



Компания «БМС КОНСАЛТИНГ»



*Александр Смычников,
консультант департамента
ИТ-консалтинга
компании «БМС Консалтинг»*

64

Прошлый год отметился несколькими крупными утечками информации, которые просто заставили специалистов в области информационной безопасности забить тревогу и, в буквальном смысле, броситься на защиту персональной информации от внешних и внутренних угроз. Именно персональной информации, поскольку по результатам исследований разнообразных аналитических команд и групп такие данные были наиболее «лакомым кусочком» для злоумышленников в прошедшем году.

Показатели по результатам 2009 года подтверждают интерес киберпреступников именно к персональной информации. Это, в свою очередь, должно повлечь за собой ужесточение контроля безопасности в организациях, которые оперируют персональными данными. В первую очередь это, безусловно, касается розничной торговли, финансовой и индустриальной отраслей экономики.

Это подтверждает и очередной ежегодный отчет, посвященный утечкам информации и угрозам информационной безопасности компаний за 2009 год, опубликованный известной аналитической командой Verizon Business RISK Team. Специалистами

команды был получен ряд весьма интересных результатов, которые демонстрируют специфику киберпреступности сегодня. В прошлом году произошло порядка 90 подтвержденных случаев утечки информации. В сумме с предыдущим, очень насыщенным, 2008 годом, было украдено порядка 285 миллионов записей персональных данных во всем мире. Внушительная цифра, не правда ли?

Но что удивительно — в 2009 году преступники даже не ухищрялись, чтобы получить доступ к нужной им информации. Как показывает отчет, лишь 17% всех атак были более или менее сложными. Все остальные случаи были связаны со стандартными распространенными и очень простыми способами компрометации данных. 98% всех утечек имели следующий сценарий: злоумышленник определял уязвимость в системе обеспечения безопасности, проникал в сеть и запускал вредоносный код изнутри. Стоит отметить, что подавляющее большинство уязвимостей, использованных преступниками, были связаны с банальными базовыми стандартами обеспечения безопасности систем и приложений (обновления безопасности, небезопасные протоколы, некорректная конфигурация аппаратного и программного обеспечения и т. п.). Что говорить, если проникновение в сеть с использованием стандартных паролей и SQL injection были наиболее популярными способами для совершения преступления? Да, количество направленных, созданных под определенную «жертву», атак практически удвоилось по сравнению с прошлым годом. Но на этом изощрения заканчиваются.

Не удивительно, что в отчете за этот год Verizon Business RISK Team уделила особое внимание узкоотраслевым стандартам в области обеспечения безопасности данных, в частности PCI DSS. Несмотря на то,

что многие специалисты утверждают, что данный стандарт всего лишь набор базовых правил обеспечения безопасности, соблюдение именно этих, «банальных», правил, могло бы уменьшить количество утечек в 3—4 раза. Особенно актуальным соблюдение требований стандарта PCI DSS выглядит в свете того, что более 60% компаний, которые пострадали от злоумышленников, представляют финансовый и банковский сектор. Компания «БМС Консалтинг», как квалифицированный аудитор систем информационной безопасности (QSA) и авторизованный вендор по сканированию (ASV) со своей стороны всегда настоятельно рекомендует своим клиентам обратить внимание на простоту и эффективность средств обеспечения информационной безопасности, которые описывает стандарт. Как и в прошлом году, компании, которые на момент утечки информации говорили о соответствии требованиям стандарта, соответствия не демонстрировали. Причем усредненное по всем 12-ти требованиям стандарта соответствие на момент утечки составило порядка 25—30%. Неправда ли не совсем достаточно, чтобы сетовать на стандарт или аудитора?

Стандарт PCI DSS — это комплекс требований, который касается не только технических средств информационной, но и физической безопасности, а также регламентации выполнения требований на нормативно-организационном уровне в компании. Не всегда обладая возможностями, желанием и необходимостью внедрять подобные комплексные меры обеспечения безопасности, компаниям, с нашей точки зрения, стоит посмотреть на этот вопрос с другой стороны. Результаты исследований показали, что, несмотря на то, что всегда «инсайдерские» (проводимые сотрудниками компании или третьими сторонами, имеющими доступ к внутренним информацион-

ным ресурсам компании) атаки считались наиболее опасными, в этом году почти три четверти утечек произошли после внешних атак и лишь 20% при «помощи» злоумышленников внутри компаний.

Для борьбы с внутренними и внешними злоумышленниками компания «БМС Консалтинг» предлагает услугу, которая поможет компаниям превентивно управлять уязвимостями информационной безопасности. Управление уязвимостями обрело наибольшую популярность еще и в связи с тем, что устранение уязвимостей и угроз информационной безопасности после возникновения инцидентов становится все более затратной процедурой. Менеджмент и технические специалисты понимают, что превентивное определение уязвимостей на сегодняшний день является еще и оправданным с финансовой точки зрения.

Управление уязвимостями в первую очередь направлено на снижение рисков информационной безопасности и представляет собой комплекс технологических, организационных и нормативных решений. Несмотря на то, что у такого подхода есть свои противники, даже они не отрицают того, что широкий спектр задач, который решается с помощью внедрения процесса управления уязвимостями, весьма и весьма привлекателен. Правильно реализованный процесс позволяет не только определять уязвимости в системах и приложениях, а классифицировать и ранжировать риски информационной безопасности, проводить инвентаризацию информационных ресурсов, управлять процессом обновления средств обеспечения безопасности. С управленческой точки зрения процесс управления уязвимостями информационной безопасности предоставляет аргументированный подход к развитию информационной безопасности компании.

Учитывая разнообразную природу утечек информации, специалисты «БМС Консалтинг» разрабатывают данный процесс для определения как внешних угроз и уязвимостей, так и внутренних. Отчетность по результатам функционирования процесса дифференцирована для управляющего персонала и технического. Если первые получают данные об общей ситуации и показатели рисков для бизнес-систем, то отчеты для технических специалистов содержат перечни угроз и потенциальных угроз, данные о системах и приложениях, на кото-

рых обнаружены уязвимости, а также конкретные методы (конфигурации, номера обновлений и т. д.) устранения обнаруженных уязвимостей. Подход «БМС Консалтинг» к определению и классификации уязвимостей затрагивает как сетевые уязвимости, так и уязвимости приложений, web-приложений, проблем соответствия разнообразным политикам и стандартам.

Стоит отметить, что подобная услуга учитывает рекомендации, приведенные в отчетах не только Verizon Business RISK Team, но и других аналитических групп. Все они сходятся во мнении, что приоритетными направлениями в повышении уровня безопасности вашей компании являются простые и всем известные средства контроля. Первым делом необходимо провести аудит и понять, какие же данные необходимо защищать. По результатам проведенного обследования надо определить какие данные не обязательно хранить. Ведь логично, что данные, которых у вас просто нет, невозможно скомпрометировать. Естественно, определенный набор данных, который жизненно важен для функционирования бизнес-процессов компании, придется оставить, но и его стоит свести к минимуму. Необходимо ужесточить в том числе контроль журналов и логов, их целостности и доступа к ним. Особое внимание должно быть уделено вопросам постоянного обновления

средств обеспечения безопасности и контроля использования стандартных паролей и профилей оборудования и программного обеспечения.

Существует еще целый набор рекомендаций, которые кажутся, на первый взгляд, настолько банальными, что неиспользование их в работе вашей службы информационной безопасности просто невозможно. Но факт остается фактом. Несмотря на обилие высоких технологий и мыслей о «комплексных стратегиях развития в направлении информационной безопасности», тотальное большинство угроз таится в несоблюдении базовых принципов информационной безопасности. Никто не сомневается в высокой квалификации сотрудников соответствующих подразделений и эффективности средств, которые они используют в работе. Идея нова: контролировать, контролировать и еще раз контролировать. А, как показала практика, внедрение процесса управления уязвимостями информационной безопасности не только повышает ее уровень, но и повышает уровень управляемости и контроля работы соответствующих программно-аппаратных средств и подразделений.

ООО «БМС Консалтинг»
04107, г. Киев,
ул. Печенежская, 32
Тел.: (044) 499-69-69, 483-10-20
Факс: (044) 499-69-68
www.bms-consulting.com

