Информационная безопасность конечных точек: состояние и тенденции

ВАЛЕРИЙ ВАСИЛЬЕВ

ОБЗОРЫ

Построение корпоративной системы информационной безопасности (ИБ) начинается с обеспечения защиты конечных точек от вредоносных программ, сетевых атак, несанкционированного доступа, кражи данных. Однако виртуализация серверов и рабочих мест, распространение мобильного доступа к ИКТ-инфраструктуре, сервисная модель потребления ИКТ-ресурсов заставляют ИБ-специалистов разрабатывать и использовать новые технологии защиты вычислительной инфраструктуры и устройств доступа к ней.

Усложнение ИБ-задач в связи с усложнением ландшафта ИБ-угроз, в свою очередь, требует комплексного подхода к обеспечению ИБ, что ведет к расширению спектра методов и средств, применяемых для защиты конечных точек, нелинейному росту объема информации, поступающей от ИБ-устройств и решений, использованию аналитических инструментов в обработке этой информации для выявления ИБ-инцидентов и ускорения реагирования на них, повышению требований к эргономике инструментов управления средствами защиты информации (СЗИ).

В нашем тематическом обзоре мы постарались дать оценку того, как изменения, происходящие в настоящее время в самой ИКТ-инфраструктуре и в способах атак на нее, влияют на подходы к построению защиты конечных точек. Для этого мы обратились к экспертам из компаний, разрабатывающих и внедряющих современные СЗИ и давно представленных на российском рынке ИБ.

Факторы влияния

По мнению менеджера по развитию бизнеса "Лаборатории Касперского" Кирилла Керценбаума, сложно найти обстоятельства, которые бы не оказывали прямого или косвенного влияния на качество и уровень обеспечения ИБ рабочих станций и серверов. В частности, озабоченность специалистов вызывает распространение так называемых таргетированных атак (APT). Г-н Керценбаум считает, что именно рост числа APT-атак вернул задачу защиты конечных точек в разряд первоочередных в стратегии обеспечения корпоративной ИБ после не столь давнего смещения фокуса корпоративной ИБ на периметр сети с целью высвобождения ресурсов конечных точек для повышения эффективности отработки основных бизнес-процессов.

Актуальность и сложность защиты конечных точек, по мнению руководителя направления инфраструктурных ИБ-решений Центра информационной безопасности компании "Инфосистемы Джет" Юрия Черкаса, усугубляется тем, что именно конечные точки все чаще выбираются первичными целями атак злоумышленников. "Если говорить о рабочих станциях, то к уязвимостям работающего на них прикладного и системного ПО добавляется человеческий фактор: попадаясь на приемы социальной инженерии, пользователи облегчают работу злоумышленникам, запуская зараженные файлы или переходя по подложным ссылкам на зараженные ресурсы Интернета", — поясняет он.

Высокие риски утечек и повреждения конфиденциальной информации (ведь на конечных точках ведется обработка большого объема данных), в том числе в связи с влиянием человеческого фактора, обусловливает, как отмечает менеджер по продукту компании "Код безопасности" Иван Бойцов, и соответствующее внимание регуляторов к ИБ конечных точек. В результате их требования к защите автоматизированных рабочих мест и серверов постоянно повышаются. Ответом на "закручивание гаек" со стороны регулятора, по словам заместителя генерального директора компании "Аладдин Р.Д." Алексея Сабанова, стал переход на сертифицированные СЗИ.

Вместе с тем архитектор по информационной безопасности ГК "Компьюлинк" Виталий Гончаров считает, что влияние регуляторного фактора на рынок ИБ снижается: "Поутихли, например, страсти по поводу соблюдения требований закона "О персональных данных", и сегодня при выборе СЗИ мы часто видим, что вместо соответствия требованиям регуляторов заказчик оценивает их общий функционал, возможность централизованного управления, простоту интеграции в существующую ИТ-инфраструктуру".

Последствия политики импортозамещения наряду с современными экономическими тенденциями г-н Гончар относит к ограничивающим факторам при выборе средств защиты конечных точек: импортозамещение привело к уходу некоторых иностранных ИБ-вендоров с российского рынка и тем самым сузило выбор СЗИ, а изменения в экономике вынуждают российские компании оптимизировать расходы на ИБ и откладывать модернизацию ИБ (когда это возможно) до лучших времен.

Однако, по мнению г-на Сабанова, применительно к выбору СЗИ импортозамещение не очень актуально — иностранных и чисто российских сертифицированных СЗИ, как он считает, на нашем рынке ИБ всегда было и использовалось больше, чем несертифицированных. В то же время он отмечает негативные сдвиги под давлением политики импортозамещения в ландшафте системного ПО: "В отдельных случаях удивляет переход с полнофункционального сертифицированного по требованиям ФСБ РФ системного ПО (например, компании Microsoft) на дорогой и малофункциональный продукт из разряда так называемого свободного ПО или переход с удобных и развитых СУБД (в частности, компании Oracle) на, скажем, Postgres, которая, кстати, родом из Калифорнийского университета США и в отличие от сертифицированных версий СУБД Oracle пока тщательно не проверена на закладки. Если нужно "ехать", а не демонстрировать "шашечки", то можно надежно защитить данные и на тех СУБД, которые давно используются в нашей стране".

По мнению г-на Сабанова, наиболее существенное влияние на защищенность конечных точек оказывают технологии тотальной слежки (включая аппаратные закладки), Big Data и средства виртуализации:. "Риски влияния этих технологических факторов на порядок выше рисков использования системного и прикладного ПО. И пока у нас не появится отечественная доверенная аппаратная база для серверных и клиентских мест, разговоры об их безопасности ни к чему не приведут".

По мнению руководителя направления ИБ-аналитики компании RedSys Александра Бодрика, нынешнее состояние ИТ напоминает "золотой" век пиратства в Карибском море. Он отмечает, что старая парадигма корпоративных ИКТ-инфраструктур превращается из "звезды" "один-ко-многим" (где центр "звезды" — ЦОД) в паутину "многие-ко-многим", где конечные точки ("корабли") обращаются к миксу облачных сервисов ("островов"). Некоторые средние и малые компании, по его наблюдениям, вообще не имеют собственной инфраструктуры — все сервисы они берут из облаков провайдеров, а конечные точки их работники приносят с собой.

Развивая эту мысль, г-н Бодрик говорит: "Киберпреступность ("корсары") через Интернет ("море") имеет возможность напасть на любой "остров" и активно атакует "богатые острова" — банки и платежные системы. Так, в результате только одного взлома платежной системы "Рапида" было похищено 171 млн. руб., а о скольких взломах мы не знаем? В то же время кроме беспечных торговых "кораблей" и "островов" мы видим сверхзащищённые "крепости" критически важных инфраструктур банков, телеком-структур, нефтегазовых компаний".

В терминологии г-на Бодрика, безопасность торговых "островов" концентрируется вокруг проверки безопасности конечных точек, при этом активно применяются разнообразные облачные ИБ-сервисы. В безопасности "крепостей" используются традиционные методы эшелонированной обороны, многоуровневые предварительные проверки всех возможных сущностей — пользователей, трафика, веб-ссылок, электронной почты, анализ поведения пользователей и выявление аномалий.

Общие подходы к обеспечению ИБ сегодня

Как полагает г-н Сабанов, общим подходом к защите конечных точек, как и прежде, остается анализ рисков: проверенный практикой и рекомендованный международными и отечественными стандартами этот подход является краеугольным камнем создания качественных систем защиты.

В связи с экономическими реалиями и ростом числа APT-атак для обеспечения ИБ конечных точек, полагает г-н Гончар, необходимо использовать системный подход, позволяющий повысить эффективность СЗИ.

Он предлагает рассматривать четыре этапа жизненного цикла обеспечения ИБ конечных точек:

настройку — на данном этапе необходимо заранее настроить конечные точки, чтобы уменьшить потенциальную область атак злоумышленников. Технические меры здесь могут включать анализ уязвимостей, настройку, установку патчей, контроль приложений;

предотвращение — этот этап характеризуется использованием СЗИ для конечных точек в реальном времени, чтобы различными методами идентифицировать и фильтровать вредоносные программы;

обнаружение — цель этого этапа состоит в том, чтобы обнаружить аномалии, которые указывают на нарушение ИБ в конечной точке. Ключевая задача — быстро обнаружить угрозы, сократив время их воздействия, если их просмотрели на этапе предотвращения. Дополнительно методы обнаружения предоставляют информацию для восстановления систем и последующего анализа произошедшего;

исправление — этот этап нацелен на восстановление систем после инцидента и его анализ, результаты которого будут использованы для необходимых изменений на этапе настройки.

Как только появляются новые угрозы, отмечает г-н Бойцов, разрабатываются новые СЗИ, в том числе предназначенные для защиты конечных точек. Порой это приводит к тому, что рабочие станции нагружаются различными средствами защиты, число которых может достигать десятка. Нередко конфликтуя между собой, каждое из них активно потребляет ресурсы конечной точки.

В последние годы, по наблюдениям г-на Бойцова, приоритеты ИБ-специалистов смещаются в сторону сокращения количества СЗИ для защиты конечных точек (разумеется, без снижения уровня защищенности): чаще применяются комплексные продукты, в которых реализуется сразу несколько защитных механизмов. Такой подход снижает нагрузку на конечные точки, позволяет оперативно реагировать на угрозы, упрощает мониторинг и управление системой защиты.

Как отмечает г-н Керценбаум, все больше внимания уделяется способности ИБ-решений выявлять признаки активных заражений, поведенческому анализу, ▸

Наши эксперты

АЛЕКСАНДР БОДРИК, *руководитель направления ИБ-аналитики, RedSys*

ИВАН БОЙЦОВ, *менеджер по продукту, "Код безопасности"*

СЕРГЕЙ ВАХОНИН, *директор по решениям, "Смарт Лайн Инк"*

ВИТАЛИЙ ГОНЧАР, *архитектор по информационной безопасности, ГК "Компьюлинк"*

КИРИЛЛ КЕРЦЕНБАУМ, *менеджер по развитию бизнеса, "Лаборатория Касперского"*

ИВАН МЕЛЕХИН, *технический директор, "Информзащита"*

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

ЮРИЙ ЧЕРКАС, *руководитель направления инфраструктурных ИБ-решений Центра информационной безопасности, "Инфосистемы Джет"*

защите конкретных ресурсов и данных: “Мы можем говорить не только о приоритетном внимании к защите рабочих станций и серверов, но и о переориентации бизнеса на защиту информации и процессов ее хранения и передачи наряду с отслеживанием аномальной активности, в первую очередь при получении доступа к защищаемым ресурсам”.

Основные используемые технологии и классы СЗИ

С прицелом на импортозамещение г-н Гончар предлагает российским корпоративным пользователям быть более внимательными к отечественным ИБ-производителям, среди которых есть работающие на международном рынке и даже входящие в разряд лидеров своих продуктовых направлений.

Основными каналами заражения конечных точек технический директор компании “Информзащита” Иван Мелехин считает Интернет и электронную почту и поэтому рекомендует контролировать и защищать их в первую очередь. Сфокусированные на эти каналы специализированные средства защиты с модулем защиты от APT (“песочницей”) позволяют, по его мнению, сэкономить средства на ИБ. В будущем такие СЗИ, как он считает, позволят защищаться практически от всех угроз.

“В большинстве случаев, — говорит г-н Черкас, — дополнительные технологии защиты рабочих станций являются частью механизмов защиты именно от современных атак — APT, Zero day и т. п. Наиболее эффективным, на мой взгляд, является использование “песочниц” в совокупности с агентами для поведенческого анализа рабочих станций”.

Примерно той же позиции придерживается г-н Мелехин. Он полагает, что систему ИБ необходимо дополнять специализированными СЗИ от APT, которые позволяют в автоматическом режиме эмулировать запуск подозрительных файлов в виртуальной среде и анализировать поведение подозрительных программ. “Опыт наших проектов показывает, что решения такого класса действительно позволяют обнаружить даже те вредоносы, которые остаются незамеченными традиционными антивирусными движками”, — говорит он.

Для защиты конечных точек, считает г-н Бодрик, следует использовать NAC-технологии. С их помощью в автоматическом режиме можно контролировать выполнение конечной точкой корпоративных стандартов безопасности: проверять, установлен ли антивирус с актуальными базами сигнатур, обновлено ли ПО, определять тип удаленной конечной точки и в соответствии с типом разграничивать доступ, выяснять, не проведен ли взлом (jailbreak) устройства доступа, блокировать доступ в сеть (или только уведомлять о попытках доступа) машинам, которые не соответствуют утвержденной политике ИБ. “В будущем, — говорит он, — можно ожидать использования технологий адаптивного доступа (adaptive access), позволяющих предоставлять доступ в контексте геолокации, контроля времени суток доступа и т. п.”.

В то же время г-н Мелехин призывает не забывать, что наличие обновлений и антивирусного ПО еще не гарантирует отсутствие вредоносов на машине пользователя. Здесь на помощь, как он считает, приходят средства инспекции трафика класса NGFW/NGIPS, которые позволяют вовремя обнаружить вредоносную активность удаленного пользователя на уровне сети и блокировать его трафик.

“Средства обнаружения зараженных машин по их сетевой активности с помощью систем класса NGFW/NGIPS и последующий анализ в “песочнице” обнаруженных на этих машинах подозрительных файлов до недавнего времени воспринимались скорее как интересная инновация, экзотика, — поясняет г-н Мелехин. — А сегодня они востребованы не менее, чем антивирусы”.

Как наиболее эффективные для предотвращения утечек данных с корпоративных компьютеров директор по решениям компании “Смарт Лайн Инк” Сергей Вахонин выделяет информационно-центричные механизмы безопасности: “Речь о системах класса Endpoint DLP, основным элементом которых является полнофункциональный агент, работающий на защищаемом компьютере или внутри виртуальных сеансов операционной системы и выполняющий задачи предотвращения утечек в любых вариантах использования конечной точки”.

Фокус защиты в таких системах, подчеркивает г-н Вахонин, должен быть смещен с сетевого периметра на рабочие станции. Кроме обычного контроля доступа пользователя к компьютеру, сети и приложениям такие системы должны обеспечивать контроль операций доступа к данным и передачи данных, а также внутренних и исходящих потоков конфиденциальных данных. Использование базовых методов контроля над операциями с данными на основе критериев “кто”, “как”, “откуда”, “куда”, “когда” не менее необходимо, чем использование других критериев безопасности. Наконец, такое решение должно инспектировать и фильтровать содержимое передаваемых, используемых и хранимых на компьютере данных в целях принятия решения о разрешении, блокировании, протоколировании, теневом копировании или направлении оповещения в каждом конкретном случае передачи данных — непосредственно в точке их передачи, непосредственно на защищаемой конечной точке.

Безопасность конечных точек традиционных корпоративных ИКТ-инфраструктур, как считает г-н Бодрик, можно повысить, применяя средства детектирования угроз и противодействия им на конечных точках (в классификации компании Gartner, это решения класса Endpoint Detection & Response, EDR). Такие средства интегрируются в современные экосистемы безопасности. Они позволяют использовать коллективную силу нескольких антивирусов (4—16 сразу), проводить быстрые расследования инцидентов на конечных точках. В будущем разработчики таких средств, по его мнению, будут поглощены антивирусными вендорами.

Еще одним направлением защиты конечных точек, полагает г-н Бодрик, можно выбрать упоминаемый выше постоянный анализ поведения пользователей, в первую очередь анализ доступа к ИКТ-ресурсам. Системы анализа поведения пользователей (User Behavioral Analysis, UBA, в классификации компании Gartner) позволяют выявить закономерности в действиях пользователей. В зависимости от производителя системы UBA позволяют отслеживать аномалии по разным признакам: обращению в необычное время или с необычного IP-адреса к критически важному серверу, детектированию классических атак Pass-the-Hash, Pass-the-Ticket, Golden Ticket.

Использование средств “нечеткого детектирования” — выявление аномалий в трафике, в активности пользователей, в активности приложений, по мнению г-на Мелехина, при должном подходе к анализу аномалий помогает выявлять типы инцидентов, которые раньше не встречались и для которых нельзя заранее сделать сигнатурный алгоритм. Решения подобного класса, как правило, разделены по принципу анализируемой информации (network anomaly, user behavior analytics, application control).

На тот же результат нацелено комплексное использование средств защиты, когда проблема рассматривается в разных плоскостях с точки зрения разных технологий защиты. Данный подход позволяет повысить достоверность выявляемых инцидентов. Средством автоматизации такого подхода, отмечает г-н Мелехин, являются системы SIEM.

В подходе, нацеленном на использование комплексных средств защиты (не путать с комплексным использованием СЗИ), как считает г-н Бойцов, практически не меняются технологии и типы защитных механизмов — это антивирусы, персональные сетевые экраны, средства обнаружения и предотвращения вторжений, криптографические подсистемы, средства защиты от несанкционированного доступа (разграничение прав и полномочий), контроль устройств, средства резервного копирования, специализированные средства для защиты от веб-угроз (антифишинг, антиспам, веб-антивирус) и т. д. Зато в них изменяется принцип построения системы: вместо набора несвязанных СЗИ, решающих разные задачи, применяются одно-два устройства или ПО, которые выполняют те же задачи без конфликтов и избыточной нагрузки.

Соглашаясь с коллегами, г-н Керценбаум подчеркивает, что при внедрении современных решений для эффективной защиты рабочих станций и серверов в первую очередь следует обращать внимание на их способность создавать специальное окружение вокруг наиболее критичных элементов и процессов рабочей среды пользователя. “В данном случае мы говорим о поведенческом анализе, контроле запуска приложений и загрузки динамических библиотек, разграничении доступа к сетевым ресурсам по типу данных, мониторинге использования съемных устройств, шифровании данных и других надантивирусных технологиях, — поясняет он. — Их работа в сумме должна не только обеспечивать защиту конечной точки от попыток взлома и заражения, но и выявлять аномальную активность на хосте, которая может быть следствием как неумышленного некорректного поведения пользователя, так и успешной попытки взлома и проникновения внутрь защищаемого периметра”. В силу развития мобильных технологий в качестве конечной точки можно в равной степени рассматривать как стационарный компьютер, так и корпоративное мобильное устройство, например смартфон или планшет.

Вместе с тем, как подчеркивает г-н Мелехин, одних СЗИ недостаточно и полностью полагаться на автоматизированные системы нельзя. Работы систем защиты нужно дополнять аналитическим разбором результатов. Это требует высокой квалификации, глубокого понимания (или плотного взаимодействия с коллегами, которые понимают) сущности защищаемых процессов и систем, а также способов атак на них, для чего необходимо иметь в штате высококвалифицированных и дорогих специалистов.

К этому российские компании не всегда готовы. Как выход г-н Мелехин предлагает прибегать к услугам внешних экспертных команд для разового или периодического выполнения аналитических задач. Результаты их работы, кстати, могут использоваться для коррекции настроек СЗИ заказчика. Многие компании полностью переходят на модель операционных затрат и передают обеспечение ИБ на аутсорсинг.

Готовность российских заказчиков

По скорости адаптации ИБ-технологий Россия, по мнению г-на Керценбаума, находится практически на том же уровне, что и страны с развитой экономикой, и о новейших подходах к обеспечению ИБ российские ИБ-специалисты узнают одними из первых и довольно часто реализуют эти подходы на практике.

Г-н Керценбаум обращает внимание также и на то, что сосредоточенная на российском рынке ИБ-экспертиза позволяет отечественным компаниям быстро и эффективно использовать зарекомендовавшие себя в мире решения по обеспечению защиты конечных точек.

По мнению г-на Бойцова, переход к комплексной защите положительно оценивает большинство российских заказчиков. Данный подход, как он считает, практически не имеет недостатков. А учитывая плюсы: экономию на стоимости лицензий, снижение нагрузки на компьютеры, низкие временные затраты на поддержку, оперативное управление, мониторинг и реагирование из единой консоли, сокращение расходов на обучение персонала, — большая часть российских организаций уже в ближайшее время, по его мнению, перейдет к использованию комплексных решений по защите информации на конечных точках.

Г-н Бодрик отмечает, что российские компании уже активно используют решения NAC. Что касается технологий UBA, то они активно тестируются в крупных компаниях финансовой и других отраслей, а первые проекты с их использованием, по его прогнозам, будут реализованы уже в 2016 г. Ввиду пассивного характера этих технологий он ожидает, что их внедрение будет занимать немного времени.

Решения класса Adaptive access, по наблюдениям г-на Бодрика, используются в стране наиболее крупными банками и платежными системами для защиты электронных финансовых сервисов. В то же время немногие задумываются о применении контекстного доступа для внутренних пользователей. Системы EDR, как он отмечает, практически не встретить в российских компаниях, хотя растет интерес к возможности использовать несколько антивирусов сразу и снизить время реагирования на атаки. По его оценкам, увы, потребуется несколько лет для реализации первых проектов EDR, даже у крупнейших российских заказчиков.

Г-н Сабанов, учитывая различия между российскими компаниями в подходах к ИБ в целом и защите конечных точек в частности, связанные с их принадлежностью к конкретным отраслям и размером их ИБ-бюджетов, в принципе оценивает уровень специалистов, принимающих решения в этих компаниях о применении тех или иных СЗИ, как весьма высокий. В то же время сегодняшний тренд на экономию не позволяет компаниям своевременно решать насущные ИБ-задачи — им приходится откладывать это на будущее.

По оценкам г-на Черкаса, в 2015 г. лишь небольшая часть российских компаний инициировала или реализовала проекты по созданию систем защиты от современных атак. В то же время около 90% заказчиков, с которыми имеет дело представляемая им компания, планируют реализовать такие проекты уже в 2016 г. На этом основании он оценивает готовность российских компаний к использованию современных средств защиты конечных точек как высокую.

Большинство корпоративных потребителей продуктов обеспечения ИБ конечных точек (endpoint protection platform, EPP), как считает г-н Гончар, в основном обращает внимание лишь на функционал защиты от вредоносных программ. Такие компании, считает он, вряд ли будут внедрять системный подход к ИБ — они ограничатся только использованием функциональных возможностей СЗИ.

Вместе с тем в своей практике он все чаще замечает нацеленность российских заказчиков на защиту от APT, объясняя это тем, что по роду своей работы имеет дело преимущественно с крупными компаниями, которые характеризуются высоким уровнем зрелости. Таким заказчикам, отмечает он, важна комплексная безопасность, и они готовы внедрять ИБ-продукты, которые предлагают широкий спектр методов защиты и подтвержденную результатами тестов высокую эффективность.