ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ОХРАНА ТРУДА. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ.

Автор: Войков Александр
Научный руководитель доктор, конф.: Марталов В. К.

Universitatea Tehnică a Moldovei

Аннотация. *В работе приведены исследования об информационной безопасности, а также об основных способах и методах обеспечения оной.*

Ключевые слова: *информационная безопасность, конфиденциальность, целостность, доступность, DDOS-атаки, вирусы, спам, аутентификация ,авторизация, администрирование, VPN, межсетевой экран, криптографические системы, фильтрация, резервное копирование* **.**

1. Введение

Ни для кого не является секретом, что 21 век – это век информационных технологий. Развитие информационных технологий, их проникновение во все сферы человеческой деятельности приводит к тому, что проблемы информационной безопасности с каждым годом становятся всё более и более актуальными – и одновременно более сложными.

Для работника сферы информационных технологий, понятие безопасность труда включает в себя и понятие информационная безопасность, теперь подробней об этом понятии.

2. Понятие информационной безопасности

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре.

В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т.п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

В качестве стандартной модели безопасности часто приводят модель из трёх категорий:

· Конфиденциальность - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

· Целостность - избежание несанкционированной модификации информации;

· Доступность - избежание временного или постоянного сокрытия информации от пользователей, получивших права доступа.

Выделяют и другие не всегда обязательные категории модели безопасности:

· неотказуемость или апеллируемость - невозможность отказа от авторства;

· подотчётность - обеспечение идентификации субъекта доступа и регистрации его действий;

· достоверность - свойство соответствия предусмотренному поведению или результату;

· аутентичность или подлинность - свойство, гарантирующее, что субъект или ресурс идентичны заявленным.

3. Категории вредоносных действий

Несмотря на разнообразия действий, которые могут нанести вред информационной безопасности их можно разделить на следующие категории:

1. Действия, осуществляемые авторизованными пользователями. В эту категорию попадают: целенаправленная кража или уничтожение данных на рабочей станции или сервере; повреждение данных пользователей в результате неосторожных действий;

2. «Электронные» методы воздействия, осуществляемые хакерами. Под хакерами понимаются люди, занимающиеся компьютерными преступлениями как профессионально (в том числе в рамках

конкурентной борьбы), так и просто из любопытства. К таким методам относятся: несанкционированное проникновение в компьютерные сети; DDOS-атаки.

Целью несанкционированного проникновения извне в сеть предприятия может быть нанесение вреда (уничтожения данных), кража конфиденциальной информации и использование ее в незаконных целях, использование сетевой инфраструктуры для организации атак на узлы третьих фирм, кража средств со счетов и т.п.

Атака типа DOS (сокр. от Denial of Service - «отказ в обслуживании») - это внешняя атака на узлы сети предприятия, отвечающие за ее безопасную и эффективную работу (файловые, почтовые сервера). Злоумышленники организуют массированную отправку пакетов данных на эти узлы, чтобы вызвать их перегрузку и, в итоге, на какое-то время вывести их из строя. Это, как правило, влечет за собой нарушения в бизнес-процессах компании-жертвы, потерю клиентов, ущерб репутации;

3. Компьютерные вирусы. Отдельная категория электронных методов воздействия - это компьютерные вирусы и другие вредоносные программы. Они представляют собой реальную опасность для современного бизнеса, широко использующего компьютерные сети, интернет и электронную почту. Проникновение вируса на узлы корпоративной сети может привести к нарушению их функционирования, потерям рабочего времени, утрате данных, краже конфиденциальной информации и даже прямым хищениям финансовых средств;

4. Спам. Всего за несколько лет спам из незначительного раздражающего фактора превратился в одну из серьезнейших угроз безопасности: электронная почта в последнее время стала главным каналом распространения вредоносных программ; спам отнимает массу времени на просмотр и последующее удаление сообщений, вызывает у сотрудников чувство психологического дискомфорта; как частные лица, так и организации становятся жертвами мошеннических схем, реализуемых спамерами; вместе со спамом нередко удаляется важная корреспонденция, что может привести к потере клиентов, срыву контрактов и другим неприятным последствиям; опасность потери корреспонденции особенно возрастает при использовании черных списков RBL и других «грубых» методов фильтрации спама;

5. «Естественные» угрозы. На информационную безопасность компании могут влиять разнообразные внешние факторы: причиной потери данных может стать неправильное хранение, кража компьютеров и носителей, форс-мажорные обстоятельства и т.д.

4. Методы обеспечения информационной безопасности

Задача обеспечения информационной безопасности должна решаться системно. Это означает, что различные средства защиты (аппаратные, программные, физические, организационные и т.д.) должны применяться одновременно и под централизованным управлением. При этом компоненты системы должны «знать» о существовании друг друга, взаимодействовать и обеспечивать защиту, как от внешних, так и от внутренних угроз.

На сегодняшний день существует большой арсенал методов обеспечения информационной безопасности:

· средства идентификации и аутентификации пользователей (так называемый комплекс 3А);
· средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;
· межсетевые экраны;
· виртуальные частные сети;
· средства контентной фильтрации;
· инструменты проверки целостности содержимого дисков;
· средства антивирусной защиты;
· системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

Каждое из перечисленных средств может быть использовано как самостоятельно, так и в интеграции с другими. Это делает возможным создание систем информационной защиты для сетей любой сложности и конфигурации, не зависящих от используемых платформ.

«Комплекс 3А» включает аутентификацию (или идентификацию), авторизацию и администрирование. Идентификация и авторизация - это ключевые элементы информационной безопасности. При попытке доступа к информационным активам функция идентификации дает ответ на вопрос: «Кто вы?» и «Где вы?» - являетесь ли вы авторизованным пользователем сети. Функция авторизации отвечает за то, к каким ресурсам конкретный пользователь имеет доступ. Функция администрирования заключается в наделении пользователя определенными идентификационными особенностями в рамках данной сети и определении объема допустимых для него действий.

Системы шифрования позволяют минимизировать потери в случае несанкционированного доступа к данным, хранящимся на жестком диске или ином носителе, а также перехвата информации при ее пересылке по электронной почте или передаче по сетевым протоколам. Задача данного средства защиты - обеспечение конфиденциальности. Основные требования, предъявляемые к системам шифрования - высокий уровень криптостойкости и легальность использования на территории России (или других государств).

Межсетевой экран представляет собой систему или комбинацию систем, образующую между двумя или более сетями защитный барьер, предохраняющий от несанкционированного попадания в сеть или выхода из нее пакетов данных.

Основной принцип действия межсетевых экранов - проверка каждого пакета данных на соответствие входящего и исходящего IP-адреса базе разрешенных адресов. Таким образом, межсетевые экраны значительно расширяют возможности сегментирования информационных сетей и контроля за циркуляцией данных.

Говоря о криптографии и межсетевых экранах, следует упомянуть о защищенных виртуальных частных сетях (Virtual Private Network - VPN). Их использование позволяет решить проблемы конфиденциальности и целостности данных при их передаче по открытым коммуникационным каналам. Использование VPN можно свести к решению трех основных задач:

1. защита информационных потоков между различными офисами компании (шифрование информации производится только на выходе во внешнюю сеть);
2. защищенный доступ удаленных пользователей сети к информационным ресурсам компании, как правило, осуществляемый через интернет;
3. защита информационных потоков между отдельными приложениями внутри корпоративных сетей (этот аспект также очень важен, поскольку большинство атак осуществляется из внутренних сетей).

Эффективное средство защиты от потери конфиденциальной информации - фильтрация содержимого входящей и исходящей электронной почты. Проверка самих почтовых сообщений и вложений в них на основе правил, установленных в организации, позволяет также обезопасить компании от ответственности по судебным искам и защитить их сотрудников от спама. Средства контентной фильтрации позволяют проверять файлы всех распространенных форматов, в том числе сжатые и графические. При этом пропускная способность сети практически не меняется.

Современные антивирусные технологии позволяют выявить практически все уже известные вирусные программы через сравнение кода подозрительного файла с образцами, хранящимися в антивирусной базе. Кроме того, разработаны технологии моделирования поведения, позволяющие обнаруживать вновь создаваемые вирусные программы. Обнаруживаемые объекты могут подвергаться лечению, изолироваться (помещаться в карантин) или удаляться.

Фильтры спама значительно уменьшают непроизводительные трудозатраты, связанные с разбором спама, снижают трафик и загрузку серверов, улучшают психологический фон в коллективе и уменьшают риск вовлечения сотрудников компании в мошеннические операции. Кроме того, фильтры спама уменьшают риск заражения новыми вирусами, поскольку сообщения, содержащие вирусы (даже еще не вошедшие в базы антивирусных программ) часто имеют признаки спама и отфильтровываются.

Один из основных методов защиты от потери данных - резервное копирование с четким соблюдением установленных процедур (регулярность, типы носителей, методы хранения копий и т.д.).

4. Заключение

Каждый из этих методов не могут гарантировать абсолютную информационную безопасность, но в совокупности они способны обеспечить достаточный уровень. Конечно, методы и технологии взлома и незаконного проникновения постоянно совершенствуются, но методы и технологии защиты также развиваются. Остается только следить, применять и по возможности содействовать развитию методов обеспечения информационной безопасности.

5. Литература

4. Доронин, А.И. Бизнес-разведка - М.: Ось-89, 2007. - 528 с.
5. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М.: Книжный мир, 2009. - 352 с.
6. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. - М.: ДМК Пресс, 2008. - 544 с.