брюсселе. CDMA призвано помочь усилить национальные системы, разрабатывающие центральные линии коммуникаций и стратегию определения будущих угроз. В дополнение к этому семь стран, членов NATO, согласились создать совместный центр по кибернетической безопасности, расположенный в Таллинне (Эстония) для управления разработками и проведения тренировочных работ в сфере военной кибернетики. Члены NATO консультируются между собой в случае атаки на компьютерные сети через Интернет.

МАГАТЭ готовит новую публикацию о кибернетической угрозе в 2009 г. Специалист информационной службы Европейского Союза Viviane Reding пообещала подготовить детальный доклад о противодействии кибератакам.

В последние годы уроки, извлекаемые из фактов нарушения безопасности, кажется, начинают доходить до сердца людей, особенно в США. В Институте ядерной энергетики говорят, что к кибернетическим угрозам очень хорошо подготовились. Пресс-атташе Института Tom Kauffman заявил, что все компьютерные системы на АЭС США автономны, представляют собой как-бы острова, они не соединены и никогда ранее не были соединены с Интернетом. Если внешние персональные компьютеры, например, ноутбуки принесены на станцию и подключены к ее сетям с целью мониторинга каких-то единиц оборудования или проведения иных испытаний, то они прежде всего должны подвергаться тщательному осмотру, их программы проверяться, и в течение всего времени работы на станции они должны находиться под постоянным контролем.

Вероятность кибератаки на станцию с изолированными компьютерными системами весьма мала. Однако, в отрасли имеются наемные работники, которые в силу своих служебных обязанностей предпринимают атаки на компьютерные системы в рамках отраслевой программы противодействия кибератакам; они при этом разрабатывают режимы и ведут протоколы.

Ответственные лица, имеющие дело с защитой высокочувствительной информации, утверждают, что компании, вовлеченные в производство электроэнергии на АЭС, «весьма озабочены» тем, кто именно в организации допущен к аварийному планированию, и пытаются гарантировать нераспространение таких сведений за пределами узкого круга руководящего персонала. Хакеру будет чрезвычайно трудно проникнуть в систему и получить доступ к этим планам; это простейший способ перекрыть утечку информации и пресечь подкуп кого-либо внутри коллектива. Более 90 % кибернетических преступлений обнаруживаются и они совершаются не хакерами, а кем-то из сотрудников организации или с их помощью.

В. Цукерник