SAP: итоги 2010 г.

Февраль 2011 г. – Компания SAP подвела итоги работы в России и странах СНГ в 2010 г. Доход от продажи ПО в России вырос на 83% (без учета сделки с Газпромом – 35%), доход от сервисных услуг – на 37%, а рост совокупного дохода в России составил 53%. Доход в сравнении с 2007 г. – самым лучшим годом по объему продаж – вырос на 10–15%.

По абсолютным показателям, SAP СНГ стал третьим подразделением компании SAP в регионе EMEA и Индия и пятым в мире по выручке за 2010 г. "Подразделение SAP СНГ впервые за 18 лет работы на рынке России и СНГ было признано лучшим подразделением года среди всех региональных офисов SAP. Мы этим гордимся, так как эта премия присуждается не только за объем продаж и рост, но также за высокую эффективность и устойчивость бизнеса, которая определяется на основе набора показателей", – отметил генеральный директор SAP СНГ Владислав Мартынов.

Trend Micro: новые решения для защиты данных в облаках

Март 2011 г. – Компания Trend Micro объявила о запуске двух новых продуктов: Trend Micro™ SecureCloud 1.1 и Trend Micro™ Deep Security 7.5 Update 1. Первое решение обеспечивает защиту данных корпоративного класса путем шифрования в облаке, второе – всестороннюю защиту от угроз всех виртуальных машин на ESX-сервере на основе безагентной технологии и интерфейса VMware vShield™ Endpoint.

Trend Micro SecureCloud™ повышает и расширяет уровень безопасности и защиты данных клиента по мере перехода от виртуализации к частным и общедоступным облачным средам. Благодаря использованию шифрования и управления ключами на основе политик SecureCloud обеспечивает защиту данных в облаке и дает свободу перемещения между поставщиками облачных сред без привязки лишь к одной системе шифрования.

SecureCloud позволяет контролировать, как и где осуществляется доступ к данным, путем определения и проверки целостности серверов, запросивших доступ к защищенным данным. Система защищает информацию от несанкционированного раскрытия или утечки, помогает добиться соответствия требованиям шифрования и автоматически обеспечивает выпуск ключей шифрования.

Усовершенствования, внедренные в последнюю версию SecureCloud, дают дополнительный контроль над облачными данными. Новые клиенты получают возможность управлять ключами шифрования для сред Amazon EC2, Eucalyptus и VMware vCloud с помощью внешней услуги SecureCloud от Trend Micro либо сервера ключей SecureCloud, работающего в их физических центрах обработки данных.

Уязвимости в системе ИБ: обнаружить и устранить!

На вопросы журнала Storage News отвечает Эдвинас Пранцулис (MM, CISA, CISM, CRISC), управляющий директор компании Qualys в Восточной Европе, на Кавказе и в Центральной Азии. Согласно результатам отчетов Frost & Sullivan и Forrester (Vulnerability Management, Q2 2010, by Chenxi Wang, Ph.D. for Security & Risk Professionals, July 15, 2010), компания Qualys уже в течение ряда лет занимает на VM-рынке лидирующие позиции.

Эдвинас Пранцулис – региональный представитель компании Qualys в Восточной Европе, CISA, CISM.

SN. Эдвинас, давайте начнем наш разговор с такой немаловажной темы как стратегия обеспечения информационной безопасности компании. Как Вы считаете, с чего следует начинать в этом вопросе и каков подход компании Qualys?

Э.П. Начинать следует, безусловно, с создания анализа рисков собственной политики защиты информации. Эта политика всегда начинается "сверху" и требует контроля со стороны высшего руководства организации. Политика защиты информации определяет средства контроля за обеспечением безопасности, такие, как стандартные конфигурации для всех устройств безопасности и приложений, включая антивирусы, сетевую защиту и обнаружение/предотвращение угроз вторжения. На сегодняшний день стратегическое управление в большинстве случаев является неавтоматизированным, довольно затруднительным процессом. Автоматизация экономит время, улучшает качество принятия решений и снижает общие издержки на обеспечение информационной безопасности в компании. Решение QualysGuard помогает провести политику безопасности путем тестирования средств управления и быстрой идентификации слабых мест в системе защиты. Затем уязвимости устраняются, что находит свое документальное подтверждение на соответствие различным стандартам безопасности.

SN. Прежде чем устранять слабые места, их нужно выявить. Давайте подробнее обсудим именно процесс выявления уязвимостей в системах защиты информации.

Э.П. Этап выявления уязвимостей начинается с создания и поддержания текущей базы данных всех IP-устройств, подключенных к сети. Организации должны категоризировать устройства согласно их ценности для бизнеса, чтобы расположить их по приоритетам для будущего процесса устранения уязвимостей. Элементы в базе данных включают все аппаратные средства, программное обеспечение, приложения, сервисы и конфигурации. Необходимо очень ответственно подойти к данному этапу. Правильно организованный контроль за этой работой даст компании два преимущества: будет идентифицировано, какие уязвимости влияют на определенные параметры IT-инфраструктуры и бизнес-процессы, кроме того, точная инвентаризация гарантирует, что в процессе исправления будут отобраны и применены правильные патчи. Проведение инвентаризации также помогает ускорить процесс сканирования, поскольку сокращается время на поиск устройств с одного рода уязвимостями. Вы можете отследить эти данные ручным способом, но управление уязвимостями намного эффективнее при автоматизации всего процесса, то есть проведения инвентаризации с использованием решения QualysGuard.

SN. Проведя инвентаризацию всех устройств, задействованных в IT-инфраструктуре компании, мы подготовили почву для процесса выявления уязвимостей в системе информационной безопасности. Каковы дальнейшие шаги?

Э.П. А далее, собственно, начинается поиск уязвимостей путем сканирования всей инфраструктуры на наличие слабых мест. Система сканирования периодически тестирует и анализирует IP-устройства, сервисы и приложения. Отчет после сканирования указывает на фактические слабые места и на то, что именно нужно исправить. Есть много возможностей для сканирования. Некоторые решения требуют приложений, которые вы устанавливаете и поддерживаете, такие, как сканеры общего пользования Nessus, MaxPatrol. Это требует немало времени, ресурсов и обычно приводит к лишним издержкам. Решение QualysGuard, предоставляемое по требованию по модели SaaS ("ПО как сервис"), не требует внедрения и сопровождения какого-либо ПО – вся инфраструктура и сама система становятся доступны конечному заказчику сразу после активации учетной записи.

SN. Итак, сканирование выявило ряд уязвимостей в системе информационной безопасности предприятия. Какие меры предпринимаются для нормализации ситуации?

Э.П. Все неполадки сразу устранить невозможно. Фактически, в крупных организациях количество данных об уязвимостях может быть очень значительным. Если же эти данные должным образом не категоризированы, сегментированы и не расположены по приоритетам, то ситуация может просто шокировать!

QualysGuard распределяет уязвимости по категориям, чтобы определить, что нужно исправить в первую очередь. Организации могут разработать свою собственную схему категоризации или перенять рейтинговые шкалы из других источников. Корпорация Microsoft, например, выделяет четыре категории устранения риска: критически важный, важный, умеренный и низкий с соответствующими показателями. QualysGuard автоматически назначает категорию и уровень серьезности для каждой обнаруженной уязвимости. Уровень серьезности указывает на угрозу безопасности и определяется на основании исследования уязвимости и степени ее сложности. QualysGuard автоматизирует весь процесс и предоставляет соответствующую информацию, которой вы можете доверять. Создаются правила, по которым система после обнаружения уязвимостей определенного уровня автоматически открывает заявки на их устранение в виде проблемных билетов и выдает рекомендации соответствующим лицам. Система QualysGuard постоянно наблюдает за происходящими изменениями и тем самым дает возможность мониторинга уровня защищенности предприятия.

SN. Наконец все уязвимости "расставлены по полочкам", каждой присвоен свой приоритет и настала пора ими всерьез заняться. Что происходит далее?

Э.П. Далее начинается процесс исправления уязвимостей. Вносятся изменения в IT-инфраструктуру, применяются различные патчи. И здесь я должен отметить еще одну особенность решения компании Qualys. Дело в том, что традиционные неавтоматизированные процессы поиска недостатков, предполагаемые патчи и другие восстановительные мероприятия очень медленные, подвержены ошибкам и являются весьма дорогостоящими. Иногда высокая стоимость внесения исправлений вместе с большим объемом недостатков в приложениях от поставщиков вынуждают организации откладывать процесс устранения недостатков на неопределенное время. К сожалению, задержка может оказаться фатальной, поскольку потенциальные слабые места быстро обнаруживаются злоумышленниками – как показывают исследования, временной интервал между появлением угрозы и вторжением постоянно сокращается. Поэтому важно устранить уязвимость как можно быстрее и тем самым минимизировать риски. QualysGuard обеспечивает контроль установки патчей и других обновлений, а также осуществляет связь с патчами уязвимости, исправлениями и доработками, необходимыми для устранения обнаруженных "дыр".

SN. Любой бизнес-процесс требует отчетности. В разговоре Вы упомянули о соответствии стандартам по информационной безопасности…

Э.П. Да, это так. Но надо сначала сказать, что после применения патча или завершения процесса исправления ошибок, организациям необходимо повторить сканирование IP-ресурсов, подключенных к сети, чтобы гарантировать, что предпринятые меры сработали и не привели к сбою других устройств сети, серверов или приложений. И вот как раз результатом проверки исправлений становится документация по соблюдению положений стандартов по безопасности, таких как PCI-DSS, Sarbanes-Oxley Act, ISO 27001 и пр. Полученные отчеты помогают как руководителям, так и аудиторам понять уровень соответствия определенным стандартам.

SN. Эдвинас, а что Вы можете сказать о стоимости решения?

Э. П. QualysGuard – это в большей степени услуга. Стоимость ее зависит от количества IP-адресов заказчика. Поэтому, если компания небольшая, то стоимость услуг становится более чем скромной. Для очень больших компаний у нас предусмотрено гибкое ценообразование. Кроме того, подчеркну, что QualysGuard не требует для себя никакой дополнительной ИТ-инфраструктуры, то есть решение предоставляется "под ключ" и не требует внедрения и сопровождения какого либо ПО. Таким образом, у заказчика появляется возможность работать с самой современной технологией в мире в сфере управления уязвимостями при самой низкой совокупной стоимости владения (TCO).

Хочу добавить, что есть также специальные условия для консалтинговых компаний и компаний, занимающихся аудитом в области ИТ и ИБ. Они могут использовать сканер в своей основной деятельности для проведения разового аудита. При таком использовании стоимость QualysGuard, конечно же, значительно ниже.

SN. Каковы, на Ваш взгляд, перспективы решения QualysGuard на российском рынке?

Э.П. По состоянию на данный момент, услугами Qualys в России пользуются более 30 компаний. В основном это банки или международные компании. Есть и компании хорошо известные, лидеры в своих сегментах, например, "Аэрофлот", Yota, PricewaterhouseCoopers, GE Money Bank и др.

Могу сказать, что с каждым годом в России все большее количество компаний сознают реальную необходимость в наших услугах и положительно оценивают подход компании Qualys к вопросам обеспечения информационной безопасности. Угроз и уязвимостей в мире становится все больше и больше, без адекватных мер по предупреждению последствий от них не обойтись. Думаю, что в скором времени ни одна серьезная организация не сможет "закрывать глаза" на эту проблему, а это значит, что наша деятельность будет востребована в России еще больше!

В России у нас имеется ряд партнеров (компании "Анализ защищенности", "Информзащита", Leta, Technoserv, Altirix Systems, EVRAAS, Microtest, Step Logic), которые как продают подписки QualysGuard конечным заказчикам, так и используют наши решения для предоставления консалтинговых услуг. Мы ставим очень высокие требования к квалификации нашим партнерам, что гарантирует высокое качество их услуг. Добавлю, что дистрибьютором Qualys на территории России является компания DataSecurity Technologies, и каждый год мы получаем новые предложения партнерства.

"Информационная безопасность банков"

16 июня 2011 г. – Ассоциация российских банков и Сообщество пользователей стандартов Банка России (ABISS) при поддержке Банка России проводят летнюю сессию ***Межбанковской конференции "Информационная безопасность банков"*** по следующей тематике: ***"Вопросы применения и соответствия стандартам PCI DSS/PA DSS."***

Участие для представителей банков и других организаций кредитно-финансовой системы бесплатное.

Получить более подробную информацию, ознакомиться с обсуждаемыми вопросами а также зарегистрироваться можно на сайте конференции: *http://www.ib-bank.ru/dss/*.