ЗАЩИТА ДАННЫХ В СЕТИ DEEPNET

ГУ НИИ ВС РБ

г. Минск, Республика Беларусь

Мастыкин А.Л.

Утин Л.Л. –к-т техн. наук, доцент

Известно, что при обеспечении безопасности сети Интернет возникает множество проблем. Специалисты в области защиты информации по-разному подходят к приоритетности вопросов обеспечения безопасности информационных ресурсов сети (далее ресурсов) и безопасности пользователя данными ресурсами.

При обеспечении безопасности ресурсов сети основными направлениями являются сохранение конфиденциальности личных регистрационных данных пользователей защищаемого ресурса, сохранение в неизменном состоянии структуры и содержания ресурса, размещенного пользователями с соответствующими правами доступа. Кроме того, должны быть предусмотрены меры по недопущению модификаций, разработанных алгоритмов работы ресурсов, таких как внедрение программ для рассылки спама.

Безопасность ресурса сети основана на комплексе мер защиты предпринятых как разработчиками, так и администраторами сайтов и серверов на которых эти ресурсы размещены. К основным из них относятся:

подтверждение того, что пользователей ресурсов не является роботизированной программой;

регистрация новых пользователей ресурса;

идентификация и аутентификация пользователей;

ограничение количества запросов пользователя;

ограничение количества пользователей одновременно обращающихся к ресурсу сети.

Безопасность пользователя ресурсами в основном зависит от его действий, а также используемого программного обеспечения, установленного на ПЭВМ.

Необходимо заметить, что то информационное пространство, доступное через такие современные браузеры как «Opera», «Internet Explorer», «Google Chrome», «Fire Fox», «Safari» и т.д. (назовем его «видимый Интернет») представляет собой лишь, небольшую, видимую часть, огромной, многоуровневой информационной структуры, которая постоянно разрастается. В «Видимом Интернете» предпринимаются попытки контроля контента на предмет легальности и именно в нем проводит время среднестатистический пользователь. Вместе с тем известна часть Интернета, содержащая информацию, предназначенную для определенного кругов пользователей («Deepnet», «DarkNet», «DeepWeb», «Глубокий интернет», «Invisible Web» и т.д.)

Эта информация может быть:

-недоступной тому, кто не знает что конкретно ему нужно, и где это находится;

-спрятана за паролями;

-находится в архивах;

-не подключена к интернету, но является частью сети;

-на неиндексируемых страницах;

- на заброшенных форумах

- огромных объемов не всегда легального контента.

Например, Darknet знаменит тем, что является местом, где многие посетители получают на свои устройства специализированное программное обеспечение даже не подозревая, что стали жертвами кибермошенничества. Успешное противодействие данным угрозам возможно при наличии у пользователей специализированных знаний в области информационных технологий и противодействия компьютерным преступлениям.

Следовательно, для относительно безопасного посещения «Темной сети» должны использоваться компьютерные программы позволяющие:

- обеспечить защиту приватности и анонимности в сети;

- шифровать текст (включая электронную почту) и файлы;

Более эффективно применение сложных и дорогостоящих технических решений, включающих собственные серверы , wifi роутеры (или другое аналогичное оборудование дальнего радиуса действия), обеспечивающее доступ в интернет. Такой подход актуален для держателей своих ресурсов в «Invisible Web». Однако для осуществления этого решения необходимы не только средства на приобретение вышеуказанного оборудования, но и соответствующая техническая подготовка. В докладе предлагается к обсуждению некоторые проблемные вопросы защиты информации в сети Deepnet.

Список использованных источников:

1. C. Sherman, G. Price: The Invisible Web: Uncovering Information Sources Search Engines Can’t See. CyberAge Books, 2001.