УДК 330:002
ББК 65.052с51
А 90
М.С. Асланян

Организация политики безопасности в лаборатории кафедры «учета и финансирования»

Аннотация:

В работе описывается организация политики безопасности работы локальной сети Лаборатории «Бухгалтерского учета, анализа и аудита», рассмотрены теоретические основы вопроса, а также принципы и методы их реализации: административные и программно-аппаратные средства.

Ключевые слова:

Политика безопасности, административные меры, политика безопасности.

Под политикой безопасности понимают «формальное изложение правил, которым должны подчиняться лица, получающие доступ к корпоративной технологии и информации». Попытаемся несколько расширить определение. Начнем с того, что эта задача не имеет простого и универсального решения, так как относится к комплексным. Она должна решаться каждый раз индивидуально. Тем не менее, как и любая проблема, она имеет ряд общих черт. Так, реализацию политики безопасности можно подразделить на две большие группы:

- административные меры (собственно, в определении говорится именно о них);
- использование специального оборудования и программного обеспечения.

Административные меры

Защита информации подразумевает использование трех основных критериев: достоверности, конфиденциальности, доступности.

Достоверность означает, что защищаемые данные не претерпели изменений (в результате передачи или умышленного модифицирования) с момента создания до момента их просмотра. Достигается, главным образом, при помощи электронной подписи.

Конфиденциальность – невозможность прочитать данные посторонними, даже если и произошла утечка информации (применение криптозащиты).

Доступность (актуальность) – это возможность получить необходимую информацию в любой необходимый момент со всеми изменениями на этот момент.

Как показывает исторический опыт, основная угроза по преодолению системы защиты заключается в человеческом факторе, то есть возможности получения информации от человека, имеющего доступ к секретной информации, или несоблюдении установленных правил безопасности. При построении системы защиты (СЗ) необходимо, в первую очередь, учесть возможность утечки защищаемой информации или средств к ее доступу со стороны персонала, имеющего доступ к этой информации. Первое решается путем тщательной подборкой кадров, второе – созданием такой системы защиты, при которой один человек не может получить неограниченный доступ к информации, подлежащей сокрытию, или к значительной ее части (вплоть до введения нескольких должностей администраторов с разными правами).

Значение четких правил зачастую недооценивают. Вместе с тем, они являются самым дешевым (почти ничего не надо приобретать) способом защитить свою сеть и доступ к информации. Кроме того, без них использование программно-аппаратных средств защиты просто будет бессмысленным. В итоге мы получим «сейф без задней стенки». Толку от нашей навороченной системы безопасности, если вся ее конфигурация и пароли хранятся в текстовых файлах, а вахтерша баба Глаша имеет физический доступ к любому компьютеру.

Планируя схему обеспечения политики безопасности, необходимо четко определить:

- от кого, от чего и на каком уровне мы собираемся защитить сеть;
- контролируемые объекты и ресурсы;
- рабочие группы пользователей и набор минимально необходимых прав для каждой из них;
- кто будет осуществлять контроль над системой безопасности и что должен будет предпринять в случае сбоев, поломки оборудования и попытки атаковать сеть;
- ответственность каждого сотрудника за нарушение правил безопасности.

Теперь обо всем этом подробнее.

Что защищать

Приступая к созданию СЗ информации необходимо помнить следующее, о чем часто забывают:

- стоимость защиты не должна превышать стоимости защищаемой информации, иначе это экономический садомазохизм;
- стоимость преодоления установленной защиты должна превышать стоимость защищаемой информации.

В противном случае такая защита не спасет, или затраты времени будут столь велики, что при успешном преодолении СЗ, полученная информация потеряет свою ценность. Немалую роль играет и отсутствие физического доступа к серверам – если у вас украдут винчестер, то все ваши жертвы во имя информационной безопасности никому не будут нужны.

Этот пункт зависит также и от деятельности лаборатории и наличия квалифицированного персонала, который сможет в дальнейшем поддерживать в рабочем состоянии все установленное программно-аппаратное обеспечение. Помните, чем сложнее СЗ, тем больше ресурсов

(людей, времени, денег) она требует для своего обслуживания.

Контролируемые объекты и ресурсы

Необходимо четко понимать, что степень защиты всей системы равна защищенности ее самого уязвимого участка. Полноценный анализ надежности системы безопасности и наличия наиболее уязвимых мест станет одной из основ всей политики.

Нужно помнить – чем меньше надо контролировать ресурсов, тем более эффективно это можно сделать, поэтому отключаем неиспользуемые протоколы и порты; все то программное обеспечение, которое не нужно для работы, должно быть безжалостно удалено. Помочь в этом вопросе могут специальные утилиты, которые определяют наличие различных дыр.

Рабочие группы пользователей

Лучше всего изначально все запретить всем группам пользователей. Причем, не отключить разрешение, а именно запретить как правило с наивысшим приоритетом. Позже, в процессе работы можно будет разрешить минимальные, необходимые для выполнения своих обязанностей действия, организовав при этом работу через SQL-запросы. Такая тактика называется «режим обучения» и используется для настройки файрволлов, фильтров трафика. Чем меньший доступ к информации можно получить через конкретную учетную запись, тем труднее составить целостное представление о характере и формате хранения данных в случае несанкционированного доступа через нее. Ограничение временными рамками, например, только рабочие часы, работы в системе уменьшает риск проникновения в защищаемую зону системы, так как в часы отсутствия контролирующего персонала действуют наиболее жесткие правила доступа. Желательно применять физические ключи (или биофизические параметры в качестве таковых) для доступа к сети. Пароли очень часто записывают на чем попало, набирают в присутствии посторонних (еще и проговаривая их вслух), что приводит к большой вероятности их рассекречивания. Очень полезно бывает отключение доступа при длительном отсутствии активности со стороны прошедшего идентификацию пользователя.

Анализ аудита действий пользователя поможет выявить нехарактерные действия последнего, если учетной записью воспользовался другой человек.

Ответственность сотрудников

Представьте: мы написали идеальные правила, каждого снабдили набором четких инструкций, установили лучшее программное обеспечение и аппаратные средства защиты… все? Отнюдь! Ничто не мешает любому из наших служащих начхать на нововведения и продолжать делать глупости. А значит, именно так они и будут поступать… до тех пор, пока не будет введена персональная ответственность сотрудников за невыполнение установленных правил. Времена публичных выговоров прошли, сейчас самая действенная мера – денежные взыскания. Может быть, потому, что числа люди воспринимают лучше, чем бранные слова.

Некоторые замечания по поводу политики

Для эффективности политика должна быть наглядной. Наглядность помогает реализовать политику, помогая гарантировать ее знание и понимание всеми сотрудниками организации. Презентации, видеофильмы, семинары, вечера вопросов и ответов и статьи во внутренних изданиях организации увеличивают ее наглядность. Программа обучения в области компьютерной безопасности и контрольные проверки действий в тех или иных ситуациях могут достаточно эффективно уведомить всех пользователей о новой политике. С ней также нужно знакомить всех новых сотрудников организации.

Для того чтобы быть эффективной, политика должна быть согласована с другими существующими директивами, законами, приказами и общими задачами организации. Одним из способов координации политик является согласование их с другими отделами в ходе разработки.

Претворение политики в жизнь

Обращаясь к вышесказанному можно привести пример применения политики безопасности в лаборатории кафедры «Учета и финансирования».

Итак, у нас в наличии имеется лаборатория, оснащенная 13 локальными машинами и сервером, соединенных внутренней сетью, подключенных к единой внешней сети АГУ и к «всемирной паутине» (Интернет). Лаборатория является структурным подразделением экономического факультета.

Главная особенность состоит в том, что в лаборатории в дневное время занимаются студенты очного отделения, а в вечернее время студентам, преподавателям и аспирантам очного и заочного отделения экономического факультета предоставляется бесплатный доступ к Интернет ресурсам. Другими словами мы имеем разнородные группы пользователей с различными правами. Сложность заключается в том, что необходимо защитить доступ к информации от внутреннего и внешнего несанкционированного доступа.

Внутренний условно можно разделить:

- пользователи (студенты, аспиранты, преподаватели);
- сотрудники, не имеющие соответствующих прав;
- другие посторонние лица.

Данная проблема решается путем установления соответствующего программного обеспечения и дополнительных утилит. На мой взгляд, наиболее удобным, практичным и выгодным является внедрение двух наиболее совместимых продуктов в области администрирования:

Gameclass – один из лидеров среди программ для контроля и управления организацией (лабораторией). Внедрение комплекса позволяет автоматизировать работу организации (лаборатории) и увеличить качество защиты всей системы, благодаря высокой степени контроля, точному учёту предоставляемых услуг и подробной финансовой и аналитической отчетности.

Runpad Shell признан лучшим автономным шеллом для использования в организациях (лабораториях). Внедрение системы позволяет защитить рабочие места от нежелательных действий пользователей, облегчить работу администраторов, благодаря высокой степени защиты и приятному пользовательскому интерфейсу.

GameClass и Runpad Shell специально адаптированы для совместной работы – программы избавлены от каких-либо конфликтов друг с другом.

Внешний в свою очередь разделяется:

- Интернет нарушители;

• вирусы, Трояны, спам и прочих вредоносных программы;

• ограничение доступа к посторонним Интернет ресурсам;

• другие виды внешних вторжений.

Решение вышесказанных проблем также осуществляется с помощью необходимого программного обеспечения и дополнительных утилит:

Прокси-сервер UserGate 4.0 – программа для подключения локальных пользователей к сети Интернет через один внешний IP-адрес. Прокси-сервер ведет точный учет трафика (NAT), имеет встроенный межсетевой экран (firewall), port mapping, систему Интернет-статистики и антивирус Касперского.

Прокси-сервер UserGate обладает интуитивно понятным интерфейсом, прост в настройке и использовании. Не обязательно обладать знаниями системного инженера, чтобы разобраться и работать с данным продуктом.

Антивирусные программы семейства Dr.Web® выполняют поиск и удаление известных компьютерных вирусов из памяти и с жестких дисков компьютера. Кроме того, используя уникальную технологию определения вирусоподобных ситуаций, они способны с высочайшей степенью вероятности обнаруживать ранее неизвестные компьютерные вирусы.

Использование антивирусных программ семейства Dr.Web® дает мощную, компактную и быстродействующую систему защиты от компьютерных вирусов, построенную на самых современных технологиях.

В совокупности все вышеперечисленные меры, программное обеспечение и дополнительные утилиты позволили:

• защитить всю информацию с соблюдением трех критериев (достоверности, конфиденциальности, доступности);

• запретить доступ к важным данным, которой могут случайно или преднамеренно повредить, что вызовет сбой на отдельной машине или системы в целом;

• запретить физическое вмешательство лиц, не имеющих на то право;

• запретить пользование Интернет ресурсам во время занятий, а при необходимости разрешить, ограничив временные рамки;

• учитывать, регистрировать и полностью контролировать все группы пользователей;

• создать модульный принцип построения системы защиты;

• максимально автоматизировать все процессы внутри системы;

• создать условия, при которых стоимость защиты будет превышать стоимость защищаемой информации.

Выводы:

Обеспечение информационной безопасности организации (лаборатории) – крайне нелегкая задача. Даже базируясь на готовых решениях, она требует постоянного внимания к себе, а использование передовых технологий еще не означает автоматически высочайшей надежности. В любой организации (лаборатории) пока еще работают люди, а раз так, в первую очередь внимание следует уделить человеческому фактору. Только реализовав в полной мере необходимый вклад в защиту на каждом вышеперечисленном этапе, подчинив правила единой концепции комплексной системы защиты, можно уверенно чувствовать себя и знать, что вашей информации ничего не угрожает. Почти ничего.

Примечания:

1. Васильков А. «Политика безопасности LAN»/ А. Васильков, [Электронный ресурс] // Политика безопасности LAN. – Режим доступа: http://www.computerra.ru/offline/2002/444/17909/.
2. Медведовский И.Д. Атака через Интернет: учебное пособие / И.Д. Медведовский, П.В. Семьянов, В.В. Платонов, под научной редакцией проф. П. Д. Зегжды/ – НПО «Мир и семья-95», 1997.
3. Бирюков, П.Н. Международное право: учеб. пособие / П.Н. Бирюков. – 2-е изд., перераб. и доп. – М.: Юристъ, 2000. – 416 с.
4. Гутман Б. «Политика безопаснотси при работе в Интернете: техническое руководство»/ Б. Гутман, Р. Бэгвилл, перевод В. Казеннова [Электронный ресурс] // Политика безопаснотси при работе в Интернете: техническое руководство. – Режим доступа: http://www.citforum.ru/internet/security_guide/index.shtml.