АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ - МАТРИЧНЫЙ ПОДХОД

Авторы: Sanjay Goel, Vicki Chen

Перевод: С.С. Химка

Источник: http://www.docstoc.com/.

В данной работе представлена методология анализа рисков информационной безопасности, которая связывает активы, уязвимость, угрозы и средства управления организации. Подход использует последовательность матриц, которые связывают различные элементы в анализе риска. Данные соединены с использованием матриц, чтобы связать активы со средствами управления таким образом, чтобы было получено расположенное по приоритетам ранжирование средств управления, основанное на активах организации,. Подход не запутывает промежуточные данные в процессе анализа, таким образом обеспечивается прозрачность процесса анализа риска и есть возможность модернизации данных. Этот подход позволяет организациям начинать анализ с малого количества данных с низкой надежностью, и постепенно совершенствовать его (дополнять у улучшать качества), используя данные собраны в течение долгого времени. Представлено типовое статистическое исследование, примененное в NY State agency. Эта методология также была применена в General Electric, и некоторых предварительные результаты этого исследования представлено данной статье.

ВВЕДЕНИЕ

Компьютерные сети и Интернет позволили увеличить производительность как в государственных структурах, так и в частных

организациях. Использование электронной почты и мгновенных сообщений выросло экспоненциально на протяжении нескольких лет и становится предпочтительным способом общения. Несмотря на взлеты и падения, Интернет продолжает вносит изменения в способы потребления в магазинах и в бизнес-модели компаний. Например, альтернативная модель распространения музыки через Интернет изменила музыкальную индустрию, а также способствовала развитию новых форматов, способов оцифровки и сжатия музыкальных файлов.

Несмотря на то, что влияние Интернет на электронную коммерцию, коммуникаций, и распространение информация очевидно, наибольший вклад компьютерные сети внесли в перестройку бизнес-процессов. Большинство рутинных корпоративных функций, в настоящее время выполняется с помощью автоматизированных процессов, связанных с базами данных. Сетевые информационные системы составляют основу предприятия и используются практически во всех сферах бизнеса, включая: выплату заработной платы, закупки, управление человеческими ресурсами, анализа и проектирования инженерных решений. Информационные системы значительно улучшили производительность предприятий. Тем не менее, полная зависимость информационных систем от критических операций сделала предприятий подверженными атакам из сети. Поскольку зависимость экономики от информационных систем возрастает, финансовые потери от нарушения информационной безопасности также увеличиваются. Этот риск финансовых потерь в связи с нарушением информационной безопасности является причиной для беспокойства и корпорации, и правительства. У большинства организаций не существует полной картины состояния своей информационной безопасности и рисков. Как правило, специальные решения относительно безопасности основаны на реализации руководящих принципов и документов, выданных государственными учреждениями или сторонними организациями. Информационные отделы могут поддерживать существующий уровень безопасности в проверке, но предприятию очень сложно иметь четкую картину состояния своей информационной

безопасности без формального анализа рисков. Персонал информационных отделов может быть компетентными в методах реализации средств безопасности, но ему зачастую не хватает опыта в финансовом моделировании и анализе рисков. Методология формального анализа рисков хорошо изучена в некоторых областях науки (финансы, инженерия, авиация и д.р.). Тем не менее, в информационной безопасности эта дисциплина только зарождается. Одной из проблем, связанной с анализом рисков информационной безопасности, является отсутствие стандартизированных показателей и методов для оценки измерения воздействия угроз и оценки в интересах контроля и острой нехваткой статистических данных для оценки рисков. Еще одной проблемой является низкое качество данных о факторах риска и уязвимостях. Это вызвано тем, что организации опасаются разглашения инцидентов нарушения информационной безопасности, потому что это может привлечь новых хакеров. Наконец, процесс анализа информационных рисков очень слабо освещен в руководящих документах, является дорогостоящим и требует глубокого изучения внутренней структуры организации. Поэтому большинство организаций зачастую ограничивается внешней оценкой рисков и проводить такие оценки периодически (ежегодно или два раза в год), а не непрерывно. Кроме того, у организации нет возможности определить качество сделанной оценки, и они вынуждены полагаться на выводы, сделанные сторонними консультантами.

В данной статье приводится методика оценки рисков, которые могут быть использованы внутри организации. Ее можно применять, используя небольшой набор данных, а также постепенно улучшать и совершенствовать анализ, используя большее количество информации. Она также позволяет организациям выполнять качественный анализ информационной безопасности в общем, а затем проводить более подробный анализ критических подмножеств.

ЛИТЕРАТУРА

Анализ рисков информационный безопасности исследовался аудиторскими фирмами (Cerullo & Cerullo, 1994) в течение долгого времени. Аудиторы обычно используют контрольные списки, чтобы проверить, уместность различных элементов безопасности и принимают свои решения, основываясь на этих контрольных списках. Баскервиль (1993) исследовал анализ рисков информационной безопасности с середины 1980-ых. Он определил контрольные списки анализа рисков для инструментов, используемых для проектирования мер безопасности для информационных систем. Паркер (1981) и Фишер (1984) использовали анализ риска как фундаментальное основание для проекта безопасности в информационных системах. Они обеспечивают обширные контрольные списки, рассматриваемые при оценке безопасности. Проблема с определенными инструментами и контрольными списками состоит в том, что они быстро становятся устаревшими и должны постоянно обновляться. Разработка таких инструментов не приводят к продвижению научных знаний для проекта информационного безопасности. Бэкхаус и Диллон (1996) попытались создать логическую модель, представив информационную безопасность как структуру ответственности и обязанности, а не стандартных контрольных списков. Андерсон, Лонли и Квок (1994) предлагают модель, основанную на идентификации и оценке угроз, происходящих от эксплуатационной окружающей среды и систем, с которыми сталкиваются активы при защите. Сах и Хан (2003) представляют подход для анализа рисков информационной безопасности, который включает в себя непрерывность эксплуатации. Они определяют ценность активов, основываясь на важности деловых функций и критичности активов к операциям. В анализе используются несколько методологий: соединенное сравнение, таблицы назначения функций актива и диаграммы зависимости актива. Другие модели для проекта информационной безопасности дополнительно сосредотачиваются на идентификации и оценке уязвимости системы и спецификации контрмер (Weiss, 1991).

Были сделаны различные попытки развить сложные инструменты для анализа риска информационной безопасности. CRAMM (Barber & Davey,

1992) является основополагающим инструментом оценки степени риска. Основноя положение, положенное в основу подхода - то, что риск зависит от стоимости активов, от угроз и уязвимостей. Данные для CRAMM получены в результате интервью с владельцами активов, пользователями системы и другим штатом технической поддержки. CORAS (Stolen, 2002) использует комбинацию языка моделирования UML и Unified Process (UP) для поддержки, основанной на модели оценки степени риска на критических по отношению к безопасности системах. Это объединяет несколько существующих методологий, таких как анализ дерева ошибок (Fault Tree Analysis), способ отказа (Failure Mode), анализ критичности эффекта (Effect Criticality Analysis) и анализ Маркова (Markov analysis) в единую платформу для того, чтобы облегчить анализ рисков. OCTAVE (Альбертс и Дорофи, 2003) является более новым инструментом анализа рисков, разработанным в институте разработки программного обеспечения Карнеги Меллона (Carnegie Mellon Software Engineering Institute). Он обеспечивает обширный набор рабочих листов и контрольных списков для того, чтобы осуществить информационную безопасность.

МЕТОДОЛОГИЯ

Данная методология связывает активы, уязвимости, угрозы и средства управления организацией и определяет важность различных средств управления, соответствующими активами организация Активы организации определены как вещи, имеющие значение. Активы могут быть материальными, такие как данные и сети и нематериальными, такие как репутация и доверие.

Уязвимость - слабости в информационном активе, которые могут использоваться угрозами, такими как база данных или веб-сервер. Угрозы - потенциальные причины нежелательных событий, которые могут привести к нанесению ущерба активам организации. Угрозы могут быть случайными или злонамеренными. Средства управления определены как меры, которые

организация может принять, чтобы минимизировать воздействие угроз на один или более активов организации.

Методология, предложенная в данной статье, использует три отдельных матрицы: матрицу уязвимостей, матрицу угроз и матрицу контроля, чтобы собрать данные, которые требуются для анализа риска.

Матрица уязвимости (таблица 1) содержит связь между активами и уязвимостями в организациях, матрица угроз (таблица 2) так же содержит отношения между уязвимостями и угрозами, а матрица контроля (таблица 3) содержат связи между угрозами и средствами управления. Значение в каждой ячейке показывает ценность отношения между элементом строки и столбца таблицы (например, активом и уязвимостью). Использует одна из трех оценок ценности: низкая, средняя или высокая.

При первоначальном анализе риска формируются списки активов, уязвимостей, угроз, и средств управления и добавляются к соответствующим таблицам. Матрицы заполняются путем добавления данных о связи элемента столбца матрица с элементом строки. Наконец, данные из матрицы уязвимости преобразуются с помощью формулы (1), а затем заносятся в таблицу 2. Таким же образом данные из матрицы угроз преобразуются с помощью формулы (2) и заносятся в таблицу. В результате формируется матрица контроля, которая содержит относительную важность различных средств управления.

Таблица 1 - Матрица активов (связь между активами и уязвимостью)

Шкала 0 – нет воздействия 1 - слабое воздействие 3 - умеренное воздействие 9 - сильное воздействие **Уязвимость**	**Активы и Затраты**	Торговые секреты	Конфиденциальная информация	Репутация (доверие)	Потерянный доход	Затраты на восстановление	Информация	Аппаратные средства	Программное обеспечение	Обслуживание	Коммуникации

Веб-сервер											
Вычислительный сервер											
Брандмауэр											
Маршрутизатор											
Клиентские узлы											
Базы данных											

Пусть есть m активов, относительная стоимость актива $a_j \in C_j$ $(j = 1, n)$. Также пусть c_{ij} это воздействие уязвимости v_i на актив a_j. Тогда совокупное воздействие уязвимости v_i на активы организации вычисляется по формуле:

$$V_i = \sum_{j=1}^{n} v_{ij} \cdot C_j \quad (1)$$

Таблица 2 - Матрица активов (связь между угрозами и уязвимостями)

Шкала 0 – нет воздействия 1 - слабое воздействие 3 - умеренное воздействие 9 - сильное воздействие **Средства контроля**	**Угроза**	Отказ в обслуживании (DoS)	Вредоносный код	Ошибки пользователя	Внутренние атаки	Спам	Физическое повреждение аппаратных
Вредоносный код							
Ошибки пользователя							
Внутренние атаки							
Спам							
Физическое повреждение аппаратных средств							

Пусть имеется p угроз, которые действуют на уязвимостей и d_{ki} - потенциал повреждения от угрозы t_k уязвимости v_i . Тогда относительное

совокупное воздействие угрозы T_k:

$$T_k = \sum_{i=1}^{m} d_{ki} \cdot V_i \quad (2)$$

Таблица 3 - Матрица угроз (связь между средствами управления и угрозами)

Шкала 0 – нет воздействия 1 - слабое воздействие 3 - умеренное воздействие 9 - сильное воздействие **Средства контроля**	**Угроза**	Отказ в обслуживании (DoS)	Вредоносный код	Ошибки пользователя	Внутренние атаки	Спам	Физическое повреждение аппаратных
Брандмауэр							
Система обнаружения вторжений (IDS)							
Обучение персонала							
DMZ							
Политика безопасности							
Конфигурация архитектуры сети							

Пусть есть q средств управления, которые могут смягчить p угроз, а e_{lk} - воздействие средства контроля z_0 на угрозу t_k. Тогда относительное совокупное воздействие средств контроля Z_0

$$Z_0 = \sum_{l=1}^{p} e_{0l} \cdot T_l \quad (2)$$

ПРИМЕР ИСПОЛЬЗОВАНИЯ МЕТОДОЛОГИИ

Исследование анализа риска по предложенной методологии проводилось в организации General Electric Energy. Она имеет

фрагментированную организационную структуру, работает в нескольких странах, включая Испанию, Германию, США, Данию и Китай. Процессы и операции очень неоднородны. Кроме того, технические отделы не имеют общей сети. Информационная безопасность очень важна в данной организации.

Однородная информационная инфраструктура необходима для защиты новых технологий, данных о доходах, а также для улучшения коммуникации и увеличения производительности. Она соединяет связанные бизнес-процессы в единый монолитный процесс. Для того чтобы с самого начала запланировать систему безопасности в организации проводился анализ информационных рисков по предложенной методологии. Это исследование представляет собой всесторонний анализ рисков собственных активов, уязвимостей и угроз, порожденных бизнес-процессами. Три матрицы, которые связывают активы с уязвимостями, угрозами и средствами управления в организациях, представлены в таблицах 4, 5 и 6 соответственно.

Таблица 4 представляет собой матрицу уязвимостей , которая связывает уязвимость системы с воздействиями/активами организации. Для построения матрицы была вычислена относительная важность активов/воздействий. Например, успешность бизнеса зависит от его способности развить и защитить новые технологии; поэтому, они высоко оценивается. Основываясь на активах, была определена ключевая уязвимость, связанная с каждым активом/воздействием, и воздействие уязвимости на активах/воздействиях было добавлено к таблице.

Таблица 4 - Матрица уязвимостей для General Electric Energy

Ранжирование приоритета 1 и 2 не важный 3 важный, но не ключевой 4 важный, но находящийся под воздействием ключевого 5 Ключевой	**Активы/Воздействия**	Контроль информации о экспорте	Репутация (Доверие)	IP контроль/управление	Конфиденциальные данные Клиентов	Потерянные Продажи/Доход	Информационная Целостность	Доступность сервисов	Коммуникации	Очистка затрат на старую и новую систему	Старые и новые программыне средства	Старые и новые аппаратных средств	Всего	Разряд (Выше более существенный)
Уязвимости, приоритет ->		11	10	9	8	7	6	5	4	3	2	1		
Брандмауэр	5	9	9	9	9	3	9	3	9	3	9	9	504	13
Передача данных	5	9	9	9	3	3	9	9	9	9	9	3	498	12
База данных	4	9	3	9	9	9	9	3	3	9	9	3	474	11
Архитектура приложений	4	9	9	9	3	3	3	3	1	9	9	9	406	10
Физическая безопасность	3	9	3	3	9	9	3	3	3	9	1	9	374	9
Ошибки конфигурации серверов интернет	2	9	1	9	9	1	3	9	3	3	9	1	372	8
Ошибки конфигурации серверов экстранет	4	1	9	9	9	1	3	9	3	3	9	1	364	7
Устойчивость паролей	3	9	9	3	9	1	3	1	3	1	9	1	352	6
Клиентские узлы (ПК и ноутбуки)	3	9	3	9	9	1	3	3	1	3	3	9	350	5
Аппаратные средства – Web-сервер, Маршрутизатор …	5	1	9	3	9	3	3	9	3	9	3	9	338	4
Ненадежное беспроводное соединение	2	9	3	9	9	1	3	3	1	3	1	1	338	4
Сервисы основанные на Интернет (VPN)	1	9	1	3	3	1	1	3	1	3	3	1	208	2
Перерыв в подаче энергии	1	0	1	0	0	3	1	9	3	3	1	1	106	1

Данные в матрице уязвимости были соединены и сортированы для того, чтобы определить относительную важность уязвимости. Так как внешние хакеры должны проникнуть через брандмауэр, чтобы получить доступу к

конфиденциальной информации, брандмауэр занимает первое место в матрице уязвимости. Кроме того, в General Electric Energy филиалы сильно распределены, поэтому передача данных, оценивается высоко. Совокупные данные о уязвимостях были добавлены к матрице угроз наряду с угрозами, соответствующими уязвимостям. Матрица 5 выглядит следующим образом:

Таблица 5 - Матрица угрозы для General Electric Energy

Ранжирование приоритета 1 и 2 не важный 3 важный, но не ключевой 4 важный, но находящийся под воздействием ключевого 5 Ключевой	**Активы/Воздействия**	Брандмауэр	База данных	Архитектура приложений	Физическая безопасность	Ошибки конфигурации серверов интернет	Ошибки конфигурации серверов экстранет	Устойчивость паролей	Клиентские узлы (ПК и ноутбуки)	Клиентские узлы (ПК и ноутбуки)	Аппаратные средства – Web-сервер,	Ненадежное беспроводное соединение	Сервисы основанные на Интернет (VPN)	Перерыв в подаче энергии	Всего	Разряд (Выше более существенный)
Приоритет -> **Уязвимости**		13	12	11	10	9	8	7	6	5	4	3	2	1		
Вторжения (Взламывание паролей)	5	9	3	3	9	9	1	9	3	9	9	9	3	1	170	11
Отказы Сервера	5	9	9	9	3	9	9	1	9	1	9	1	1	9	158	10
Физическое повреждениеаппаратных средств	4	1	9	9	9	9	9	0	3	3	3	1	1	3	132	9
Вымогательство	4	1	3	3	3	9	3	3	3	9	9	3	3	1	122	8
Внутренние атаки	3	3	3	3	3	9	1	3	9	9	1	3	1	1	114	7
Spoofing & masquerading	2	1	9	1	3	1	1	1	9	9	9	9	1	1	110	6
Отказ в обслуживании	4	9	1	0	9	1	3	1	9	1	9	3	3	1	100	5
Ошибки	3	3	9	3	3	3	1	3	9	3	3	1	1	1	90	4

пользователей																
Нарушение экспортного контроля	3	1	0	1	1	9	1	1	1	9	1	3	1	1	76	3
Вредоностный код	5	1	1	1	1	9	1	1	1	9	1	1	1	1	74	2
Переполнение буфера	2	1	1	1	3	1	1	1	3	9	3	3	3	1	62	1

Таблица 6 показывает матрицу контроля, в которую были добавлены совокупные данные об угрозах из матрицы угрозы и соответствующие им средства управления. Относительное воздействие различных средств управления на угрозы было также определено, учитывая субъективные суждения, после чего данные были занесены в таблицу и расположены по приоритетам. Эта информация, вместе со стоимостью средств управления используется для планирования безопасности. Результаты этого анализа и совокупные данные из матриц будут использоваться во время интеграции производственных процессов и для выбора программного обеспечения и аппаратных средств.

Таблица 6 - Матрица средств контроля для General Electric Energy

Ранжирование приоритета 1 и 2 не важный 3 важный, но не ключевой 4 важный, но находящийся под воздействием ключевого 5 Ключевой	**Угрозы**	Вторжения (Взламывание паролей)	Отказы Сервера	Физическое повреждениеаппаратных	Вымогательство	Внутренние атаки	Spoofing & masquerading	Отказ в обслуживании	Ошибки пользователей	Воровство компьютеров (ноутбуки/серверы)	Нарушение экспортного контроля	Вредоностный код	Переполнение буфера	Всего	Разряд (Выше более существенный)
Приоритет -> **Ср-ва управления**		12	11	10	9	8	7	6	5	4	3	2	1	436	12
Вторжения (Взламывание паролей)	5	9	1	1	9	9	9	9	9	3	3	3	9	422	11

Отказы Сервера	5	9	3	3	9	1	1	9	1	3	3	9	9	366	10
Физическое повреждениеаппаратных средств	5	9	9	0	3	3	3	1	9	1	3	1	1	316	9
Вымогательство	4	1	9	1	3	1	1	3	1	9	1	1	1	308	8
Внутренние атаки	2	9	1	0	0	3	3	3	3	1	9	3	9	306	7
Spoofing & masquerading	4	3	9	1	0	1	1	3	9	1	3	3	1	240	6
Отказ в обслуживании	4	3	1	1	9	3	3	3	3	3	9	3	9	234	5
Ошибки пользователей	3	3	9	3	9	3	3	0	3	1	3	0	0	215	4
Нарушение экспортного контроля	3	1	1	0	3	9	9	3	9	1	1	1	3	201	3
Вредоностный код	3	3	1	1	3	3	3	9	3	0	0	1	9	145	2
Переполнение буфера	2	1	1	0	0	1	1	3	9	1	0	1	1	94	1

ЗАКЛЮЧЕНИЕ

В данной статье представлена удобная методология для оценки рисков информационной безопасности, которую могут легко использовать организации. Методология обеспечивает удобные шаблоны, которые могут постепенно совершенствоваться с увеличением количества доступной информации. Методология обеспечивает прозрачность процесса анализа. Исследование на примере General Electric Energy выдвигает на первый план важные проблемы безопасности, с которыми сталкивается организация. Методология, адоптирующаяся к постоянно изменяющимся угрозам, уязвимостям и активам, полезна компаниям для того, чтобы самостоятельно провести оценки степени риска. Эта простая методология поможет провести анализ риска большому количеству компаний, которые часто отказываются от него из-за дорогих и сложных методологий, предложенных ревизорами.

ИСПОЛЬЗОВАННЯ ЛИТЕРАТУРА

1. Alberts, C., and Dorofee, A., Managing Information Security Risks: The

Octave Approach, Pearson
Education Inc., 2003.

2. Backhouse, J. and Dhillon, G. (1996). Structures of responsibility and security of information systems. European Journal of Information Systems, 5(1), 2-9.
3. Barber, B. and Davey, J. (1992). The use of the CCTA risk analysis and management methodology CRAMM. Proc. MEDINFO92, North Holland, 1589 –1593.
4. Baskerville, R. (1993). An Analytical Survey of Information System Security Design Methods: Implications for Information Systems Development. ACM Computing Surveys, 375-414.
5. Cerullo, M.J., and Cerullo, V. (1994). EDP risk analysis. Computer Audit Journal, (2), 9-30.
6. Fisher, R. (1984). Information Systems Security. Prentice-Hall.
7. Parker, D.B. (1981). Managers Guide to Computer Security. Prentice-Hall, Inc, Reston, VA, USA.
8. Stolen, K., den Braber, F. & Dimitrakos T. (2002). Model-based Risk Assessment – The CORAS Approach.
9. Suh, B. and Han, I. (December 2003). The IS Risk Analysis Based on a Business Model, Information and Management, 41(2), 149-158.
10. Weiss, J.D. (1991). A System Security Engineering Process. In Proceedings of the 14th National Computer Security Conference, Washington, DC.