3. Morgan Stanley стал жертвой серьезной утечки данных http://www.securitylab.ru/news/404944.php
4. Хакеры атаковали сайты 40 министерств Южной Кореи http://www.securitylab.ru/news/404990.php
5. Киберпреступники наносят Великобритании ежегодный ущерб 27 млрд фунтов http://www.securitylab.ru/news/404871.php
6. Ярочкин В.И.Информационная безопасность: учебник для вузов.-5-е издание. – М.: Академический проспект, 2008. – 544с.
7. Угрозы информационной безопасности http://itsecblog.ru/ugrozy-informacionnoj-bezopasnosti/

ПОЛИТИКА БЕЗОПАСНОСТИ И ЕЁ АНАЛИЗ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Денис ГАЛЕЦКУЛ,
Приднестровский Государственный Университет имени Т.Г.Шевченко

Локальная вычислительная сеть - компьютерная сеть, покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт). Также существуют локальные сети, узлы которых разнесены географически на расстояния более 12 500 км (космические станции и орбитальные центры). Несмотря на такие расстояния, подобные сети всё равно относят к локальным.

Должны быть поставлены следующие цели при разработке эффективной защиты ЛВС:

- обеспечить конфиденциальность данных в ходе их хранения, обработки или при передаче по ЛВС;
- обеспечить целостность данных в ходе их хранения, обработки или при передаче по ЛВС;
- обеспечить доступность данных, хранимых в ЛВС, а также возможность их своевременной обработки и передачи
- гарантировать идентификацию отправителя и получателя сообщений.

Адекватная защита ЛВС требует соответствующей комбинации политики безопасности, организационных мер защиты, технических средств защиты, обучения и инструктажей пользователей и плана обеспечения непрерывной работы.

Многие организации используют средства ЛВС для обеспечения нужд обработки и передачи данных. ЛВС логически и физически рассредоточена по всей организации.

Службы безопасности, защищающие данные, а также средства по их обработке и передаче, также должны быть распределены по всей ЛВС. Пользователи должны быть уверены в том, что их данные и ЛВС адекватно защищены. Защита ЛВС должна быть интегрирована во всю ЛВС и должна быть важной для всех пользователей.

Распределенное хранение данных обеспечивает пользователей прозрачным доступом к части дисковой памяти удаленного сервера. Распределенное хранение данных предоставляет такие возможности, как удаленную работу с данными и удаленную печать. Удаленная работа с данными позволяет пользователям получать доступ, читать и сохранять данные. В общем случае, удаленная работа с данными обеспечивается путем предоставления пользователям возможности подключения к части удаленного устройства дисковой памяти (файлового сервера, сервера баз данных и других серверов приложений) так, как будто это устройство подключено напрямую. Удаленная печать позволяет пользователю печатать на любом принтере, подключенном к любому компоненту ЛВС.

Проблемы безопасности ЛВС

1. Распределенное хранение данных - проблемы

Файловые серверы могут контролировать доступ пользователей к различным частям файловой системы. Этого обычно осуществляется разрешением пользователю присоединить некоторую файловую систему (или каталог) к рабочей станции пользователя для дальнейшего использования как локальный диск. Это представляет две потенциальные проблемы. Во-первых, сервер может обеспечить защиту доступа только на уровне каталога, поэтому если пользователю разрешен доступ к каталогу, то он получает доступ ко всем файлам, содержащимся в этом каталоге. Чтобы минимизировать риск в этой ситуации, важно соответствующим образом структурировать и управлять файловой системой ЛВС. Следующая проблема заключается в неадекватных механизмах защиты локальной рабочей станции.

2. Удаленные вычисления - проблемы

Удаленные вычисления должны контролироваться таким образом, чтобы только авторизованные пользователи могли получать доступ к удаленным компонентам и приложениям. Серверы должны обладать способностью аутентифицировать удаленных пользователей, запрашивающих услуги или приложения. Эти запросы могут также выдаваться локальными и удаленными серверами для взаимной аутентификации. Невозможность аутентификации может привести к тому, что и неавторизованные пользователи будут иметь доступ к удаленным серверам и приложениям. Должны существовать некоторые гарантии в отношении целостности приложений, используемых многими пользователями через ЛВС.

3. Топологии и протоколы - проблемы

Топологии и протоколы, используемые сегодня, требуют, чтобы сообщения были доступны большому числу узлов при передаче к желаемому назначению. Это гораздо дешевле и легче, чем иметь прямой физический путь между каждой парой машин. (В больших ЛВС прямые связи неосуществимы). Вытеакющие из этого возможные угрозы включают как активный, так и пассивный перехват сообщений, передаваемых в линии. Пассивный перехват включает не только чтение информации, но и анализ трафика (использование адресов, других данных заголовка, длины сообщений, и частоту сообщений). Активный перехват включает изменение потока сообщений (включая модификацию, задержку, дублирование, удаление или неправомочное использование реквизитов).

Прочие проблемы безопасности ЛВС включают:

1) неадекватную политику управления и безопасности ЛВС,
2) отсутствие обучения особенностям использования ЛВС и защиты,
3) неадекватные механизмы защиты для рабочих станций,
4) неадекватную защиту в ходе передачи информации.

Слабая политика безопасности также увеличивает риск, связанный с ЛВС. Должна иметься формальная политика безопасности, которая определяла правила использования ЛВС, для демонстрации позиции управления организацией по отношению к важности защиты имеющихся в ней ценностей. Политика безопасности является сжатой формулировкой позиции высшего руководства по вопросам информационных ценностей, ответственности по их защите и организационным обязательствам. Должна иметься сильная политика безопасности ЛВС для обеспечения руководства и поддержки со стороны верхнего звена управления организацией. Политика должна определять роль, которую имеет каждый служащий при обеспечении того, что ЛВС и передаваемая в ней информация адекватно защищены.

Использование ПК в среде ЛВС также приносит риск в ЛВС. В общем, в ПК практически отсутствует меры защиты в отношении аутентификации пользователей, управления доступом, контроля деятельности пользователей и т.д.

Отсутствие осведомленности пользователей в отношении безопасности ЛВС также увеличивает риск. Пользователи, не знакомые с механизмами защиты, мерами защиты и т.п. могут использовать их неправильно и, возможно, менее безопасно. Ответственность за внедрение механизмов и мер защиты, а также за следование правилам использования ПК в среде ЛВС обычно ложится на пользователей ПК. Пользователям должны быть даны соответствующие инструкции и рекомендации, необходимые, чтобы поддерживать приемлемый уровень защиты в среде ЛВС.

БУДУЩЕЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ирина РОТАРЬ,
Школа им. М. Коцюбинского (Кишинев, Республика Молдова)

Для того чтобы полностью раскрыть тему, давайте разберёмся в терминологии.

Безопасность – это такое состояние сложной системы, когда действие внешних и внутренних факторов не приводит к ухудшению системы или к невозможности её функционирования и развития (Заплатинский В. М. «Терминология науки о безопасности».)

Информация - (от лат. *informatio* — осведомление, разъяснение, изложение, от лат. *informare* — придавать форму) — в широком смысле абстрактное понятие, имеющее множество значений, в зависимости от контекста. В узком смысле этого