ПИНСК В СОВРЕМЕННОЙ БЕЛАРУСИ

Тезисы докладов
научно-практической конференции
молодых ученых Пинщины

Пинск, 21 мая 2004 года

ПИНСК, 2004

Рецензенты:

Нефагина Г.Л. – д. ф. н., профессор
Голубев С.Г. – д. э. н., профессор

Пинск в современной Беларуси: тезисы докладов научно-практической конференции молодых ученых Пинщины, Пинск, 21 мая 2004г.

П.А. Павлов
Пинский филиал Белорусского государственного
экономического университета
г. Пинск

ПРОБЛЕМЫ БЕЗОПАСНОСТИ В ЭЛЕКТРОННОМ БИЗНЕСЕ

Безопасность любой системы электронной коммерции в целом заключается в защите от различного рода вмешательств в ее данные. Все эти вмешательства можно разделить на несколько категорий:

- хищение данных (например, хищение номеров кредитных карточек из базы данных);
- вмешательство (например, перегрузка данными сайта, не предназначенного для такого большого объема информации);
- искажение данных (например, изменение сумм в файлах платежей и счетов-фактур);
- разрушение данных (например, при передаче с сайта или сайту от пользователя);
- отказ от произведенных действий (например, от факта оформления заказа или получения товара);
- неумышленное неправильное использование средств сайта добросовестным пользователем;
- несанкционированный доступ к информации:
- несанкционированное копирование, обновление или другое использование данных;
- несанкционированные транзакции;
- несанкционированный просмотр или передача данных.

При этом нельзя не учитывать, что в вопросах безопасности в данной сфере имеется ряд объективных проблем правового характера - технологии развиваются значительно быстрее законодательной базы, злоумышленника трудно поймать на месте преступления, а доказательства и следы преступлений легко могут быть бесследно уничтожены. Все это обуславливает необходимость тщательной разработки компаниями политики защиты своего электронного бизнеса. Полная и абсолютная безопасность недостижима, так как системы электронного бизнеса построены на базе множества готовых и сделанных на заказ программных приложений различных поставщи-

ков и значительного количества внешних сервисов, предоставляемых провайдерами соответствующих услуг или бизнес-партнерами. Значительная часть этих компонент и сервисов обычно непрозрачны для IT-специалистов компании-заказчика, кроме того, многие из них часто модифицируются и усовершенствуются их создателями. Все это невозможно тщательно проверить на предмет потенциальных дефектов защиты, и еще сложнее все эти дефекты устранить. И даже если бы это было возможно, нельзя исключить так называемый человеческий фактор, так как все системы создаются, изменяются и управляются людьми, а согласно исследованиям Института компьютерной безопасности 81% респондентов отметили, что наибольшее беспокойство у компаний вызывает именно внутренняя угроза - умышленные или неумышленные действия собственных сотрудников.

В проблеме защиты от внутренних угроз есть два аспекта: технический и организационный. Технический аспект заключается в стремлении исключить любую вероятность несанкционированного доступа к информации. Для этого применяются такие известные средства, как:

- поддержка паролей и их регулярное изменение;
- предоставление минимума прав, необходимых для администрирования системы;
- наличие стандартных процедур своевременного изменения группы доступа при кадровых изменениях или немедленного уничтожения доступа по увольнении сотрудника.

Организационный аспект состоит в разработке рациональной политики внутренней защиты, превращающей в рутинные операции такие редко используемые компаниями способы защиты и предотвращения хакерских атак, как:

- введение общей культуры соблюдения безопасности в компании;
- тестирование программного обеспечения на предмет хакинга;
- отслеживание каждой попытки хакинга (не зависимо от того, насколько успешно она завершилась) и ее тщательное исследование;
- ежегодные тренинги для персонала по вопросам безопасности и киберпреступности, включающие информацию о конкретных признаках хакерских атак, чтобы максимально расширить круг сотрудников, имеющих возможность выявить такие действия;
- введение четких процедур отработки случаев неумышленного изменения или разрушения информации.

Для защиты от внешнего вторжения сегодня существует множество систем, по сути являющихся разного рода фильтрами, помогающими выявить попытки хакинга на ранних этапах и по возможности не допустить злоумышленника в систему через внешние сети. К таким средствам относятся:

- **маршрутизаторы** - устройства управления трафиком сети, расположенные между сетями второго порядка и управляющие входящим и исходящим трафиком присоединенных к нему сегментов сети;
- **брандмауэры** - средства изоляции частных сетей от сетей общего пользования, использующих программное обеспечение, отслеживающее и пресекающее внешние атаки на сайт с помощью определенного контроля типов запросов;
- **шлюзы приложений** - средства, с помощью которых администратор сети реализует политику защиты, которой руководствуются маршрутизаторы, осуществляющие пакетную фильтрацию;
- **системы отслеживания вторжений (Intrusion Detection Systems, IDS)** - системы, выявляющие умышленные атаки и неумышленное неправильное использование системных ресурсов пользователями;
- **средства оценки защищенности (специальные сканеры, др.)** - программы, регулярно сканирующие сеть на предмет наличия проблем и тестирующие эффективность реализованной политики безопасности.

В целом, первое, что следует сделать компании - это разобраться, что и от кого должно быть защищено. В качестве основных игроков на этом поле выступают акционеры компании, потребители, сотрудники и бизнес-партнеры, и для каждого из них необходимо разработать собственную схему защиты. Все требования по безопасности должны быть задокументированы, чтобы в дальнейшем служить руководством для всех реализаций электронно-коммерческих приложений и средств их защиты в различных направлениях деятельности компании. Кроме того, это позволит сформировать отдельный бюджет для обслуживания проблем безопасности в рамках компании и оптимизировать расходы на эти нужды, исключив дублирование каких-либо вопросов защиты при разработке каждого отдельного бизнес-проекта.

К сожалению, сегодня практика такова, что политика защиты отдается руководителями на откуп IT-подразделению, сотрудники которого полагают что технологические вопросы важнее каких-то там "бумажных" предписаний, и к тому же, не являются специалистами в отдельных облас-

тях бизнеса, также требующих четких процедур защиты в рамках компании.

Кроме того, при сопряжении различного программного обеспечения могут появиться специфические проблемы, не известные производителям каждого из интегрированных продуктов. Исследование таких взаимодействий должно предварять любые технологические и бюджетные решения. И этому пока также уделяется слишком мало внимания.

СОДЕРЖАНИЕ