Новый подход к обеспечению ИБ современной организации

Подходы, лежащие в основе целенаправленных атак, растущий профессионализм киберпреступников, разделение труда и аутсорсинг в их среде требуют принципиально нового подхода к обеспечению ИБ, основанного на главенствующей роли детектирующих средств защиты. В качестве одного из подобных детектирующих средств защиты автор предлагает рассмотреть ныне несправедливо забытые ханипоты.

Ключевые слова: детектирование, ханипот, целенаправленные атаки, качественно новый подход к ИБ

Павел Витальевич Волчков,
заместитель руководителя отдела консалтинга Центра информационной безопасности
Компания «Инфосистемы Джет»
pvolchkov@jet.msk.su

Несмотря на все предпринимаемые усилия, количество кибератак в мире продолжает расти год от года. По оценке Сбербанка, сделанной в 2016 году, количество киберпреступлений в России к 2018 году может вырасти в четыре раза относительно показателей, имевших место на момент прогнозирования, при этом общие потери от них превысят 2 трлн руб. Такое положение дел не может не огорчать и заставляет задуматься о правильности подходов к обеспечению информационной безопасности.

Что же является сегодня причиной роста количества атак, направленных на различные организации, а главное – их успешности?

К сожалению, достаточно много организаций по-прежнему уделяет недостаточное внимание вопросам информационной безопасности. Основным драйвером ИБ для них являются регуляторы и их нормативные требования. При этом философия защиты этих самых регуляторов заключается в изначально неверном посыле – необходимости опираться на превентивные контроли информационной безопасности. Как показывает практика, в условиях текущего развития ИТ-технологий и колоссальных требований к скорости протекания бизнес-процессов данный посыл является устаревшим.

Почему же системы обеспечения ИБ, основанные на превентивных контролях, не способны защитить от целенаправленных кибератак? Тому есть две причины: размытый сетевой периметр большинства современных компаний и обыкновенный человеческий фактор (иными словами – социальная инженерия).

En New Approach at Information Security

P. V. Volchkov,
Deputy Head of the Consulting Department of the Information Security Center
Jet Infosystems
pvolchkov@jet.msk.su

Approaches underlying the targeted attacks, the growing professionalism of cybercriminals, the division of labor and outsourcing in their environment require a fundamentally new approach to providing information security based on the dominant role of detecting security. As one of such detecting means of protection, the author suggests examining now unfairly forgotten honeypots.

Keywords: detection, honeypot, APT, a qualitatively new approach to information security

Поговорим о сетевом периметре. Сегодня у многих организаций он включает в себя не только набор внешних IP-адресов с опубликованными сервисами. В сетевой периметр компаний входят мобильные устройства работников и их домашние компьютеры, сети Wi-Fi и сетевые порты для подключения устройств обслуживания клиентов, которые могут быть разбросаны по разным регионам страны (в случае, если компания – территориально-распределенная, с множеством отделений или точек продаж). Как итог – защищать такой периметр на 100 % становится практически невозможно.

В свою очередь, специфика целенаправленных атак (социальная инженерия + использование уязвимостей нулевого дня + наличие значительного запаса времени) приводит к тому, что злоумышленник практически гарантированно преодолевает любую защиту периметра и иные превентивные контроли.

Читатель может возразить, заметив, что в современных системах обеспечения информационной безопасности детектирующие контроли занимают не менее важное место, чем превентивные, однако тут есть с чем поспорить. Едва ли текущие реализации детектирующих контролей можно считать эффективными. Главная проблема всех основных средств защиты информации, обеспечивающих функции детектирования (IDS/IPS, WAF, DAM, Integrity Control, NetFlow анализаторы и т. д.) – огромное количество ложных срабатываний. Данная проблема должна решаться перманентным тюннингом политик средств защиты под конкретную ИТ-инфраструктуру, но в подавляющем большинстве организаций этого не происходит по причине нехватки кадровых ресурсов и квалификаций. Кроме этого, все более значимой проблемой становится наличие в инфраструктуре так называемого Shadow-IT (неучтенных ИТ-ресурсов, существование которых неизвестно работникам службы ИБ и которые не покрываются средствами защиты). О том, что данная проблема становится все более актуальной, свидетельствует возрастающее количество запросов от наших клиентов на такую, казалось бы, тривиальную задачу, как инвентаризация объектов сети.

Другой проблемой текущего подхода к построению систем защиты является идея строго формального моделирования угроз ИБ, в рамках которого учитываются только известные угрозы. Вследствие этого, результатом плана обработки рисков ИБ становится набор мер, необходимость которых априори не вызывает сомнений. Действительно, нужно ли делать анализ рисков, чтобы понять, что необходим антивирус или периметровый межсетевой экран?

«Открытия Америки» в вышеобозначенных проблемах, конечно, нет. Мы лишь еще раз показали то, что и так лежит на поверхности. А теперь постараемся предложить пути решения сложившейся ситуации, как мы их видим.

Как и в любой другой предметной области никакой «серебряной пули» здесь не существует – надо искать комплексное решение.

Во-первых, признаем, что не стоит полностью отвергать классический подход, основанный на использовании превентивных контролей совместно с текущими средствами детектирования. У него все же есть свои преимущества – обеспечение базового уровня безопасности и нейтрализация наиболее распространенных угроз.

Во-вторых, компаниям стоит обратить свое внимание на аутсорсинг в сфере ИБ, поскольку именно в этом случае при совершении целенаправленной атаки на организацию, ей сразу же будет оказана помощь профессионалов, специализирующихся на противодействии целенаправленным атакам.

Наконец, в-третьих, выстраивать системы обеспечения ИБ необходимо не с позиции «мы должны не пустить злоумышленника в сеть», а с позиции «любой сетевой периметр может быть скомпрометирован и необходимо максимально быстро обнаружить факт проникновения».

Тут уместна параллель с обеспечением физической защиты. Ни один человек, беспокоясь о безопасности собственной квартиры, не станет полагаться на защиту двери в подъезд или двери на лестничную клетку. Более того, хорошо известно, что даже дверь в квартиру, оборудованная лучшим замком, не является гарантированной защитой от взломщиков, так как еще есть балкон или окна, решетки на которые ставить очень не хочется, а самое главное, потому что любой замок может быть взломан при наличии достаточного количества времени и соответствующей квалификации.

Если добавить к превентивным средствам детектирующие в виде сигнализаций и средств видеонаблюдения, а также корректирующие в лице группы быстрого реагирования, у злоумышленника просто не хватит времени на обход первых (превентивных). Именно такая идея – не дать злоумышленнику достаточного количества времени для преодоления внутренних «логических» заборов – и должна лежать в основе современных комплексных систем защиты информации.

По-другому это можно сформулировать так: главным становится не защита абстрактных, постоянно изменяющихся активов, выделение и актуализация которых само по себе является задачей высокой сложности, а активное противодействие злоумышленнику. При этом основной задачей становится профилирование злоумышленника, фактически классическая модель нарушителя, но с акцентом на мотив, а основой для построения системы защиты – детектирующие контроли.

Естественность перехода к новой парадигме подтверждают и зарубежные издания. Gartner предсказывает изменения структуры бюджетов ИБ в течение ближайших лет. Аналитики компании прогнозируют, что к 2020 году на работу, связанную с быстрым обнаружением ИБ-инцидентов и реагированием на них, будет выделяться порядка 60 % бюджетов ИБ предприятия по сравнению с менее чем 30 % в 2016 году[1].

[1] *http://www.gartner.com/newsroom/id/3337617*

Особую роль в реализуемых мерах защиты играет максимальная универсализация детектирующих мер защиты. Важно, чтобы эти меры как можно в меньшей степени зависели от изменений ИТ-инфраструктуры и оставались максимально актуальными. При этом уровень ложных срабатываний должен быть минимальным, не зависеть от имеющихся человеческих ресурсов и их квалификации, параметров защищаемых активов, их внутренних свойств, ценности, режимов обработки, требований по доступности и т. д.

Как же добиться таких показателей? Здесь помогут и коммерческие SOC (*Security Operation Centers*), и UBA (*User Behavior Analytics*), однако особое внимание, на наш взгляд, стоит уделить старому и несправедливо забытому решению – ханипоту.

Напомним, ханипот – это заведомо уязвимый объект сети, провоцирующий злоумышленника на атаку, а следовательно, на проявление себя. Правильно внедренный ханипот способствует как раз не защите активов, а противодействию активности нарушителя. Он слабо чувствителен к изменению ИТ-инфраструктуры, поэтому даже при развертывании новой информационной системы нет необходимости проводить формальный анализ рисков и подключать хосты системы к СЗИ – достаточно просто разместить сенсоры ханипота в сегментах новой системы. Ханипот практически лишен ложных срабатываний, так как основной принцип его работы заключается в том, что легитимные работники никогда не будут предпринимать в отношении сенсоров ханипота каких-либо действий: осуществлять удаленных вход, сканировать порты, обращаться к доступным сервисам и т. д. Следовательно, любая манипуляция с сенсорами будет считаться инцидентом ИБ, требующим немедленного реагирования.

Ну и самое главное: на этапе эксплуатации ханипот максимально независим от свойств защищаемых активов, поскольку не взаимодействует с ними и не может оказать на них негативного влияния. Именно это, в первую очередь, выгодно отличает его от классических средств детектирования, таких как IDS, DAM, WAF и пр.

Кроме функциональных преимуществ, перечисленных выше, у ханипотов есть и другие плюсы.

Масштабирование. Сенсоры ханипота, обычно представляют собой преднастроенные виртуальные машины. Это позволяет с легкостью масштабировать решение как в сторону увеличения, так и в сторону сокращения количества сенсоров.

Борьба с Shadow-IT. Ханипоты являются одним из ответов на все возрастающую проблему Shadow-IT, то есть неучтенных ИТ- и ИБ-службами ресурсов, которые в силу своей «невидимости» не покрыты классическими средствами защиты, не обновляются и фактически не защищаются. Ханипот же, поскольку он не нацелен на защиту конкретных активов, позволяет хоть в какой-то степени снизить негативный эффект от Shadow-IT в обеспечение безопасности за счет защиты инфраструктуры в целом, вне зависимости от того, какие в ней содержаться активы, учтенные или нет.

Отсутствие нагрузки на ИТ-инфраструктуру и необходимости менять сетевую архитектуру. Ханипот – пассивное средство защиты, которое, по сути, не увеличивает нагрузку на ИТ-инфраструктуру. Трафик, передаваемый между компонентами ханипота, незначителен, как и логи, передаваемые по syslog. Про просадку производительности на серверах «боевых» систем речь не идет вообще, так как ханипот с ними не интегрирован. Также практически не требуется изменение сетевой архитектуры. Единственное, что необходимо учесть на стадии проектирования, это ресурсы среды виртуализации, но и их нельзя назвать значительными, ведь на сенсорах ханипота не предполагается разворачивание «тяжелых» бизнес-приложений.

Конечно, не всё так просто: внедрение ханипота требует предварительного проектирования и подготовки, и основной сложностью здесь является сокрытие его в ИТ-инфраструктуре. Тем не менее, сложность этой задачи не сопоставима со сложностью внедрения таких решений как WAF, IPS или SIEM. ■

НОВОСТИ

BIS Summit 2017 Saint-Petersburg

31 марта 2017 года впервые в Санкт-Петербурге состоялось продолжение крупнейшей Международной конференции BIS Summit, которая ежегодно на протяжении 10 лет проходит в Москве. Мероприятие было организовано Ассоциацией по вопросам защиты корпоративной информации (BISA) при поддержке Правительства Санкт-Петербурга.

Международная конференция BIS Summit, которую на этот раз принял в своих стенах отель Park Inn by Radisson Pulkovskaya, – это дискуссионная площадка для ведущих экспертов российского и международного рынков информационной безопасности, руководителей бизнеса и представителей государственных организаций.

Главная тема прошедшего саммита – «Государство, бизнес и общество в новых реалиях цифрового мира. Возможности, риски, противоречия». В пленарной части «Готовность ИБ к новым рискам. Мировые рынки и актуальные тенденции» приняли участие председатель Комитета по информатизации и связи Правительства Санкт-Петербурга Денис Чамара, Президент группы компаний InfoWatch Наталья Касперская, заместитель генерального директора ГК InfoWatch, президент ассоциации BISA Рустэм Хайретдинов, начальник управления безопасности АО «Национальная система платежных карт» Василий Окулесский, заместитель начальника Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере ГУБЗИ Банка России Павел Ревенков.

После дискуссии с ключевыми спикерами прошли четыре секционных заседания. Кроме того, участники мероприятия смогли ознакомиться с новейшими разработками вендоров и оценить возможности перспективных технологий в сфере информационной безопасности. В демонстрационной зоне «Технопарк» была представлена вся линейка решений InfoWatch, а также продукты и решения «Лаборатории Касперского», Samsung, WorksPad, Infotecs и других компаний.