Роль систем управления сетью в управлении эксплуатационными рисками ИТ

Информационный документ

Автор: Дирк Паесслер

Опубликовано: июль 2008 г.

www.paessler.com

info@paessler.com

PAESSLER®
the network monitoring company

Содержание

Краткое изложение

Жизнь полна всевозможных рисков. Хотя их и невозможно устранить полностью, но мудрые люди и организации выделяют ресурсы на уменьшение рисков, что позволяет им контролировать возможные потери.

В бизнесе управление рисками традиционно ассоциируется со страхованием. В ИТ акцент делается на технологических мерах исправления конкретной проблемы, часто с небольшим предварительным планированием. Понятно, что такой бессистемный подход к решению проблем имеет серьезные недостатки, в том числе возможность неэффективного расходования имеющихся ресурсов.

В сфере ИТ, как правило, акцент делается на двух видах рисков– вредоносных программах и восстановлении данных. Следствием этого может стать игнорирование других видов рисков, которые также должны рассматриваться (см. недавний отчет Gartner «IT Risk Management: A Little Bit More Is a Whole Lot Better», доступный по ссылке www.gartner.com).

С другой стороны, слишком интенсивное управление рисками ведет к расходованию ресурсов, которые лучше инвестировать в другие направления бизнеса, из-за чего необходимо соблюдать баланс усилий. Необходимо тщательно подходить к выделению ресурсов, чтобы обеспечивалось максимальное снижение рисков при минимальных затратах.

На многих направлениях управления эксплуатационными рисками ИТ зачастую пренебрегают важностью вопросов управления сетью. Разумеется, его значимость в решении потенциальных сетевых проблем, таких как отказы коммутаторов и перегрузки сети, является основным аргументом для инвестирования в ПО управления сетью. Тем не менее, оно также может играть определенную роль в выявлении и решении других потенциальных проблем, в том числе таких, как загрузка нежелательных материалов в сеть предприятия, или назначение приоритетов различным классам сетевого трафика, чтобы повысить эффективность бизнеса.

{удалено} В современном мире, где даже минимальные задержки транзакционного трафика имеют большую цену, ПО управления сетью может быть ключевым инструментом поиска проблем.

Всестороннее исследование рисков, с которыми сталкивается ИТ, содержится в пакете документов «Задачи информационных и смежных технологий» (Control Objectives for Information and related Technology, CobiT) версии 4.1, который может быть загружен с сайта ассоциации Information Systems Audit and Control Association (ISACA) по ссылке www.isaca.org/CobiT. Этот пакет документов посвящен рискам, связанным с ИТ, в частности, вопросам эксплуатации сетей. В нем представлен трехэтапный подход к выявлению, оценке и планирования общей стратегии смягчения эксплуатационных рисков ИТ. В нем также приводится практический пример использования мониторинга сети в качестве ключевого компонента этой стратегии.

Ссылки

Gartner Group:

“IT Risk Management: A Little Bit More Is a Whole Lot Better”

www.gartner.com

ISACA:

CobiT-article on risk management

www.isaca.org/CobiT

Классификация эксплуатационных рисков ИТ

Плохая новость: устранить риски невозможно. Целью управления рисками является выявление проблем, которые могут и должны контролироваться, и снижаться до приемлемого, с точки зрения бизнеса, уровня. Это будут остаточные риски, которые могут рассматриваться как издержки бизнеса.

Малым и средним предприятия (МСП), возможно, придется принять в качестве допустимых некоторые маловероятные, но потенциально разрушительные риски, что связано с недостаточностью ресурсов для их смягчения.

К сожалению, малые и средние ИТ-организации часто используют подход к безопасности на основе угроз вместо настоящего стратегического риск-менеджмента. Угрозой стали сетевые компьютерные вирусы – ИТ-отделы стали устанавливать антивирусное ПО; угрозой стали вторжения и взломы – стали устанавливать брандмауэры для защиты сетей от внешних воздействий и т.д.

Такой подход имеет две основных проблемы:

- Во-первых, он близорук и обращает внимание только на часть угроз из общего портфеля рисков – как правило, на технологически устранимые.
- Во-вторых, он фрагментарен и предполагает только ответное реагирование: Это приводит к росту числа устройств и служб, нацеленных на одиночные проблемы, без центрального управления. Такой ИТ-отдел, постоянно занятый «тушением пожаров», никогда не сможет добиться успеха. Он должен сделать шаг назад и разработать план мероприятий в отношении рисков.

Классы рисков

ИТ-отделы сталкиваются с тремя основными классами эксплуатационных рисков:

Технологические риски

Сюда относятся традиционные риски ИТ, от отказов оборудования и распространяемых по сетям компьютерных вирусов и червей, и до более экзотических вариантов, таких как DDoS-атаки, попытки вторжения со стороны т.н. варволкеров и вардрайверов, проникающих в беспроводные сети, находясь при этом вне зданий.

Многие средства решения этих проблем имеют технологическую природу, но при этом также важны очевидные и логичные политики. Очевидной политикой является неукоснительно соблюдаемое правило, согласно которому на портативных устройствах используются мощный брандмауэр и антивирусная система. Другая такой политикой является правило, согласно которому персоналу категорически запрещается устанавливать свои собственные, зачастую незащищенные, узлы WiFi.

Мощный инструмент мониторинга сети, такой как PRTG Network Monitor Paessler, может обеспечить раннее предупреждение о необычной, подозрительной активности в сети и определить источник такого трафика.

Юридические и кадровые риски

Сюда относятся следующие вопросы: подготовка к возможным требованиям юридического раскрытия информации (может включать в себя сбор электронной

переписки для гражданских исков); загрузка персоналом нежелательных материалов из Интернета, которые могут стать потенциальными плацдармами вторжения в сеть; возможный саботаж или шпионаж со стороны персонала.

Этими видами угроз труднее управлять, потому что для этого не существует четко прописанных технологических решений.

Ключом к снижению таких рисков является сильная кадровая политика и хороший менеджмент.

Менеджеров требуется обучать хорошим методам руководства и управления. Распространенной ошибкой является предположение о том, что хорошего работника достаточно повысить до управленца, и он автоматически станет хорошим менеджером.

Тем не менее, и здесь управление сетью может в состоянии помочь решить некоторые потенциальные проблемы. Некоторые из них могут быть обнаружены с помощью такого инструмента, как PRTG Traffic Grapher Paessler, который в режиме реального времени обеспечивает мониторинг сетевого трафика и использования полосы пропускания.

Природные и техногенные катастрофы

Наводнения, землетрясения, большие бури и ураганы случаются очень редко, но бывают очень разрушительны.

Определение адекватных стратегий преодоления таких рисков является одной из самых сложных задач риск-менеджмента.

Имеются различные стратегии, отличающиеся ценой и уровнем защиты. Они должны рассматриваться в контексте общего состояния бизнеса.

Тем не менее, борьба со стихийными бедствиями должна начинаться со здравого смысла.

В современном, сетевом мире, даже относительно небольшие организации могут найти для себя ЦОДы, размещенные вдали от районов, подверженных стихийным бедствиям, в современных и безопасных сооружениях (возможно, используемые совместно с другими предприятиями) или передать управление ИТ-инфраструктурой аутсорсерам или поставщикам услуг SaaS, которые смогут обеспечить более высокий уровень безопасности, чем само предприятие на своей площадке.

Опять-таки, это делает инструменты управления сетью, такие, как имеющиеся у компании Paessler, важным средством управления такими рисками. В обоих случаях сеть, включая последнюю милю Интернета, становится центральным, если не сказать важнейшим, элементов доставки бизнесу всех видов ИТ-услуг.

Трехэтапный план

Хотя многие мелкие ИТ-отделы и достойны всяческого порицания за полное отсутствие планирования, не менее важно избегать и увлечения излишним планированием. Для малых и средних предприятий, и даже некоторых крупных, планирование управления рисками может быть довольно неформальным процессом, наподобие упражнений по заполнению электронной таблицы.

Этап 1. Список и рейтинг рисков применительно к издержкам бизнеса

Первым шагом в этом упражнении является выявление основных рисков по каждой из трех категорий.

Списки стандартных рисков известны и доступны. Одним из самых полных является соответствующий раздел из «IT governance framework CobiT», однако эти списки могут быть излишне подробны и охватывать более широкий круг вопросов, чем те, которые может потребоваться учесть ИТ-организации.

Каждый проект включает в себя ряд собственных рисков, включая возможность того, что работа никогда не завершится, или что будет завершена плохо, или выйдет из бюджета и графика.

Можно достаточно легко составить полный список рисков, но ранжировать их по потенциальным затратам бизнеса и важности намного сложнее.

Хотя списки рисков являются универсальными, затраты бизнеса могут широко варьировать от организации к организации.

Например, если для финансовых трейдеров будут недопустимы даже небольшие задержки при передаче сделок, то компания-производитель может быть терпима к задержкам в обработке заказов, хотя ей, возможно, потребуется высокая производительность ERP-системы. Это иллюстрирует сложность оценки общей стоимости для бизнеса каждого из рисков.

Разработчикам плана потребуется провести консультацию с руководителями бизнеса, чтобы выяснить, что может быть предложено руководством любых ассоциаций своей отрасли и коллегами из других компаний того же вертикального рынка.

Хотя оценка и не должна быть точной, но она очень важна. Она станет основой при расчете объемов инвестиций, направленных на снижение уровня рисков. В ней должна уточняться, что основное внимание следует обратить на защиту организации от основных угроз, таких как вирусы и черви.

Тем не менее, должны затрагиваться и другие важные вопросы планирования.

Сколько должно быть потрачено на основные угрозы по сравнению с другими рисками?

Когда инвестиции достигнут точки падения отдачи?

Ответы на эти жизненно важные вопросы планирования зависят, в частности, от стоимости ущерба, наносимого этими ИТ-угрозами.

Также должна обязательно учитываться вероятность события. Например, вирусы являются постоянной головной болью, но не требуют больших расходов на устранение проблем и не вызывают серьезных нарушений. Тогда как крупная катастрофа, несмотря на ее низкую вероятность, вполне сможет полностью уничтожить бизнес.

Этап 2. Оценка затрат на снижение угроз

Она не должна быть точной и не должна содержать документов с предложениями по условиям реализации (RFP) и т.п. Достаточно будет оценок, основывающихся на опубликованных в Интернете исследованиях и прошлом опыте. Разработчики плана

должны иметь в виду, что в расходы будут включены расходы на персонал и оплату рабочего времени, а также целевое финансирование. В ряде случаев возможно прямолинейное решение, когда смягчение рисков предполагает покупку и установку оборудования или ПО. В других случаях, в частности в случае аварийного восстановления, доступны разнообразные стратегии, варьирующиеся по величине затрат и эффективности.

Определение того, какая из них лучше подойдет для какой-либо организации, зависит от множества факторов:

- Устойчивость к длительным простоям
- Наличие ресурсов для решения проблемы
- Живучесть в случае крупных катастроф

Малый бизнес, чтобы выжить в условиях катастроф, будет расходовать деньги на удаленные (облачные) технологии резервирования данных. Если же компания может позволить себе полное резервное всех данных на ленты и их хранение в защищенном месте, то при выборе технологии резервирования данных смотрят на то, соответствует она реальным потребностям организации или нет. Кроме того, важными вариантами для рассмотрения являются более гибкие решения, такие как использование поставщиков услуг SaaS или аутсорсинговых компаний, занимающихся резервированием данных.

Кроме того, разработчики плана могут выяснить, что затраты на снижение каких-то рисков окажутся больше предполагаемых потерь. В таких случаях, вероятно, не стоит заниматься инвестированием в снижение таких рисков.

Кроме того, при определении стратегии снижения рисков должна учитываться относительная устойчивость компании к рискам, обозначенная ее высшим руководством.

Этап 3. Долгосрочное планирование

Снижение рисков требует постоянной интенсивной работы, так как всегда имеет место нехватка ресурсов, создающая потребность в долгосрочном планировании.

С течением времени структура рисков меняется, поэтому постоянно должны рассматриваться свежие подходы к данному вопросу.

Например, риск вирусов остается неизменным, но изменяются сами вирусы. Таким образом, хотя организация может быть настоящим ветераном в борьбе с такого рода рисками, ей все равно необходимо постоянно сохранять бдительность.

Новый риски, такие как беспроводные сети и варволкеры (вардрайверы), могут появляться на любых этапах, а бизнес-мероприятия компании (такие как выход на новые рынки и отрасли или приобретения бизнесов) могут менять картину основных рисков.

Большая иллюстрация: снижение рисков и сеть

Разработчики планов по управлению рисками должны учитывать влияние решений по снижению рисков на работу всей сети и на планирование других вопросов, касающихся ИТ.

При рассмотрении мер снижения рисков следует уделять больше внимания не вопросам стоимости, а выбору между использованием внутрикорпоративных или контрактных услуг.

Часто решения принимаются с учетом относительной стоимости, наличия специальных знаний и навыков или внутренних правил.

Тем не менее, тщательный процесс принятия решений может стать эффективным способом изменения общей картины рисков. Продавец принимает на себя ряд рисков, таких как безопасность данных и их восстановление, но, в свою очередь, компания принимает на себя риск того, что продавец может не удовлетворять соглашениям об уровнях обслуживания (SLA) или, что согласованные SLA могут перестать устраивать компанию спустя какое-то время. Если ИТ-отдел сможет уменьшить инвестиции в некоторые направления снижения рисков, он будет инвестировать в управлении услугами, от которых зависит бизнес компании.

Управление сетью является еще одним важным инструментом, зачастую недоиспользуемым в интересах снижения рисков. Связь этой технологии с некоторых областями рисков, в первую очередь касающимися сетевых компонентов и управления горячим резервом и переключениями, очевидна и это, как правило, является главной причиной покупки решений по управлению сетью. Однако эта же технология косвенно используется и на других направлениях управления рисками.

Одно из важнейших направлений связано с рисками задержек передачи данных в случае перегрузок сетевого трафика.

Технология VoIP, как известно, чувствительна к задержкам, а введение VoIP в сети сопровождается приоритизацией трафика для обеспечения доставки голосовых пакетов адресатам без задержек.

Другие приложения могут быть чувствительны к задержкам передачи данных. Например, в некоторых отраслях, таких как передача информации по валютным, фондовым и сырьевым торговым площадкам, хронические задержки при передаче транзакций могут привести к финансовым потерям.

В случае современных высокоавтоматизированных производств, работающих в режиме реального времени, даже небольшие задержки постоянные в передаче данных могут приводить к падению темпа работы производственных линий, в результате чего будут теряться объемы производства. Потеря автоматизированного заказа или отгрузочных данных в случае поставок по строгому графику (JIT, «just-in-time») может иметь катастрофические последствия. Поэтому мощная система управления сетью позволяет повысить рентабельность многих производств уже только за счет отсутствия задержек передачи жизненно важных данных.

Хорошее управление сетью также может помочь определить причины заторов и других проблем в системе. В современной высокомобильной среде, с увеличением числа управленцев и работников умственного труда, берущих с собой ноутбуки и другие устройства, используемые вне офисной системы защиты корпоративной сети, возрастает опасность занесения вредоносного ПО внутрь защищенного брандмауэром «безопасного периметра» своими же собственными сотрудниками.

Часто первым признаком присутствия таких рисков как самопроизвольные массовые

рассылки спама, отказы в обслуживании систем моментальных сообщений или распространение «червя» по системам организации, являются всплески сетевого трафика, регистрируемые ПО управления сетью. Оно же часто является главным инструментом отслеживания проблем и поиска источников их возникновения.

Беспроводные сети WiFi добавляют собственные риски

ИТ-отделы утрачивают контроль над тем, что за устройства подключаются к их сети, в результате чего появляются новые риски, начиная с несовместимости приложений и мобильных устройств конечных пользователей, до доступа к сети со стороны посетителей и прочих неавторизованных лиц.

Сеть часто простирается за физические границы (стены) здания, что делает ее потенциально уязвимой перед вардрайверами или варволкерами, получающими доступ к сети, и, возможно, корпоративным приложениям и данным откуда-то с тротуара или автостоянки.

Как известно, WiFi-модемы очень легко подключить к сети. И сетевые администраторы часто обнаруживают неофициальные сети WiFi, появляющиеся в тех офисах, где сотрудники подключают к сети свои беспроводные модемы. Как правило, эти сотрудники даже не задумываются о том, чтобы включить защиту доступа к WI-FI модему, создавая тем самым потенциальную брешь в безопасности, позволяющую обхода злоумышленникам обойти корпоративные брандмауэры и провести вторжение в сеть предприятия или занести в нее вредоносное ПО.

Мощная система управления сетью может помочь ИТ-отделу обнаруживать и нейтрализовывать потенциальные риски, связанные с беспроводными сетями, и сохранять контроль над беспроводной средой.

Подробный мониторинг интенсивности сетевого трафика стал сегодня особенно важным из-за существенных изменений, произошедших в видах и объемах деловых данных. Символьные данные, преобладавшие до недавнего времени в рабочем трафике персонала, сейчас дополняются большими объемами графической информации, а также цифрового аудио и видео. Это легко может привести к перегрузке офисной сети, рассчитанной на обычные данные символьного типа. Довольно сложно отличить обычный бизнес-трафик от развлекательного, или враждебного, указывающего на создание точки вторжения в сеть на каком-то из рабочих мест.

Часто источником этого трафика являются такие сайты, как YouTube , большая часть трафика которых не является враждебной. Например, предприятия заменяют командировки теле- и видеоконференциями, проводимые как из совещательных и переговорных залов, так и прямо с рабочих мест. Это может сэкономить компаниям крупные суммы, расходуемые на командировки, повысить производительность труда персонала за счет отсутствия потерь времени на дорогу, поднять дух персонала, а также способствовать снижению выбросов двуокиси углерода.

Быстрый рост объема такого трафика, стимулируемый ростом цен на топливо и расходов на командировки, может увеличить риски, связанные с перегрузкой трафика сети из-за пиковых нагрузок, что может вызвать снижение качества услуг, предоставляемых по сети. Хороший инструмент управления сетью, умеющий

визуализировать динамику роста использования сетевых устройств, такой как PRTG Network Monitor Paessler, является первой линией обороны против такого рода рисков. Он может играть важную роль и в мониторинге быстрого роста сетевого трафика, и сборе данных для планирования увеличения пропускной способности сети.

Компания Paessler и управление рисками

Paessler предлагает различные приложения, включающие полный комплект средств мониторинга корпоративный сетей любого масштаба и обеспечивающие возможности наглядного контроль за критически важными частями сетей. В отличие от своих конкурентов, компания провела редизайн всех своих инструментов, переведя их на оптимизированную технологическую базу и улучшив общую функциональность, эффективность и удобство использования.

Набор инструментов компании Paessler состоит из:

PRTG Network Monitor

www.paessler.com/prtg является простым в использовании Windows-приложением для мониторинга и анализа доступности сети, трафика и видов нагрузки.

Он сочетает в себе возможности старых решений компании Paessler – IP-Check Server Monitor и Paessler Router Traffic Grapher. Это помогает организациям контролировать критически важные сетевые ресурсы и обнаружить сбои системы или проблемы с производительностью сразу же, минимизируя простои и их экономические последствия. Текущие параметры и долгосрочные тенденции использования сетевых устройств также могут быть использованы для анализа использования полосы пропускания, памяти и процессоров. Возможен удаленный сеть мониторинг и управление сетью с помощью веб-браузеров.

***Продукция компании** Paessler*

PRTG Network Monitor:

Мониторинг доступности и использования сети:

www.paessler.com/prtg

SNMP Helper:

Мониторинг производительности Windows: www.paessler.com/snmphelper

Webstress Server Tool:

Нагрузочное и стрессовое тестирование веб-сайтов:

www.paessler.com/webstress

SNMP Helper

www.paessler.com/snmphelper позволяет PRTG Network Monitor собирать детальную информацию о производительности серверов Windows, и рабочих станций. {удалено}

Всего нескольких щелчков мыши обеспечат контроль за несколькими тысячами параметров и счетчиков производительности ПК.

Webserver Stress Tool

www.paessler.com/webstress – это мощное HTTP клиент-серверное тестовое приложение, предназначенное для выявления тех критических проблем с производительностью веб-сайта или веб-сервера, которые могут помешать их нормальной промышленной эксплуатации в интересах бизнеса. Моделируя одновременный доступ сотен или тысяч пользователей, оно проверяет производительность веб-сервера при нормальных и стрессовых нагрузках, чтобы убедиться, что время доступа к критически важной информации и услугам не превышают ожидаемого пользователями времени отклика. Подробные журналы испытаний и удобные графики упрощают процесс анализа результатов тестов. Webserver Stress Tool для Windows позволяет проверить практически любой HTTP-сервер (статические страницы, JSP/ASP или CGI) в плане работоспособность кода, производительности и реакции на стрессовые нагрузки.

Все эти инструменты входят в различные наборы ПО и включают в себя как бесплатную, так и 30-дневную ознакомительную версию, позволяющую опробовать основные функции ПО, прежде чем принимать решение о его покупке.

Заключение

В конечном счете, не бывает никаких гарантий. Жизнь полна всевозможных рисков, и любая компания должна быть готова принять на себя определенные риски. Управление рисками не является гарантией того, что не сможет случиться ничего плохого, потому что даже с самыми безопасными средами случаются проблемы. Вместо этого, целью управления рисками является снижение их воздействия до приемлемого уровня, являющегося приемлемым одновременно в плане расходов и выживания бизнеса компании.

Если ИТ-отдел может этим управлять, то можно считать его программу управления рисками успешной.

О компании *Paessler AG*

Компания была основана в 1997 г. Головной офис Paessler AG находится в Нюрнберге. Продукцией компании является высокорентабельное ПО, одновременно и мощное, и простое в использовании.

Линейка продукции компании состоит из ПО для мониторинге и тестирования сетей, а также для анализа веб-сайтов. Этим ПО пользуются сетевые администраторы, операторы веб-сайтов, персонал сервис-провайдеров и другие ИТ-специалисты по всему миру. Бесплатные и ознакомительные версии всех продуктов компании можно загрузить с сайта www.paessler.com.

PAESSLER®
the network monitoring company

Paessler AG • Burgschmietstrasse 10

90419 Nuremberg • Germany

www.paessler.com • info@paessler.com