“Когда произойдет утечка?”

Интервью с Сергеем Кузнецовым – Главой Представительства, региональным директором SafeNet Europe B.V. (в настоящее время – подразделение Identity and Data Protection компании Gemalto) в России и СНГ.

Сергей Кузнецов – Глава Представительства, региональный директор SafeNet Europe B.V. (подразделение Identity and Data Protection компании Gemalto) в России и СНГ.

SN. Что будет меняться в ведении и в структуре бизнеса (и, в частности, в России) после приобретения SafeNet голландской компанией Gemalto?

С.К. 8 января 2015 г., после получения соответствующих разрешений от регуляторов и согласования сделки с антимонопольными ведомствами, компания Gemalto завершила сделку по приобретению компании SafeNet. Объявленная сумма сделки составила $890 млн. Компания SafeNet была интегрирована в направление Gemalto, или сегмент Payment & Identity, классифицируемое как Platforms & Services в терминологии Gemalto.

К настоящему времени штат сотрудников объединенной компании Gemalto насчитывает более 14 тыс. человек, которые работают в 46 странах мира. Принципиально важно в данном слиянии то, что заказчики получают доступ, наверное, к лучшим в мире решениям в области защиты данных на уровне ядра (датацентра, сети, облака и т.д.) и на уровне доступа. В этих областях решения компаний Gemalto и SafeNet полностью комплементарны, что позволило объединенной компании нарастить позиции в области защиты данных, транзакций, безопасности в облаке, защите лицензионного программного обеспечения с самых первых дней функционирования.

Важно подчеркнуть, что большинство продуктовых решений сохранят свою идентичность и бренд, что позволит заказчикам продолжать работать с привычными им продуктами и решениями такими, как, eToken или HSM Protect Server и другими, причем, естественно, все процессы и сотрудники компании будут продолжать работать в зонах своих ответственностей. Что касается России и стран СНГ, то в этом регионе вся существующая команда продолжает функционировать, как и до объединения.

SN. Что можете сказать о финансовых итогах 1-го кв. 2015 г. и ключевых тенденциях?

С.К. Основные факты за 1-й кв. 2015 г.:

- доход компании составил 686 млн евро, что на 29% выше этого показателя за прошлый год исходя из исторических валютных курсов, или на 19%, исходя из постоянного валютного курса, при этом росту бизнеса способствовало присоединение компании SafeNet;
- рост доходов наблюдался во всех основных сегментах и направлениях.

Ключевые тенденции 2015 г.:

- высокий рост в сегменте платежных решений (Payment), который обусловлен продолжающимся распространением технологии EMV;
- стремительное развитие Интернета вещей, в том числе распространение беспроводных модулей и встраиваемых элементов безопасности (embeddedsecureelements, eSE);
- увеличение спроса на инструменты защиты данных и на решения для кибербезопасности, а также их стандартизация;
- ожидается, что в сегменте мобильных технологий будут по-прежнему наблюдаться колебания, до тех пор, пока в экосистеме бесконтактных платежей не будут приняты новые технологические усовершенствования (TEE, HCE, токенизация), представленные в 2014 г.;
- ускорение роста в сегменте правительственных программ.

Естественно, актуальные тенденции Bring Your Own Device, а также связанные с выходом обновления требований PCI DSS 3.0, по-прежнему будут играть огромную роль в текущих требованиях к системам безопасности и защиты данных.

SN. Что можно сказать о текущей статистике утечек данных? Меняется ли их характер?

С.К. По данным индекса BLI (Breach Level Index – индекс критичности утечек данных) количество утечек данных в 2014 г. выросло на 49%, и в общей сложности за год было скомпрометировано около одного миллиарда записей данных. В 2014 г. основной целью киберпреступников стали персональные данные – 54% от всех инцидентов, что больше, чем в любой другой категории, в том числе больше числа инцидентов с кражей финансовых данных. Чаще всего утечки происходили в розничной торговле и в секторе финансовых услуг. При этом только 58 утечек данных (4% от общего числа) включали данные, которые были частично или полностью зашифрованы.

Изменилась тактика в работе киберпреступников: сиюминутной выгоде от хищения номеров кредитных карт они все чаще предпочитают хищение персональных данных, которые можно будет использовать в течение более продолжительного времени, например, для создания фальшивых учетных данных.

Объем утечек стал измеряться уже сотнями миллионов записей. Наиболее крупные из них:

- *AliExpress*: 300 000 000 – доступ к учетным записям;
- *eBay*: 145 000 000 – хулиганство;
- *Home Depot:* 109 000 000 – финансовая информация;
- *Korean Credit Bureau*: 104 000 000 – идентификационные данные;
- *JPMorgan Chase*: 83 000 000 – идентификационные данные.

Сегодня уже не стоит вопрос: произойдет ли утечка данных? Вопрос заключается в том, когда именно это случится и какой нанесет ущерб. В большинстве случаев системы предотвращения утечек и мониторинг угроз позволяют лишь выявить факт инцидента, но не всегда позволяют его предотвратить. В этих условиях традиционные инструменты (системы обеспечения безопасности по периметру, межсетевые экраны, антивирусные системы) должны стать частью более комплексной стратегии безопасности.

Сегодня уже не стоит вопрос: произойдет ли утечка данных? Вопрос только в том, когда это случится и какой будет ущерб.

Концепция периметра безопасности уже давно перестала быть актуальной в отношении данных: они перемещаются и хранятся в самых различных окружениях с различным уровнем защиты. Все больше пользователей получают доступ к этим данным из различных точек доступа, поэтому организациям следует использовать многоуровневый динамический подход к обеспечению безопасности этих данных. Когда данные попадают в сеть, организации уже не имеют возможности их контролировать, а корпоративные системы предотвращения вторжений или средства антивирусной защиты во внешних сетях уже не работают.

В этих условиях применение технологий безопасности непосредственно в отношении данных, в том числе за счет использования средств многофакторной аутентификации, шифрования данных (что с 2012 г. является уже стандартом всех отраслевых стандартов по безопасности, – *прим. ред.*) и внедрения инструментов безопас-

ного управления ключами шифрования является, по сути, последним рубежом обороны от злоумышленников.

SN. Что можно противопоставить угрозам, связанным с распространением технологии Интернета вещей?

С.К. В основе концепции Интернета вещей лежат программируемые логические контроллеры (Programing Logic Controllers – PLC) – небольшие компьютеры, которые могут быть запрограммированы для управления самыми различными устройствами и оборудованием, но у PLC есть свои слабые места.

Один из способов проникновения в сеть заключается в подписи вредоносного кода с помощью украденного ключа сертифицирующего органа – файлов с данными, содержащих идентификационную информацию, помогающую подтвердить свою подлинность в сети. Маскируясь под доверенный ключ, со временем этот код получает доступ к PLC-системе и причиняет ущерб. Чтобы предотвратить подобные атаки, требуется надежная система безопасности для защиты секретных ключей и сертификатов, которая бы гарантировала подписание только легитимного кода. Именно поэтому в рамках современных стратегий защиты данных необходимо использовать более строгие механизмы доступа, в том числе с многофакторной аутентификацией (multi-factor authentication, MFA) и шифрованием данных.

Аппаратные модули безопасности (hardware security module, HSM) представляют собой специально разработанные устройства для защиты ключей и сертификатов шифрования. Модули HSM – это криптографические устройства, используемые для защиты инфраструктуры организаций за счет шифрования, дешифрования, аутентификации и цифровой подписи сервисов для широкого спектра приложений, в том числе для передаваемых по сети данных.

Механизмы MFA, также известные как двухфакторная аутентификация, позволяют организациям обезопасить доступ к корпоративным сетям, базам данных и приложениям. Принцип работы этой системы заключается в том, что пользователей просят подтвердить свою личность, предоставив одновременно "нечто, что они знают" (пароль или PIN-код) и "нечто, что они имеют" (токен или смарт-карта).

SN. Можно ли привести пример успешного использования двухфакторной аутентификации из последних внедрений?

С.К. Один из таких показательных примеров – внедрение современных средств криптографической защиты на базе продуктов SafeNet в Налоговом комитете Республики Таджикистан.

Чтобы предоставить контрагентам возможность автоматически отправлять различные формы отчетности, было принято решение использовать систему защиты на базе электронных ключей eToken нового поколения. Для этого был создан Центр Сертификации Открытых Ключей при «ГУП ЦПНА» и разработано соглашение по использованию сертифицированных средств криптографической защиты для безопасной передачи данных, используя электронную цифровую подпись вместо физической подписи и печати. В процессе тестирования электронные ключи показали свою надежность и не вызвали никаких проблем у пользователей, сводя к минимуму потребность в технической поддержке.

Теперь для подключения к единой системе документооборота Налогового комитета контрагенты получают токены SafeNet eToken 5100. Переносной двухфакторный USB-аутентификатор обеспечивает безопасный доступ и возможность использования цифровой подписи для отправки документов на одном и том же или на разных устройствах. Инновационный eToken использует сертификаты безопасности для хранения данных, например, закрытых ключей, паролей и цифровых сертификатов в защищенной среде микросхемы смарт-карты. При этом, даже в случае утери, eToken не может быть использован неавторизованным лицом, так как для входа в систему и применения цифровой подписи пользователи должны предоставить свой личный аутентификатор SafeNet и пароль.

В конце 2014 г. Налоговый комитет Республики Таджикистан перешел на обновленные eToken 5200. Эти электронные ключи обладают большей степенью надежности, они универсальны и могут быть использованы на любом устройстве, так как не требуют установки никакого программного обеспечения.

Активным пользователем системы стал один из крупнейших банков Республики Таджикистан – «Государственный Сберегательный Банк «Амонатбонк». В 2014 году «Амонатбонк» перешел на систему электронной передачи информации о платежах, в том числе, поступающих в бюджет. Автоматическая разбивка по ИНН и синхронизация информации о плательщиках повысила прозрачность финансовых потоков и снизила общую нагрузку.

Другим хорошим примером может служить внедрение аутентификации как услуги (Safenet Authentication Service, SAS) для компании “Эльдорадо”. До последнего времени в России и СНГ только физические USB-устройства официально классифицировались как двух- или многофакторная аутентификация. Мне особенно приятно отметить, что система и сервис предоставления одноразовых паролей по требованию набирают популярность. И этому есть ряд причин: у конечного заказчика появляется возможность относить расходы, связанные с аутентификацией, к операционным расходам; есть возможность сконцентрироваться на коренных бизнес процессах, а непрофильный вид деятельности, такой, как безопасность – отдать на аутсорсинг доверенному партнеру или своему специализированному отделу; и, конечно, ряд неоспоримых преимуществ, связанных с возможностью поддержки мобильных устройств, корпоративных и личных, отсутствие необходимости иметь физический токен – достаточно программного, установленного на ваш телефон или планшет, наконец, высочайший уровень автоматизации, масштабирования и простоты внедрения и использования. Можно много спорить, что кому нравится, и кто что выбирает, но, как правило, именно конечные пользователи компаний голосуют моментальным желанием использовать этот инструмент, что увеличивает продуктивность, что само по себе очень редко применимо для систем безопасности. Безопасно – далеко не всегда значит неудобно.

Безопасно – не значит неудобно.

Teradata вложилась в Presto

Июль 2015 г. – Компания Teradata объявила о заключении многолетней программы развития open source-разработки Presto и обеспечении первой в истории отрасли ее коммерческой поддержки. Teradata вложится в open source проект под лицензией Apache®, который обеспечит улучшенные характеристики современной базы кодов Presto, улучшит масштабируемость, итерационные запросы, а также возможность направлять запросы одновременно в несколько репозиториев данных.

Разрабатываемый и используемый Facebook, Presto представляет собой мощный open source-«движок» SQL-запросов следующего поколения, поддерживающий аналитику big data. Растущий интерес к Presto выражается в переходе на его использование ведущими компаниями в своих областях, включая Airbnb, DropBox, Gree, Groupon, а также Netflix.

Presto работает на нескольких Hadoop-дистрибутивах. Кроме того, Presto может непосредственно из Hadoop-платформы отправлять запросы в Cassandra, реляционные базы данных или частные хранилища данных. Эта кросс-платформенная аналитическая характеристика позволяет пользователям Presto извлекать максимум бизнес-ценности из «озер данных» любого размера, исчисляемых гига- или петабайтами.

Предусмотрено три этапа развития Presto.

Этап 1 – Усовершенствование базовых функций, упрощающих ввод Presto, включая инсталляцию, изучение сопроводительной документации, а также базовый мониторинг.

Этап 2 – Интеграция Presto вместе с другими ключевыми компонентами экосистемы big data, такими, как стандартный Hadoop-дистрибутив инструментов управления, операционная совместимость с YARN, а также коннекторы, расширяющие охват функционала Presto за пределы файловой системы Hadoop distributed file system (HDFS). Эти возможности будут доступны в конце 2015 г.

Этап 3 – Запуск архитектуры ODBC (Open Database Connectivity, Открытых средств связи с базами данных) и интерфейса JDBC (Java Database Connectivity API, взаимодействие Java и баз данных по API) для расширения возможностей адаптации Presto организациями и усиления интеграции с инструментами бизнес-аналитики. Улучшенная защищенность за счет доступа по модели распределенных служебных ролей. Эти расширения будут доступны в 2016 г.