Рекомендации по противодействию шпионскому программному обеспечению

Пять основных правил, следование которым позволяет успешно противодействовать самой распространенной угрозе информационной безопасности нашего времени - шпионскому программному обеспечению.

1. Установите как антивирусное, так и антишпионское программное обеспечение от признанного разработчика - каждое из них по отдельности может быть не достаточно эффективным против всего существующих спектра угроз.

2. На предприятиях убедитесь, что обновления автоматически загружаются на центральный сервер и проходят тестирование перед установкой на все пользовательские системы. Недавно несколько законных, но содержащих ошибки, обновлений привели к неработоспособности систем, поэтому необходимо тестировать все обновления сигнатур на репрезентативной системе перед запуском их в рабочую эксплуатацию. Розничным потребителям следует настроить автоматическое обновление своих антивирусных и антишпионских программ.

3. Устанавливайте критические пакеты обновлений для ваших операционных систем своевременно. Для розничных потребителей это обычно означает необходимость настройки автоматической установки обновлений системы. На предприятиях необходимо быстро протестировать пакеты обновлений, прежде чем начинать их широкомасштабное развертывание.

4. Установите персональный межсетевой экран и настройте его таким образом, чтобы по максимуму запретить исходящие соединения и получать оповещения при попытках их установления.

5. Убедитесь в том, что у вас под рукой имеются установочные CD-ROM для операционной системы и приложений. Некоторое шпионское программное обеспечение так глубоко заражает систему, что практически единственным способом его удаления, является полная переустановка системы.