PCWEEK RUSSIAN EDITION REVIEW
ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И РЕШЕНИЯ ДЛЯ БИЗНЕСА
ИТ-БЕЗОПАСНОСТЬ
ФЕВРАЛЬ • 2015 • МОСКВА
http://www.pcweek.ru

Российский рынок ИБ: итоги 2014 г. и ближайшие перспективы

ОБЗОР

ВАЛЕРИЙ ВАСИЛЬЕВ

Очень непростой 2014 г. остался позади, и теперь самое время оценить основные события и тенденции, имевшие место на российском рынке информационной безопасности (ИБ), а также обозначившиеся в этой области проблемы, которые предстоит решать в ближайшем будущем. Для этого мы пригласили к участию в данном обзоре экспертов в области ИБ, представляющих как поставщиков ИБ-решений, так и заказчиков.

Наследуемые тренды

Среди тенденций, наметившихся в прошлом году в сфере ИБ, Валентин Крохин выделяет две, на его взгляд, наиболее важные. Первая заключается в том, что проблематика ИБ начала напрямую влиять на бизнес-процессы столь сильно, что и бизнес, и государство стали гораздо внимательнее относиться к ИБ. Как важное проявление этой тенденции, он отмечает начало создания новых центров реагирования на ИБ-инциденты (CERT), в том числе отраслевых, наряду с расширением спектра функций уже существующих при одновременном росте активности регуляторов. Вторую из выделенных г-ном Крохиным тенденций — импортозамещение — единодушно отмечают все наши эксперты.

По мнению Алексея Сабанова, декларированный российскими властями курс на импортозамещение поделил российских разработчиков, использующих в той или иной степени импортные компоненты, на два лагеря: лукавые кричат, что они и сами российские, и делают "чисто" отечественные системы; честные упорно трудятся над созданием продуктовых линеек, содержащих все меньше зависимых от иностранных поставок элементов, а работа эта, как он предполагает, продолжится долгие годы.

Напомним, что импортозамещение — вынужденная мера в ответ на экономические и политические санкции против России со стороны некоторых стран с развитой экономикой. Олег Сафрошкин подчеркивает, что если та или иная российская структура, государственная или частная, попадает в санкционный список, то многие североамериканские и западноевропейские поставщики не смогут с ней работать, что отразится на поддержке и возможности эффективно использовать закупленные продукты. Такая структура также рискует испытать на себе инициацию программно-аппаратных закладок для несанкционированного доступа в корпоративную инфраструктуру.

Санкции, по мнению Павла Головлева, остро обозначили ту проблему, на которую аналитики указывали уже давно: реальные связанные с санкциями риски для бизнеса лежат в плоскости, которая, если и попадает в поле зрения регуляторов, то остается для них все-таки terra incognita в силу бизнесового характера этих рисков. Нужно учитывать, что импортные технологии и продукты слишком сильно проникли в нашу жизнь (а в области ИБ особенно), поскольку у нас никто не занимался на государственном уровне реальной информационной безопасностью, ориентированной на потребности бизнеса.

Большинству специалистов, по мнению Кирилла Мартыненко, сегодня ясно, что некоторые импортные решения и продукты пока просто нечем заменить, однако, как он полагает, можно надеяться, что уже в 2015 г. сложившаяся ситуация приведет к появлению принципиально новых российских разработок.

Вместе с тем Павел Эйгес не склонен считать, что компании, не попавшие в санкционные списки, а таковых подавляющее большинство, оценивают санкционные риски настолько высоко, что готовы направить свои существенно ограниченные в настоящее время ресурсы на превентивное импортозамещение. По его мнению, единственный объективный фактор, подталкивающий российские компании искать сегодня замену некоторым импортным товарам и решениям, — это значительный ценовой рост из-за повышения курса доллара и евро к рублю.

Следующим по важности после стратегии импортозамещения трендом, наследуемым от прошедшего года, Вячеслав Медведев признает рост опыта российского государства в фильтрации Интернета. Он отмечает постепенное понимание со стороны ответственных структур того, что и как нужно фильтровать в Интернете: если на начало 2014 г. фильтрация по сути дела была фикцией (все желающие обходили ее без особых проблем), то к концу года наметился реальный интерес к запрету анонимайзеров, сети TOR и подобных технологий.

Джабраил Матиев считает, что вследствие разоблачений Эдварда Сноудена заметно снизилось доверие пользователей к программному и аппаратному обеспечению. Появился даже специальный термин, характеризующий сегодняшний день как "постсноуденовская эпоха".

Непростая экономическая обстановка в стране, по наблюдениям г-на Сафрошкина, активизировала рынок ИБ-аутсорсинга: сегодня многие компании, по его мнению, всерьез задумываются о возможности передачи части непрофильных для них функций (к которым следует относить и задачи ИБ) на аутсорсинг.

Изменения ландшафта ИБ-угроз

Г-н Сабанов рассматривает прошедший 2014-й как год начала освобождения от иллюзий в оценке общего фона вокруг российских ИБ-разработок, ИБ-услуг и ИБ-регулирования. По его мнению, былого спокойствия и ощущения мира уже нет, и в ближайшее время нам его не вернуть.

В кибервойнах, отмечает г-н Матиев, участвуют спецслужбы противоборствующих стран; кибератаки проводятся на высочайшем технологическом уровне и высококвалифицированными специалистами. Противостоять таким воздействиям самостоятельно отдельные компании просто не в состоянии.

Главные отличия российского ландшафта ИБ-угроз от общемирового г-н Сабанов увязывает с более резко проявленным в нашей стране экономическим кризисом, с принятыми в отношении России экономическими и политическими санкциями, с вынужденными ответными мерами руководства России, в частности упомянутым импортозамещением.

Эксперты отмечают существенное усложнение киберкриминального фона, что выражается, с одной стороны, в увеличении количества сложных таргетированных атак, с другой — широком использовании сложных технологий в массовых атаках. Так, ощутимый ущерб в прошлом году компаниям различного профиля (в основном не ИКТ) принесли вирусы-шифровальщики, которые стали заметно совершеннее; DDOS-атаки продолжали наращивать свою мощь темпами, опережающими возможности методов противодействия.

По словам Павла Эйгеса, рост количества угроз превысил порог "одна новая угроза в секунду", сложность угроз позволяет проводить атаки "ниже уровня радара" большинства корпоративных ИБ-систем. И эти изменения только набирают темп. "Я думаю, что в ближайшие год-два нас ждет уже не количественный, но качественный скачок — переход в реальность Internet of Things (IoT) перевернет наше понимание как самого Интернета, так и безопасности в Интернете", — говорит г-н Эйгес.

Как наиболее распространенные из числа внешних угроз г-н Крохин выделяет рост атак на онлайн-сервисы и мобильные приложения, прежде всего банковские, а из числа внутренних угроз — взрывной рост инсайдерского мошенничества, прежде всего в розничной торговле, по большей части связанный с низкой лояльностью персонала.

К реальным новым угрозам, на которые в России стали обращать внимание, г-н Медведев относит возможность отключения от иностранных ИКТ-сервисов. Он также отмечает, что заметная часть клиентов, использующих локально устанавливаемое ПО, не исключает возможность в условиях санкций перехода на пиратские копии.

Набирающий обороты ИКТ-аутсорсинг, считает г-н Сафрошкин, тоже таит в себе свои риски ИБ: перенос части вычислительной инфраструктуры в арендованный ЦОД или в облако провайдера ставит задачу по защите информации в недоверенной инфраструктуре, а передача обслуживания всей ИКТ-инфраструктуры или отдельных ее компонентов на аутсорсинг предполагает налаживание контроля системных администраторов аутсорсера.

По мнению г-на Головлева, виды ИБ-угроз не меняются, и новые техники атак появляются редко. Зато меняются способы реализации угроз, и, конечно, сами компании меняются, очень часто подставляя под угрозу образующиеся в ходе изменений незащищенные места. Поэтому он призывает всегда видеть за неким общим ландшафтом ИБ-угроз те конкретные угрозы, которые актуальны для данной конкретной структуры, строить свои модели угроз, свои стратегии и тактики защиты. Например, предупреждает он, в наступившем году много людей сменит место работы, а это повлечет за собой увеличение числа утечек информации, снижение уровня защиты и увеличение числа сбоев и ошибок, и к этому следует подготовиться.

Наши эксперты

СЕРГЕЙ ВОРОНЕЦКИЙ, *главный эксперт отдела информационной безопасности управления службы безопасности RU-CENTER Group, эксперт ассоциации BISA*

ПАВЕЛ ГОЛОВЛЕВ, *начальник управления безопасности информационных технологий банка "СМП Банк", эксперт ассоциации BISA*

ВАЛЕНТИН КРОХИН, *заместитель директора Центра информационной безопасности компании "Инфосистемы Джет"*

КИРИЛЛ МАРТЫНЕНКО, *эксперт ассоциации BISA*

ДЖАБРАИЛ МАТИЕВ, *руководитель отдела информационной безопасности компании IBS Platformix*

ВЯЧЕСЛАВ МЕДВЕДЕВ, *ведущий аналитик отдела развития компании "Доктор Веб"*

АЛЕКСЕЙ САБАНОВ, *заместитель генерального директора компании "Аладдин Р.Д."*

ОЛЕГ САФРОШКИН, *менеджер по развитию бизнеса компании "Информзащита"*

ПАВЕЛ ЭЙГЕС, *региональный директор McAfee в России и СНГ*

"К нашему бизнесу в России мы можем подходить без ссылок на кризис"

Прошедший год ознаменовался значительными изменениями в общемировом ландшафте ИБ-угроз, обусловленными, с одной стороны, все более очевидным переводом ИКТ-ресурсов на облачную платформу, а с другой — существенным усложнением самих ИБ-угроз. В России все это сопровождалось еще и резким усложнением общей политико-экономической ситуации.

О том, как отвечает на новые вызовы McAfee/Intel Security, подразделение ИБ корпорации Intel, рассказал региональный директор McAfee в России и СНГ ***Павел Эйгес****.*

Павел Эйгес

Прошлый год преподнес немало сюрпризов, негативно сказавшихся на российском ИТ-рынке, включая ИБ-сегмент. Как Intel Security будет работать в условиях кризиса? Какие задачи ставит перед собой?

В новых реалиях региональный офис не ставит перед собой никаких особенных антикризисных задач. Мы смотрим вперед с умеренным оптимизмом и тому есть ряд причин. Во-первых, 2014-й стал очередным годом увеличения продаж McAfee в России. Во-вторых, с момента открытия российского регионального офиса McAfee в 2008 г. прайс-лист компании для местного рынка номинирован в рублях, поэтому наши заказчики и партнеры защищены от любых валютных рисков. Да, в феврале нынешнего года мы скорректировали прайс-лист (впервые с 2011 г.), но если сравнить наши текущие цены с прошлогодними в долларовом эквиваленте, то можно увидеть, что они существенно снизились. В-третьих, очевиден растущий интерес к нашим комплексным высокоинтегрированным ИБ-решениям, позволяющим заказчикам не только сократить общую стоимость владения ими (TCO), но и построить гораздо более управляемую и надежную систему ИБ. Мы предлагаем такие решения в мире и в России на протяжении уже ряда лет в рамках парадигмы Security Connected, которую продолжаем развивать.

Все это, на мой взгляд, позволяет нам подходить к нашему бизнесу без ссылок на кризисное состояние экономики. Более того, по результатам января и февраля 2015 г. мы уже видим существенный рост продаж в сравнении с тем же периодом прошлого года.

В российской экономике декларирован курс на импортозамещение, в том числе в ИТ-сфере. Что это означает для вашей компании и как может отразиться на ее бизнесе?

Позвольте задать встречный вопрос: кем декларирован? Да, в публичном пространстве мы видим информационное давление в этом направлении, но никаких законодательных инициатив пока нет и, учитывая членство России в ВТО, мы вряд ли их увидим в ближайшее время.

Возвращаясь к вопросу, думаю, следует выделить два его аспекта. Первый — это наличие экономических запретительных санкций, наложенных Европой и США на очень небольшой список российских компаний. Естественно, те, кто попал в этот список, вынуждены искать замену продуктам и решениям, которые они ранее закупали у европейских или американских поставщиков. Остальные компании никаких санкционных ограничений не испытывают. И я не думаю, что в этих компаниях оценивают санкционные риски настолько высоко, что направляют свои существенно ограниченные в настоящее время ресурсы на превентивное импортозамещение. Единственный объективный фактор, подталкивающий российские компании искать сегодня замену некоторым импортным товарам и решениям, — это значительный ценовой рост из-за повышения курса доллара и евро к рублю. Как я уже отмечал выше, в случае с McAfee этот фактор минимизирован.

В связи с изменением ландшафта ИБ-угроз меняются и требования к средствам защиты. Как в связи с этим будет развиваться продуктовый портфель компании? На чем вы сфокусируетесь?

Вы абсолютно правы — ландшафт угроз в последний год существенно изменился: рост количества угроз превысил порог "одна новая угроза в секунду", сложность угроз позволяет проводить атаки "ниже уровня радара" большинства корпоративных ИБ-систем. И, что важно, эти изменения только набирают темп. Я думаю, что в ближайшие год-два нас ждет уже не количественный, но качественный скачок — переход в реальность Internet of Things (IoT) перевернет наше понимание как самого Интернета, так и безопасности в Интернете.

Предвидя этот тренд, McAfee уже много лет продвигает свою парадигму объединённой безопасности — Security Connected. Согласно этой парадигме на смену эшелонированной обороне приходит понятие "контекстно-связанной защиты". Реализуемые по такому принципу системы гораздо более информативны, существенно быстрее оповещают об атаке и позволяют гораздо более адекватно и быстро отреагировать на атаку. Весьма важно и то, что такие решения обходятся намного дешевле.

В прошлом году мы представили рынку шину обмена контекстами угроз — McAfee Threat Intelligence Exchange, которая сокращает время реакции на атаку до нескольких миллисекунд за счет интеграции аппаратной "песочницы" McAfee Advanced Threat Defense с инфраструктурой защиты конечных точек под управлением McAfee ePO. Еще до наступления IoT-эры нас ждет революция и в области защиты конечных точек, которую несут нам решения класса Security on Chip.

Претендующий на использование в серьезных проектах ИБ-продукт должен соответствовать определенным нормативным требованиям. Как идет процесс сертификации ваших продуктов в России?

Мы всегда подходили к этому процессу очень серьезно, проводя ежегодно сертификацию нескольких модулей нашей платформы. Сейчас мы предлагаем рынку сертифицированные решения сетевой и контекстной защиты, заканчивается сертификация "песочницы", на подписании во ФСТЭК сертификат на McAfee SIEM, который задержался по причине проведения дополнительного анализа кода. Нельзя не упомянуть сертификацию McAfee NGFW, которую мы начали после окончания технологического поглощения продуктовой линейки StoneSoft, весьма популярной в России.

Какие из ваших решений наиболее популярны у российских заказчиков? Какие проекты на их основе из числа недавних вы считаете наиболее интересными?

Возможно, это кого-нибудь удивит, но в нашем обороте в России и СНГ антивирусы составляют не более 25%. Остальное — это сетевая безопасность (межсетевые экраны и системы обнаружения вторжений), на которые приходится немногим более 50% всех продаж, остальное — это системы контентной фильтрации, к которым я отношу кроме Web- и email-шлюзов также решения DLP и SIEM. Очень сложно выделить какой-то один продукт, так как в большинстве случаев наши проекты реализуются на основе трех и более продуктов. Тем не менее могу назвать несколько хитов прошлого года: McAfee IPS в связке с McAfee SIEM и ATD, McAfee Web/email Gateway в связке с ATD и, конечно, McAfee NGFW.

Г-н Мартыненко отмечает технологическое усложнение атак на банкоматы. От физического взлома и кражи денежных средств, как из сейфов, злоумышленники перешли к использованию высокоразвитых вредоносных программ, которые доставляются до цели в том числе и при помощи сотрудников сервисных компаний, обслуживающих банкоматы. Согласно его наблюдениям, в разы увеличилось количество попыток мошенничества, связанного с интернет-платежами. Тренд при этом остался прежний — все чаще атаке подвергаются юридические, а не физические лица, что связано с объемом денежных средств, на которые нацеливаются мошенники.

В силу специфики таргетированных атак универсального решения для защиты от них не существует. Поэтому, как заметил г-н Матиев, повысилось значение комплексного аналитического подхода к защите информации, интерес к таким решениям, как SIEM. Из-за роста числа утечек данных по-прежнему в тренде, по его мнению, решения класса DLP. Распространение облачных технологий актуализирует спрос на решения по защите виртуализированных сред.

Регулирование ИБ-рынка в 2014 г.

Действия регуляторов в области ИБ всегда были острой проблемой для участников ИБ-рынка — одни ждали новаций от регуляторов с большой настороженностью, опасаясь помех в налаженных процессах, другие — как света путеводной звезды во тьме непонятных угроз, третьи — как возможности решить ИБ-задачи формальным соответствием.

Ситуация, однако, как отмечают эксперты, меняется к лучшему. По мнению г-на Крохина, регуляторы в 2014 г. дали участникам ИБ-рынка надежду на то, что их деятельность направлена на решение реальных проблем отрасли. Планы регуляторов по выпуску документов и изменению регламентов показывают, что качество работы регуляторов растет и можно ожидать появления действительно полезных документов.

Утверждая, что в сфере регулирования ИБ сегодня доминируют два закона — "Об электронной подписи" (63-ФЗ) и "О защите персональных данных" (152-ФЗ), г-н Сабанов отмечает, что подзаконные акты к ним становятся все более проработанными и реалистичными. В немалой мере этому, как он считает, способствует то, что регуляторы стали чаще советоваться с участниками рынка.

Положительные процессы, развивающиеся во ФСТЭК России, благодаря которым эта служба становится все более динамичной и соответствующей современным реалиям, отмечает г-н Головлев.

Иллюзии возможности кулуарного сотворения необходимых рынку документов и рекомендаций, надеется г-н Сабанов, канули в Лету. Сегодняшняя обстановка должна, полагает он, сплотить всех основных участников рынка. Если регуляторы, крупные заказчики, разработчики и поставщики сплотятся и начнут сообща конструктивно вырабатывать необходимые для регулирования рынка документы, это будет сплав, подобный дамасской стали, считает он.

Проработанность и законченность, по мнению г-на Сабанова, наиболее видны в документах, относящихся к закону "О персональных данных". Что же касается давно назревших изменений в 63-ФЗ, то, по его словам, они готовятся, но пока обсуждаемые проекты изменений не отвечают в полной мере требованиям сегодняшнего дня. В частности, по-прежнему не уделяется должного внимания регулированию назревших проблем безопасной организации процессов идентификации и аутентификации участников удалённого электронного взаимодействия, по-прежнему игнорируется задача использования устройств, безопасно генерирующих закрытые ключи, так называемых устройств с неизвлекаемыми закрытыми ключами. Несмотря на то что такие устройства были рекомендованы соответствующей директивой использования электронной подписи ещё в 1999 г., а в принятом в 2014-м положении ЕС 910/2014 закреплены в качестве необходимого условия доверенного применения квалифицированной электронной подписи, у нас продолжается игнорирование таких устройств.

В ряду наиболее актуальных вопросов, ждущих своих ответов, кроме упомянутых г-н Сабанов называет обеспечение юридической значимости электронных документов, интероперабельность средств электронной подписи (не только в части ее создания, но и в части проверки), создание пространства доверия к электронным документам с правовыми последствиями, регулирование безопасности облачных вычислений…

Курс на импортозамещение и введение в действие закона о запрете обработки персональных данных (ПДн) граждан РФ за пределами страны (ФЗ РФ от 21 июля 2014 г. № 242-ФЗ), отмечает г-н Матиев, вызвали в сообществе специалистов оживленные дискуссии о возможности их реализации. Определенные трудности исполнения вызывает прежде всего неоднозначность его трактовки различными участниками рынка, а также недостаточное количество времени для его исполнения: требование о необходимости хранения ПДн в пределах Российской Федерации вступает в действие с 1 сентября 2015 г.

Сергей Воронецкий называет закон № 242-ФЗ "темной лошадкой", поскольку сложно оценить, каким будет его реальное исполнение, в том числе и в части контроля исполнения, и как он отразится на бизнесе различных компаний.

С технологической точки зрения в 2015 г. самым сложным в следовании стратегии импортозамещения, по мнению г-на Матиева, будет подбор аналогов иностранным решениям. Он отмечает, что к таким резким перестройкам готовы не все сегменты рынка. Поэтому (в зависимости от изменения политической ситуации в стране) можно предполагать принятие каких-нибудь дополнительных мер и регуляторных решений относительно использования нероссийских средств защиты.

Немаловажное значение для рынка ИБ, отмечает г-н Матиев, имел выход в свет приказа ФСТЭК России от 14 марта 2014 г. № 31 "Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды".

Для банков, по мнению г-на Мартыненко, одним из важнейших событий года стал выход обновленной редакции стандарта Банка России СТО БР ИББС. По его оценкам, документ стал более структурированным и теперь, по сути выполняя требования только этого стандарта, любой российский банк уже будет иметь достойную систему ИБ.

Г-н Мартыненко обращает внимание на то, что один из разделов стандарта посвящен требованиям к наличию функционала DLP (напрямую класс систем в стандарте не указан, что отрадно). Он считает, что Банк России тем самым

ПРОДОЛЖЕНИЕ НА С. 12 ▸

Крепко ли вы спите?

ВЯЧЕСЛАВ МЕДВЕДЕВ, ВЕДУЩИЙ АНАЛИТИК ОТДЕЛА РАЗВИТИЯ КОМПАНИИ "ДОКТОР ВЕБ"

Проблема безопасности всегда была актуальной — для компаний, государства в целом, да и для отдельных пользователей. Проводятся семинары, выпускаются стандарты и приказы, принимаются дорожные карты… Количество сообщений о доходах злоумышленников вызывает зависть у простых работников, сравнивших свои зарплаты с расходами после очередного новогоднего подорожания.

Но в итоге все остается в общем-то без особых изменений. В подавляющем большинстве компаний на обычных компьютерах и важных серверах в качестве защиты стоит "просто" антивирус, отвечающий на все вызовы угроз безопасности, как последний герой. Чего вы хотели? Кризис.

А в это время темная сторона гибко реагирует на вызовы времени. Одни злоумышленники, ощутив падение платежеспособного спроса, поднимают расценки на расшифровку заблокированной информации до 1500 евро (в классификации Dr.Web — Trojan.Encoder.686), другие, поняв, что "пора валить", используют для этого компьютеры жертв (www.anti-malware.ru/news/2015—02-02/15453), третьи ищут места, где еще отсутствуют вирусы и троянцы конкурирующих криминальных группировок.

Естественно, большинство хакеров в поисках хлебных мест еще и еще раз перелопачивают в поисках уязвимостей ОС Windows и приложения, созданные для этой популярной системы. Но есть и первопроходцы Интернета вещей.

В ходе анализа 752 различных устройств, поддерживающих низкоуровневый протокол HART, было обнаружено 29 уязвимостей в компонентах порядка 500 устройств. — www.anti-malware.ru/news/2014—12-02/15107

Вирус можно передать и через электронные сигареты. — www.securitylab.ru/news/462249.php

Были проверены все USB-контроллеры восьми крупнейших мировых производителей: Phison, Alcor, Renesas, ASmedia, Genesys Logic, FTDI, Cypress и Microchip. Хорошая новость в том, что около половины устройств не имеют уязвимостей. Плохая новость: вы не можете сказать, какая конкретно половина. — http://xakep.ru/badusb-v-raznyh-kontrollerah

1800 доменов взломано в результате эксплуатации уязвимости нулевого дня в Adobe Flash Player. — http://blogs.cisco.com/talos/angler-variants

Установив нужное оборудование, можно "видеть" устройства, которые были просто в зоне действия Wi-Fi точки доступа, — даже не подключались к ней. Публичные хотспоты в метро, магазинах и аэропортах — кто контролирует мир? — http://geek-times.ru/post/242979

Кого боятся американские адмиралы? Русских медведей? Исламских террористов?

Начальник отдела морских систем вооружений (NAVSEA) ВМС США вице-адмирал Уильям Хиларайдс заявил, что подлодки типа Virginia уязвимы для кибератак. — http://news.usni.org/2014/10/22/navsea-submarines-control-systems-risk-cyber-attack

"Главная внутренняя угроза, — по словам адмирала, это моряк, который ищет, куда бы подключить свой мобильник и кинуть СМС-ку жене". Ну или незаблокированный USB-порт. — http://breakingdefense.com/2014/10/set-set-cyber-zebra-navy-shipboard-cybersecurity

Но все это пока поиски и концепты. 2014 год ознаменован обнаружением уязвимостей в Linux и появлением значительного — по меркам прошедших лет — количества вредоносных программ для этой ОС, интересом злоумышленников к банкам, системам здравоохранения.

Мир злоумышленников продолжает коммерциализироваться. Началось сращивание киберпреступности и терроризма. Мир стремительно виртуализируется, но его безопасность при этом становится все более хрупкой. Повсеместное понижение уровня понимания "а как это работает" и слепая надежда на новейшие технологии — это страшно. Тем более для людей, которые должны быть уверены в своей безопасности и безопасности тех, за кого они отвечают.

Сколько было надежд на сеть Tor! Но злоумышленники просто регистрировали серверы Tor и инфицировали проходящие файлы, а затем:

Томас Уайт предупредил сообщество о потере контроля над своей серверной инфраструктурой и блокировке учётной записи хостинг-провайдером. Непосредственно перед инцидентом было зафиксировано подключение к серверам неизвестного USB-устройства и открытие корпуса серверов. — http://permalink.gmane.org/gmane.network.tor.user/34619

Кто-то еще полагается на гарантированную защиту данных от любых угроз, если эти данные размещены в облаках?

Прошедший год был отмечен победными атаками шифровальщиков, миллиардными утечками, обнаружением зияющих дыр в ПО — и отказами по их закрытию. Часть пользователей впечатлилась. Но ведь есть еще места, где люди буквально просят прислать им немного вирусов!

"Уже неоднократно говорил — живу без антивирусов примерно с 2002 года. Полёт нормальный. Давно пришло время понять, что все эти „антивирусы" — относительно нечестный способ отъёма денег у малограмотного населения. Любой „антивирус" — ухудшение безопасности (если интересно — поясню)".

Это цитата с одного из форумов. Мнение достаточно популярное, поэтому ссылку не указываем.

Но время идет и

"ма-ма! ☹ кто сталкивался с таким шифровальщиком?"

"П…но тысячи файлов в папках. Первая эпидемия у меня за последние лет 8. Я в неадекватном состоянии, это просто ужас..."

Цитата с того же форума. Причем, судя по обсуждениям, выясняется, что даже если защита и была, то она состояла исключительно из антивируса.

Напуганные статистикой и движимые государственной необходимостью регуляторы всего мира выпускают приказы и разрабатывают стандарты. Ознакомившись с ними и впечатлившись стоимостью и сложностью выполнения требований, потенциальные жертвы атак выстраивают бумажные стены отчетов о своей готовности к бою с любой нечистью.

Гром гремит, но современный мужик даже не собирается креститься. И, к сожалению, данный прогноз сбудется со стопроцентной вероятностью.

В свое время NASA предложило всем желающим поучаствовать в определении задач для марсохода — и было вынуждено закрыть эту инициативу, поскольку большинство хотело устроить "гонки смерти" — загнать марсоход в дюны и посмотреть, что получится. Дальше — больше. Korea Electric Power Corporation, управляющая 23 ядерными реакторами, рекомендовала местным жителям не приближаться к месторасположениям данных АЭС в ближайшие несколько месяцев в связи со взломом неизвестным хакером информационной сети.

PS. Есть подозрение, что когда на Марс проникнет жизнь, то вирусы и там появятся первыми.

PPS. И по результатам расследования инцидента окажется, что на системе защиты решили сэкономить, посчитав, что уж куда-куда, а на Марс вирус не проникнет — там же работают только профессионалы.

Российский...

ПРОДОЛЖЕНИЕ СО С. 11

закрепил один из трендов 2014 г. — активизацию борьбы с утечками данных, количество и ущербы от которых заметно возросли.

Вступление с 16 марта 2015 г. в силу требований обновленного положения 382-П Банка России, полагает г-н Мартыненко, безусловно повлияет на некоторые критичные бизнес-процессы банков, и банки уже сейчас должны быть к этому готовы. В первую очередь это запрет на эмиссию расчетных и кредитных карт, содержащих только магнитную полосу: после 1 июля 2015 г. все карты должны содержать микропроцессор. Обновленный пункт 2.3 положения 382-П потребует применения в банках систем предотвращения мошенничества.

Существенным минусом, по мнению г-на Медведева, стало изменение правил сертификации продуктов безопасности. Если раньше заявитель указывал лишь системные требования, и сертифицированные продукты в результате могли защищать любое ПО, подпадающее под них, то теперь нужно указывать конкретные операционные системы, на которые защита распространяется. Получается, что сертификация средств защиты для ОС Windows 20xx и Windows 20xx R2 теперь оплачивается отдельно, так же как и под варианты поставки (Standard, Enterprise…).

С учетом того, что сертификация под каждую такую версию ОС стоит отдельных денег, компании-заявители не могут предоставить своим клиентам защиту под все используемые ими программные платформы из-за выходящей за рамки разумного стоимости сертификации. К тому же сертификации длятся не менее чем по полгода (а обычно и долее), и к моменту получения сертификата новая версия средства защиты не может быть использована для защиты новейших систем.

Прогнозы изменений

Эксперты ожидают как неизбежности сокращения ИБ-бюджетов, уменьшения объемов или замораживания закупок ИБ-продуктов и проектов по развитию и модернизации систем ИБ, фокусирования заказчиков на поддержании уже существующих систем защиты.

Одновременно эксперты довольно оптимистичны в общей оценке уровня ИБ российских компаний, хотя, считает г-н Воронецкий, их готовность противостоять актуальным ИБ-угрозам будет ниже, чем в предыдущие годы (возможно, исключением станут представители ИКТ- и финансового сегментов). Причины этого снижения, по его мнению, заключаются в том, что у нас по-прежнему не принято заниматься системным анализом рисков ИБ (вместо этого практикуется традиционный подход, выражающийся в обеспечении базового уровня безопасности плюс проведение ИБ-мероприятий, зависящих от специфики конкретных бизнес-систем), а также в том, что инвестиционный подход финансирования ИБ все еще непопулярен в стране.

Оценивая готовность российских компаний противостоять современным угрозам, г-н Крохин отмечает сильную неоднородность в различных сегментах корпоративной ИБ: в сфере "классической" инфраструктурной ИБ (VPN, межсетевые экраны, антивирусная защита шлюзов и конечных точек и т. п.) дела обстоят относительно хорошо; несколько хуже ситуация в части защиты веб-сервисов и мобильных приложений; совсем плохо положение с безопасностью при реализации программ BYOD — компании еще не осознали всю степень угроз этого направления; низкая ИБ-готовность в АСУ ТП (и эта проблема только усугубляется).

В банковском секторе, по мнению г-на Мартыненко, необходимо будет заниматься развитием функционала DLP и предотвращением мошенничества (в русле выполнения требований новой редакции отраслевого стандарта), развивать направление защиты банкоматов и платежных терминалов (чтобы снизить ущербы от явно участившихся атак на эти устройства) и, конечно, строить защиту от таргетированных атак (как главного общего современного ИБ-зла).

По мнению г-на Воронецкого вряд ли в ближайшее время появятся технологии, способные резко изменить положение дел в области ИБ. Однако он уже сейчас готов предложить разработчикам направление для поиска технологических ИБ-новаций: по его мнению, сегодня очень не хватает мощных, желательно распределенных средств борьбы с DDOS-атаками.

Г-н Крохин считает, что ожидания скорейших улучшений в защите от DDoS-атак в наступившем году небеспочвенны. Он также предполагает, что произойдут позитивные изменения в области автоматизации процессов расследований инцидентов, в расширении функционалов Web Application Firewall и "песочниц". Произойдет резкий скачок в развитии отечественных средств ИБ в целом, в том числе и по показателям качества функционирования.

Из актуальных технологических проблем помимо тех, на которые указывают другие эксперты, г-н Сабанов выделяет ИБ-задачи, порожденные реальным переходом к облачным вычислениям, проблемы обеспечения ИБ в классе решений "умные вещи и сооружения" и при применении 3D-принтеров.

По мнению г-на Сабанова, пришло время сосредоточиться на проблемах совместимости и интероперабельности создаваемых систем защиты информации, для чего, считает он, придётся внести некоторые изменения в статус стандартов. Сегодня, напоминает он, российские стандарты, согласно закону "О техническом регулировании" (184-ФЗ), носят необязательный характер и, видимо, пришло время пересмотреть это положение.

Главные же проблемы в области ИБ, отмечает г-н Головлев, связаны не с технологиями, а по-прежнему с людьми. Он советует вендорам и интеграторам спуститься с небес на землю и помогать заказчикам и клиентам решать конкретные практические задачи за адекватные деньги.

Подавляющее число российских компаний, согласно наблюдениям г-на Медведева, имеют слабое представление о современных ИБ-угрозах, а также о том, как от них защищаться. Так, большинство из них до сих пор уверено, что проблему пропуска вирусов всегда можно решить заменой одного антивируса на другой. Поэтому более важной, чем технологические, он считает проблему информирования.

С учетом того, что в России так и не созданы национальные центры анализа угроз и информирования о них, мало вероятно повышение уровня информированности, в том числе (к большому сожалению) и лиц, принимающих решения, о современных угрозах и методах защиты от них, считает г-н Медведев. Поэтому, увы, российские компании будут защищаться привычными (читай, консервативными) методами даже там, где можно существенно сократить расходы, изменив схему защиты.