Автор: Максим
20.03.2009 17:10 - Обновлено 21.03.2009 08:52

Решения по обеспечению информационной безопасности ЛВС

Современные компании, производственный процесс которых хотя бы в минимальной степени связан с использованием ресурсов Интернет, неизбежно сталкиваются с рядом проблем касающихся безопасности их информационных активов. Требования бизнеса к информационной безопасности ставят перед компаниями важнейшие цели, включающие в себя:

- обеспечение защищенности, достоверности и сохранности информации,
- эффективное противодействие современным угрозам информационной безопасности исходящим как со стороны сети Интернет, так и со стороны сотрудников компании,
- повышение уровня реагирования на появляющиеся информационные угрозы,
- сокращение эксплуатационных расходов и повышение общей эффективности использования сети Интернет сотрудниками компании.

Компания НетПроб предоставляет услуги по подготовке, внедрению и сопровождению комплекса решений обеспечения информационной безопасности корпоративной интранет/экстранет-сети клиента. Предлагаемые решения позволят добиться высокого уровня информационной безопасности локальной вычислительной сети компании-заказчика, повысят степень контроля и управления доступом к ресурсам Интернет для сотрудников компании.

Основные решаемые задачи:

- **Публичный доступ**: обеспечение доступа пользователей Интернет к публичным ресурсам локальной сети компании, размещенным в демилитаризованной зоне (DMZ), таким как WEB / XML -сервисы, почта, корпоративные системы взаимодействия с клиентами, другие информационные сервисы компании. Обеспечение надежной защиты информации и ресурсов компании от возможного влияния со стороны злоумышленников, конкурентов, вредоносного ПО.
- **Безопасный доступ к сети Интернет (фильтрация и контроль доступа)**: обеспечение безопасного контролируемого доступа к ресурсам Интернет со стороны сотрудников компании.
- **Взаимодействия с другими офисами компании посредством корпоративной ВЧС (site-to-site VPN)**: обеспечение защищенного сетевого взаимодействия территориально разделенных офисов клиента через публичные сети.
- **Подключение удаленных/мобильных сотрудников (site-to-client VPN)**: предоставление защищенного контролируемого доступа удаленным сотрудникам компании к внутренним информационным ресурсам ЛВС клиента.
- **Активная защита от сетевых угроз:** обеспечение эффективной защиты внутренних ресурсов ЛВС клиента от угроз исходящих как со стороны сети Интернет, так и со стороны пользователей ЛВС.
- **Антивирусная защита:** защита вычислительных ресурсов ЛВС компании – серверов и рабочих станций сотрудников от вредоносного воздействия вирусов.

Комплекс решений включает в себя следующие функциональные структурные элементы:

- механизмы предотвращения вторжений и защиты сетевого оборудования ЛВС клиента - обеспечивают адекватное противодействие современным угрозам информационной безопасности как со стороны сети Интернет, так и со стороны пользователей ЛВС;
- механизмы анализа и контроля доступа в Интернет - обеспечивают управление и контроль сетевого доступа к ресурсам сети Интернет на уровне отдельных пользователей;
- система антивирусной защиты - для защиты от вредоносного кода ПК

пользователей ЛВС клиента;

- система контроля конфигураций ПК – для обеспечения контроля технической конфигурации ПК в части управления внешними портами, интерфейсами доступа, дисководами ПК;
- механизмы контроля доступа пользователей к ресурсам ЛВС – авторизация пользователей для предоставления доступа к канальной составляющей ЛВС, контроль состояния ПК пользователей (наличие патчей, антивирусов, отстуствие вредоносного кода и пр.)
- подсистема доступа внешних пользователей – для организации безопасного авторизованного доступа пользователей из сети Интернет к информационным ресурсам, расположенным в DMZ ЛВС.