УДК 004.056; Р-93

Т.А. Рыбина, Н.И. Белодед

Академия управления при Президенте Республики Беларусь

БЕЗОПАСНОСТЬ WEB-СЕРВЕРОВ

Создавая свои документы, общаясь с различными людьми, достигая своих целей, мы все пользуемся одной известной аксиомой: информация должна быть в безопасности. Именно поэтому большинство из нас обеспечивают защиту своих данных различными путями. Однако, защищая сервер, человек не всегда задумывается о том, как будет работать эта защита, а ведь именно от этого зависит безопасность нашей информации. Интернет уже давно перестал быть просто сетью из html-страниц. Сегодня это еще и сложные приложения, скрипты, транспортные сети, телеконференции, электронная почта и многое другое, значит и система безопасности также должна становиться более сложной и совершенной.

Впервые проблема безопасности web-серверов была опубликована в 1985 году Стивом Беллоуином, но реальный масштаб угрозы для серверов доказал червь Code Red. Он вывел из строя именно те серверы, которые не следили за своей растущей уязвимостью (эта беспечность в итоге стоила миллионы долларов). Основными причинами растущей уязвимости сегодня являются: регулярная смена конфигурации сетей (особенно характерно для развивающихся организаций); большое число лиц, имеющих root или администраторский доступ к серверу; использование как пиратского, так и лицензионного программного обеспечения и др. Из всего этого видно, что защита сервера сводиться к управлению рисками.

Для каждого вида информации необходим свой уровень защиты. Сегодня ее иерархию делят на шесть уровней. Первый – самый элементарный и обязательный (главный инструмент защиты – firewall). Второй уровень подразумевает конфигурацию операционной системы, под управлением которой работает сервер. Третий уровень – защита сети, оснащение датчиками атаки сетевого оборудования и программного обеспечения провайдера. Четвертый уровень – установка программного обеспечения на уровне хостинга (на этом уровне, как правило, возникает множество проблемам). Пятый уровень принято делить на два подуровня: A и B. На уровне A устанавливается специальное программное обес-

печение, которое играет роль прослойки между операционной системой сервера и всеми приложениями, на уровне В устанавливается ориентированные на конкретные приложения firewall и/или прокси-серверы. Шестой уровень – своеобразная вершина безопасности. Этот уровень предполагает использование операционных систем и приложений, разработанных специально для данной компании.

Уровень защиты пользователя необходимо выбирать исходя из его потребностей и финансовых возможностей. Но существуют и общие, наиболее простые правила, которые необходимо соблюдать. Так, например, размещение сервера в демилитаризованной зоне (DMZ); блокирование firewall входящих соединений со всеми портами, например, кроме http и https; предварительное планирование расширения сети и обозначения сегментов сети, способных к расширению; использование лицензионного ПО, желательно одного производителя; периодическое сканирование серверов для проверки отсутствия на нем уязвимых мест и др.

Список литературы

1. Федотов А.М. Проблемы безопасности информации в www информационных системах / А.М. Федотов. – М.: Мир, 2000. – 254 с.

2. Медведовский И.Д. Атака через INTERNET / И.Д. Медведовский, П.В. Семьянов, В.В. Платонов; под ред. проф. П.Д. Зегжды / НПО: «Мир и семья – 95».– 1997. – 334 с.

3. Петров В.В. Как выбрать www-сервер / В.В. Петров // Мир ПК. – 197. – № 3. – 343 с.

4. Казеннов В. Безопасность www-сервров / В. Казеннов. – 1999. – 545 с.

5. Ефремов А. Иерархия защиты веб-серверов / А. Ефремов // Экспресс-электроника. – 2004. – № 3. – С. 49.