ПОЛИТИКА БЕЗОПАСНОСТИ: РАЗРАБОТКА И РЕАЛИЗАЦИЯ

Шония Отар, Цомая Нино
Грузинский Технический Университет

Резюме

Рассматривается процесс разработки и реализации политики безопасности. Выявляются фундаментальные принципы построения и управления политикой безопасности, её детальное содержание, определяется процесс обеспечение безопасности компьютерной информации, также рассматривается процесс подключение к глобальной с точки зрения обеспечения безопасности информации. В конце статьи рассматривается оценка информационной безопасности, т.е. аудит безопасности после разработки и выполнения политики безопасности.

Ключевые слова: информационная безопасность, комплексная безопасность, политика безопасности, аудит информационных процессов, аудит безопасности.

1. Введение

Обеспечение комплексной безопасности является необходимым условием функционирования любой компании. Эта «комплексность» заключается, прежде всего, в продуманности, сбалансированности защиты, разработке четких организационно-технических мер и обеспечении контроля над их исполнением.

Вначале необходимо провести аудит информационных процессов компании, выявить критически важную информацию, которую необходимо защищать. Иногда к решению задачи подходят однобоко, полагая, что защита заключается в обеспечении конфиденциальности информации. При этом упускается из виду необходимость обеспечения защиты информации от подделки, модификации, парирования угроз нарушения работоспособности системы. Аудит информационных процессов должен заканчиваться определением перечня конфиденциальной информации предприятия, участков, где эта информация обращается, допущенных к ней лиц, а также последствий утраты (искажения) этой информации.

После реализации этого этапа становится ясно, что защищать, где защищать и от кого: ведь в подавляющем большинстве инцидентов в качестве нарушителей будут выступать — вольно или невольно — сами сотрудники компании. И с этим ничего нельзя поделать: придется принять как данность. Различным угрозам безопасности можно присвоить значение вероятности их реализации. Умножив вероятность реализации угрозы на причиняемый этой реализацией ущерб, получим риск угрозы. После этого следует приступать к разработке политики безопасности.

2. Основная часть

Фундаментальные принципы построения и управления политикой безопасности представлены на рисунке 1.

На схеме показан принцип построения политики безопасности. «Как в строительстве» если убрать нижние «кирпичи», или «фундамент» то все что выше развалиться. Пустым «кирпичом» обозначена систем резервного копирования системы, без которой даже не может употребляться фраза «безопасность информационной системы».

Политика безопасности представляет с собой документ «верхнего» уровня, в котором должны быть указаны:

- лица, ответственные за безопасность функционирования компании;
- полномочия и ответственность отделов и служб в отношении безопасности;
- организация допуска новых сотрудников и их увольнения;
- правила разграничения доступа сотрудников к информационным ресурсам;
- организация пропускного режима, регистрации сотрудников и посетителей;
- использование программно-технических средств защиты;
- другие требования общего характера.

Рис.1. Принципы построения системы безопасности

Таким образом, политика безопасности — это организационно-правовой и технический документ одновременно. При его составлении надо всегда опираться на принцип разумной достаточности и не терять здравого смысла.

Этот принцип означает, что затраты на обеспечение безопасности информации должны быть не больше, чем величина потенциального ущерба от ее утраты. Анализ рисков, проведенный на этапе аудита, позволяет ранжировать их по величине и защищать в первую очередь не только наиболее уязвимые, но и обрабатывающие наиболее ценную информацию участки. Если в качестве ограничений выступает суммарный бюджет системы обеспечения безопасности, то задачу распределения этого ресурса можно поставить и решить как условную задачу динамического программирования.

Особое внимание в политике безопасности следует уделить разграничению зоны ответственности между службой безопасности и IT-службой предприятия. Зачастую сотрудники службы безопасности, в силу низкой технической грамотности, не осознают важности защиты компьютерной информации. С другой стороны, IT-сотрудники, являясь «творческими» личностями, как правило, стараются игнорировать требования службы безопасности. Кардинально решить эту проблему можно было бы, введя должность CEO (англ. Chief Executive Officer — высшее должностное лицо компании, т.е. генеральный директор, председатель правления, руководитель) по информационной безопасности. Ему подчинялись бы обе службы.

В политике безопасности не стоит детализировать должностные обязанности сотрудников (хотя приходилось видеть и такое). Они должны разрабатываться на основе политики, но не внутри нее.

Серьезное внимание в политике безопасности уделяется вопросам обеспечения безопасности информации при ее обработке в автоматизированных системах: автономно работающих компьютерах и локальных сетях. Необходимо установить, как должны быть защищены серверы, маршрутизаторы и другие устройства сети, определить порядок использования сменных носителей информации, их маркировки, хранения, порядок внесения изменений в программное обеспечение.

Общими рекомендациями по этому поводу являются:

- в системе должен быть администратор безопасности;
- должен быть назначен ответственный за эксплуатацию каждого устройства;

- системный блок компьютера надо защищать печатями ответственного и работника IT-службы (или службы безопасности);
- жесткие диски лучше использовать съемные, а по окончании рабочего дня убирать их в сейф;
- если нет необходимости в эксплуатации CD-ROM, дисководов, они должны быть сняты с компьютеров;
- установка любого программного обеспечения должна производиться только работником IT-службы;
- для разграничения доступа сотрудников лучше всего использовать сочетание паролей и смарт-карт (токенов). Пароли генерируются администратором безопасности, выдаются пользователю под роспись и хранятся им также как и другая конфиденциальная информация;
- следует запретить использование неучтенных носителей информации. На учтенных носителях выполняется маркировка, например, гриф, номер, должность и фамилия сотрудника.

Безусловно, внедрение любой защиты приводит к определенным неудобствам пользователя. Однако эти неудобства не должны быть существенными, иначе человек станет игнорировать правила.

Крайне внимательно следует отнестись к подключению своих информационных ресурсов к Интернету. В политике безопасности этот вопрос предлагается выделить в отдельный раздел. Подключение к Глобальной сети обычно преследует следующие цели:

- получение информации;
- размещение своей информации о предоставляемых услугах, продаваемых товарах и т.д.
- организация совместной работы удаленных офисов или работников на дому.

В двух первых случаях идеальным с точки зрения безопасности было бы использование для работы во Всемирной паутине автономного компьютера, на котором ни в коем случае не должна храниться конфиденциальная информация. На нем обязательно устанавливаются антивирусные средства защиты с актуальной базой, а также правильно настроенный Firewall. При этом особый контроль стоит уделить работе на этом компьютере со сменными носителями информации, а также перлюстрации исходящей почты.

При необходимости организации распределенной работы сотрудников компании наиболее приемлемым решением считаются виртуальные частные сети (VPN). В настоящее время известно множество фирм-разработчиков, представляющих услуги по установке и настройке соответствующего программного обеспечения.

Несмотря на все принятые меры, нарушения информационной безопасности могут иметь место. В политике безопасности следует обязательно предусмотреть меры ликвидации этих последствий, восстановления нормальной работоспособности компании, минимизации причиненного ущерба. Большое значение здесь имеет применение средств резервирования электропитания, вычислительных средств, данных, а также правильная организация документооборота.

3. Заключение

Разработав и воплотилив в жизнь политику безопасности необходимо оценить информационную безопасность, т.е. провести аудит безопасности. Известны два подхода к оценке информационной безопасности на предприятии:

Первый — оценка безопасности на качественном уровне. Эксперт высказывает свое видение состояния дел в компании, дает рекомендации по устранению замеченных им изъянов. Недостаток такого подхода — его субъективизм. Хотелось бы иметь действительно независимую, объективную оценку информационной безопасности. Причем было бы неплохо, чтобы эту, количественную, оценку признавали и другие компании — ваши потенциальные

партнеры. Очевидно, что для этого необходима разработка некоторого набора правил или стандарта в области безопасности информационных систем.

К счастью, почти ничего создавать не надо: стандарт, позволяющий дать количественную оценку информационной безопасности, уже имеется. Речь идет о международном стандарте ISO 17799. Этот документ был принят международным институтом стандартов в конце 2002 года на основе ранее разработанного Великобританией стандарта BS7799.

Стандарт ISO 17799 позволяет получить количественную оценку комплексной безопасности компании. Этот процесс настолько формализован, что существует программное обеспечение, позволяющее самостоятельно выполнить оценку безопасности своей компании. Это программное обеспечение представляет собой, по существу, вопросник. Сгенерированный программой отчет отправляется в адрес компании, имеющей полномочия на проведение сертификации на соответствие этому стандарту, и та присылает вам соответствующий знак и процент соответствия стандарту.

Литература:

1. Волокин А.В., Маношкин А.П. Информационная безопасность государственных организаций и коммерческих фирм. Справочное бюро. Ст-Петербург, 2002

2. Царегородцев А.В. Информационная безопасность в распределённых управляющих системах: Монография. Ст-Петербург, 2003

3. ჩოგოვაძე გ., გოგიჩაიშვილი გ., სურგულაძე გ., შეროზია თ., შონია ო. მართვის ავტომატიზებული სისტემების დაპროექტება და აგება. სტუ. თბ., 2001

4. Морозов Н.П., Чернокнижиций С.Б. Защита деловой информации для Всех. М., 2003

5. Галицкий А.В., Рябко С.Д., Шангин В.Ф. Защита информации в сети. Анализ технологий и синтез решений. М., 2004

6. შონია ო., შეროზია თ., შონია დ., ცომაია ნ. ინფორმაციული სისტემების უსაფრთხოება. სტუ, შრ.კრ. მართვის ავტომატიზებული სისტემები" №1(2), 2007

7. Шетков А.Ю. Защита компьютерной информации от несанкционированного доступа. М., 2004.

POLICY OF SAFETY: PROCESSING AND REALIZATION

Shonia Otar, Tsomaia Nino
Georgian Technical University

Summary

The article discusses the development and implementation of security policy, reveals the fundamental principle construction and management of security policy, its detailed content, determined by the process of ensuring security of computer information, considers the process of connection to the global in terms of information security. At the end of the article the evolution of information security is addressed, i.e. security audit after the development and implementation of security polices.

უსაფრთხოების პოლიტიკა: შემუშავება და რეალიზაცია

ოთარ შონია, ნინო ცომაია
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

განხილულია უსაფრთხოების პოლიტიკის შემუშავებისა და რეალიზაციის პროცესი. გამოვლენილია ფუნდამენტური პრინციპების აგება და პოლიტიკური უსაფრთხოების მართვა, მისი დეტალური შემადგენლობა, განისაზღვრება კომპიუტერული ინფორმაციის უსაფრთხოების უზრუნველყოფის პროცესი, ასევე განიხილება შეერთების გლობალური პროცესი ინფორმაციის უსაფრთხოების უზრუნველყოფის თვალსაზრისით. სტატიის ბოლოს წარმოდგენილია ინფორმაციული უსაფრთხოების შეფასება, ეგრეთწოდებული უსაფრთხოების აუდიტი, პოლიტიკური უსაფრთხოების დამუშავებისა და გამოყენების შემდეგ.