БЕЗОПАСНОСТЬ ДЛЯ БИЗНЕСА. ВЗГЛЯД CISCO SYSTEMS

Любой руководитель компании задумывается о многих ключевых вопросах, влияющих на развитие его бизнеса. Это:

- рост доходов,
- снижение издержек,
- соответствие законодательству и нормативным требованиям,
- клиентские сервисы,
- репутация,
- повышение инвестиционной привлекательности
- и другие.

Информационная безопасность далеко не всегда значится в этом списке. Данная задача, неразрывно связанная со стратегией развития бизнеса и служащая одной из его движущих сил, обычно считается чисто технической и тактической. Компания Cisco Systems, обладая многолетним опытом работы в этой области, готова стать для Вас доверенным советником (Trusted Business Advisor) в области защиты информации и помочь в правильном построении процесса управления информационной безопасностью.

Миссия компании Cisco Systems в области безопасности

Миссия нашей компании в области информационной безопасности заключается в создании условий для безопасного роста бизнеса наших заказчиков. Причем безопасность обеспечивается прозрачным и невидимым для конечного пользователя способом – все, как в хорошем автомобиле, – пассивные защитные механизмы работают ежесекундно и, не создавая помех, обеспечивают безопасность как водителя и пассажиров, так и окружающих их людей. В минуты же серьезной опасности включается активная защита, предотвращающая или смягчающая последствия аварийных ситуаций.

Отличительной особенностью нашего подхода является изначальное встраивание защитных механизмов во все решения нашей компании – в телефонию, системы хранения, беспроводные решения, видеоконференцсвязь и т. д. Это значит, что даже без инвестиций в специализированные решения по безопасности наше оборудование уже обеспечивает базовый уровень защищенности.

Безопасность и информационные технологии

Интернет, родителем которого часто называют компанию Cisco, радикально изменил отношение к ведению бизнеса. Компании выводят возможности установления взаимоотношений с заказчиками, поставщиками, партнерами, своими сотрудниками на качественно новый уровень. Стремление компаний стать лидерами в своем сегменте рынка привело к появлению новых приложений для управления предприятием (ERP), цепочками поставок (SCM), взаимодействия с заказчиками (CRM), управления производством (АСУ ТП или SCADA), дистанционного обучения (eLearning) и т. п. – приложений, которые снижают издержки на выполнение транзакций, ускоряют многие бизнес-процессы, увеличивают удовлетворенность пользователей и снижают совокупную стоимость владения информационной системой.

БЕЗОПАСНОСТЬ – ПРИОРИТЕТ № 1

«Так как информационные технологии являются стратегическим активом наших заказчиков, безопасность их приложений и ресурсов, критических с точки зрения бизнеса, является для нас приоритетом № 1».

Джон Чемберс,
CEO Cisco Systems

Безопасность является фундаментальным элементом любой стратегии электронного ведения бизнеса. Открытие своих сетей для большего числа пользователей и приложений приводит к росту опасностей для информационных ресурсов. С ростом рисков растет важность задач управления ими и повышения уровня защищенности компании от внешних и внутренних несанкционированных информационных воздействий. Компания Cisco Systems, помогая своим заказчикам в их бизнесе, не может обойти вниманием область информационной безопасности и предлагает уникальную стратегию защиты корпоративных сетей – Cisco Self-Defending Network.

Стратегия Cisco Self-Defending Network

Идея самозащищающейся сети Self-Defending Network (SDN) достаточно проста: в настоящее время поддержание целостности и конфиденциальности корпоративной информации, а также непрерывности бизнеса в течение всего жизненного цикла бизнес-процессов является ключом к успеху любой компании. Значение информации и контроля доступа к ней еще никогда не было так велико. Таким образом, задачей архитектуры безопасности является предоставление своевременного доступа законным пользователям с одновременной возможностью обнаружения и предотвращения нарушений безопасности. Современные сети должны реагировать на такие нарушения, сохраняя свои доступность, надежность и функциональность. Во многих отношениях целью процесса обеспечения безопасности является обеспечение непрерывности бизнеса. Вместо того чтобы становиться жертвой, инфраструктура должна быть способна «поглощать» атаки и сохранять работоспособность, подобно иммунной системе человека, позволяющей организму функционировать при наличии в нем вирусов и бактериальных инфекций.

Стратегия Self-Defending Network построена на концепции ограниченности ресурсов (финансовых, человеческих, временны́х и т. п.) и необходимости их бережного использования во избежание их истощения и роста издержек. Также эти системы используют все преимущества существующей инфраструктуры, оказывая минимальное воздействие на ИТ-операции и бизнес-процессы компании.

Управление рисками

ПРАВИЛЬНЫЙ ПОДХОД

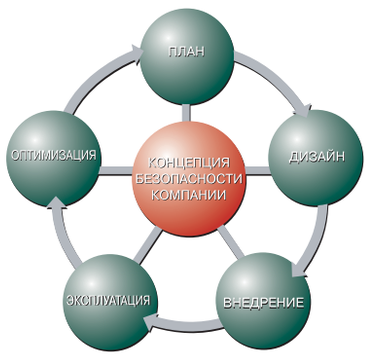
«Данный подход позволяет установить правильное соотношение рисков в масштабе предприятия и усилий по соблюдению соответствия, а также снизить расходы, связанные с ИТ-аудитом, поскольку в случае корректно построенного предприятием механизма контроля аудиторским организациям требуется тратить гораздо меньше времени и ресурсов на оценку рисков».

Дж. Л. Баяк,
Ассоциация ИТ-аудита ISACA

Высшее руководство компании сосредотачивает внимание на проблеме согласования информационных систем и сетей со стратегией предприятия, одновременно управляя новыми рисками (операционными и информационными), ставящими под угрозу конфиденциальность, целостность и доступность бизнес-процессов и информации. Исторически сложилось так, что подход к управлению рисками, касающимися информации и сетевой безопасности, реализовывался несколькими различными подразделениями и отделами, что приводило к дублированию усилий и функций. Очевидно, что эти разные подходы зачастую могут быть несовместимы, а системы контроля накладываются, противоречат или подрывают работу друг друга.

Концепция самозащищающейся сети Cisco Self-Defending Network – это сквозная стратегия корпоративной обороны, поскольку она является основой для защиты всех данных, приложений и бизнес-процессов. Она представляет собой основную составляющую стратегии организаций по управлению рисками нарушения информационной безопасности, поскольку предоставляет комплексный и системный подход к проблеме сетевой безопасности, поддерживающий общепризнанные в отрасли механизмы контроля и передовые методы обеспечения безопасности. Этот подход позволяет организациям усовершенствовать механизм управления операционными и информационными рисками и обеспечить их соответствие нормативным документам.

Полный жизненный цикл сервисов и услуг



Учитывая сложность и масштабность современных информационных технологий для бизнеса, обеспечить их безопасность – не такое простое дело. Группа консультантов компании Cisco Systems готова помочь Вам:

- в разработке стратегии и архитектуры управления информационными рисками;
- во внедрении и настройке средств управления рисками согласно утвержденной стратегии;
- в оптимизации уже внедренных и настроенных средств защиты;
- в поддержке внедренных решений при помощи круглосуточной службы технической поддержки (Technical Assistance Center);
- в аудите созданной инфраструктуры на соответствие требованиям международных стандартов ISO 17799/27001, CoBIT, ITIL и т. п.

Соответствие законодательству

Практически все организации испытывают повышенное давление со стороны правительства и отдельных ведомств, заинтересованных вопросами надлежащего использования информации, в особенности финансовых данных. Многие российские руководящие органы и общественность серьезно озабочены проблемами информационной безопасности и начинают предпринимать надлежащие действия, направленные на обеспечение целевого использования и защиты как корпоративной информации, так и персональных данных. Аналогичная задача возникает и при выходе компании на международный рынок (например, на IPO).

В результате всем компаниям, планирующим работать еще не один год, необходимо соответствовать растущему числу законов и постановлений. К их числу можно отнести акт Сарбейнса-Оксли, ISO 17799 (и его развитие ISO 27001), закон Грэмма-Лича-Блайли (GLBA), HIPAA, Базель II, Руководящие документы Федеральной службы по техническому и экспортному контролю (бывшая Государственная техническая комиссия при Президенте России), «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», ГОСТ Р ИСО/МЭК 15408 и др. Решения Cisco Systems по информационной безопасности соответствуют практически всем требованиям этих стандартов и рекомендаций. Во многих случаях это подтверждается соответствующими сертификатами. На сегодняшний день решения компании Cisco имеют свыше 200 сертификатов по требованиям информационной безопасности, выданных в России, что существенно превышает число сертификатов, полученных какой-либо другой компанией (российской или зарубежной), работающей на отечественном рынке информационной безопасности.

Лидерство и инновации

БЕЗОПАСНОСТЬ – КУЛЬТУРА КОМПАНИИ

«Безопасность начинается с меня, CEO компании, и спускается вниз до каждого рядового сотрудника… Это обязательно».

Джон Чемберс,
CEO Cisco Systems

Согласно исследованиям компании Synergy, компания Cisco последние 3 года занимает первое место на рынке сетевой безопасности, удерживая долю в 36%, что в три раза превышает показатели ближайшего конкурента. Оборот Cisco Systems в области информационной безопасности за 2005 календарный год только на территории России составил 40 миллионов долларов США. Эти показатели, по данным CNews, позволили нашей компании уже не первый год подряд занимать первое место в России среди игроков рынка информационной безопасности.

Наша лидирующая роль была бы невозможной без серьезных инвестиций в исследования, разработки и участие в деятельности различных стандартизующих организаций и рабочих групп. Не будет преувеличением сказать, что на наших

исследованиях «построены» Интернет и его безопасность; эксперты Cisco участвовали в разработке свыше 60 общепризнанных стандартов в области защиты информации. Но наша компания не останавливается на достигнутом и продолжает активно участвовать в разработке различных стандартов по информационной безопасности.

Без исследований невозможно разрабатывать решения, которые бы удовлетворяли как требованиям заказчиков, так и рекомендациям различных регулирующих органов и нормативных документов. Именно поэтому компания Cisco инвестирует около 10% своего общего бюджета в исследования и разработки, связанные с информационной безопасностью. В абсолютных цифрах это составляет около 300 миллионов долларов ежегодно. Такой подход позволяет компании Cisco лидировать практически во всех сегментах рынка средств защиты информации, на которых представлены решения компании.

Уровень зрелости безопасности

Мы готовы поддержать Вашу компанию, на каком бы уровне зрелости информационной безопасности она ни находилась, и провести Вас к вершине, на которой безопасность превращается из тормоза в одну из движущих сил бизнеса. На этом уровне информационная безопасность четко увязана со стратегией развития компании, имеет измеримые бизнес-показатели эффективности и является неотъемлемой частью культуры компании.

Наши заказчики

В первую очередь мы, компания Cisco Systems, сами являемся пользователями наших решений. Среди наших международных заказчиков можно назвать Муниципальную транспортную систему Монреаля (Канада), Спринт (США), банк «Меридиан» (Сербия), Swisscom (Швейцария), Boeing (США), AT&T (США), Siemens (Германия), American Mountain Credit Union (США) и многие другие. Среди российских заказчиков можно назвать РАО ЕЭС, ОАО «РЖД», «Салаватнефтеоргсинтез», ООО «Сургутгазпром», Уральский оптико-механический завод, Tchibo, банк «Кольцо Урала», пивоваренный завод «Вена» и др.

Cisco Systems
Россия, 115054, Москва
бизнес центр «Риверсайд Тауерс»
Космодамианская наб., 52
стр. 1, этаж 4
Тел.: +7 (495) 961 14 10
Факс: +7 (495) 961 14 60
www.cisco.ru
www.cisco.com

Cisco Systems
Россия, 191186, Санкт-Петербург,
бизнес центр «Регус»
Невский проспект, 25,
этаж 2, офис 30
Тел.: +7 (812) 346 77 17,
Факс: +7 (812) 346 78 00
www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099 Алматы
бизнес центр «Самал 2»
Ул. О. Жолдасбекова, 97
блок А2, этаж 14
Тел.: + 7 (3272) 58 46 58
Факс: + 7 (3272) 58 46 60
www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004 Киев
бизнес центр «Горайзон Тауерс»
Ул. Шовковична, 42-44, этаж 9
Тел.: + 7 (38044) 490 36 00
Факс: + 7 (38044) 490 56 66
www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong • SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe