Октябрь 2016 г.

Борьба с угрозами безопасности с помощью интеллектуальных решений для обеспечения безопасности конечных точек и управления ими

Назначение приоритетов уязвимостям и ускоренное устранение последствий с применением IBM QRadar и IBM BigFix

IBM

Содержание

Введение

Начиная от созданного под заказ вредоносного программного обеспечения и заканчивая эксплойтами нулевого дня, во всем мире резко возрастает число сложных угроз для безопасности, при этом уровень сложности таких атак постоянно повышается. Современные киберпреступники научились находить своих жертв посредством электронной почты или веб-технологий, а также использовать для своих целей уязвимости самих конечных точек. Масштабные скоординированные атаки, проводимые с высоким уровнем исполнения, теперь характерны для широких сегментов интернета, а традиционные механизмы обеспечения безопасности зачастую оказываются неспособными противостоять таким атакам. В то же время постоянно растет число модификаций вредоносного ПО.

Как организации могут справиться с такими сложными угрозами безопасности? Безусловно необходимым и важным является поддержание высокого уровня базовой безопасности путем последовательного применения политик безопасности и пакетов исправлений ПО для конечных точек и серверов. Однако если в сетях на момент сканирования присутствует несколько уязвимостей на один IP-адрес, медленный процесс выявления и устранения таких слабых мест может стать причиной образования опасных пробелов в системе обеспечения безопасности. Сегодня ИТ-специалистам приходится принимать сложные, основанные на оценке риска решения относительно того, на чем им следует сконцентрировать свои усилия, не имея при том полного представления о состоянии системы безопасности. Такая ситуация становится еще более критичной, когда число уязвимостей возрастает, а у организации не хватает ресурсов и навыков, чтобы устранить обнаруженные уязвимости. В дополнение к возможности эффективно выявлять уязвимости, организациям также необходимо учитывать более широкий контекст уязвимостей и связывать уязвимости с уровнями риска, чтобы сконцентрировать свои усилия на устранении уязвимостей в зонах наибольшего риска.

В этом официальном отчете рассмотрены способы борьбы со сложными угрозами безопасности путем внедрения интегрированного, интеллектуального и автоматизированного подхода к обеспечению безопасности конечных точек. В нем также поясняются способы расширения контекста и функциональных возможностей платформы IBM® QRadar Security Intelligence Platform за счет возможностей решения IBM BigFix для интеллектуальной защиты конечных точек и имеющихся в этом решении средств управления ими, чтобы идентифицировать, определить приоритеты и устранить риски для безопасности. В публикации также рассматривается стратегическая значимость совместного использования этих решений для борьбы с самыми современными разновидностями атак.

Платформа IBM QRadar Security Intelligence Platform

Платформа QRadar Security Intelligence Platform является ключевым решением, используя которое организации могут эффективно противостоять все более изощренным атакам, защищать свои сетевые среды и интеллектуальную собственность и не допускать прерываний в ведении бизнеса. Данная платформа не только осуществляет мониторинг журналов и потока данных в сети, но и собирает сведения и отслеживает действия широкого ряда источников данных, а также в реальном времени осуществляет корреляцию с правилами и интеллектуальный анализ угроз для быстрой идентификации нарушений безопасности, которые могут требовать незамедлительных действий.

Диспетчер рисков IBM QRadar Risk Manager, созданный на платформе QRadar Security Intelligence Platform, дает организациям возможность проактивно управлять конфигурациями сетевых устройств и сопоставлять их с сетевой топологией для анализа и идентификации рисков безопасности и возможных путей атаки.

Диспетчер уязвимостей IBM QRadar Vulnerability Manager, также созданный на платформе QRadar Security Intelligence Platform, обеспечивает эффективный способ обнаружения уязвимостей устройств, подключенных к сети. Он также может собирать и консолидировать результаты сканирования, предоставляемые различными сканерами уязвимостей. В результате использования данных, передаваемых платформой QRadar Security Intelligence Platform и диспетчером рисков QRadar Risk Manager, QRadar Vulnerability Manager может выступать в роли точки централизованного управления для составления отчетности по уязвимостям и назначения приоритетов для всей организации.

Решение IBM BigFix для обеспечения безопасности конечных точек

Наилучшим методом защиты конечных точек от угроз является выявление уязвимостей программного обеспечения или конфигурации и их устранение до того, как эксплойт сможет нанести ущерб всей сети. Решение BigFix предоставляет функциональные возможности для обеспечения безопасности конечных точек и управления ими, чтобы организации могли осуществлять мониторинг конфигурации конечных точек, установленного программного обеспечения, операционной системы, применения исправлений, а также составлять отчеты о соблюдении политик безопасности по всем устройствам с применением готовых или специально разработанных политик. Решение BigFix также способно оперативно устранять несоответствия, используя сообщения IBM Fixlet для изменения состояния конфигурации конечной точки, применения необходимых исправлений, удаления файлов вредоносного ПО или завершения подозрительных процессов. Такой непрерывный цикл мониторинга — отчетности — исправлений может эффективно сокращать окно возможностей для атак.

Как указано в отчете о расследованиях утечек данных в 2015 году, почти половина недавно выявленных уязвимостей была использована злоумышленниками в течение первых четырех недель после публикации соответствующей информации, поскольку злоумышленники понимают, что многие организации не в силах эффективно и быстро устранить новые уязвимости[1]. Эффективное применение исправлений, как и ранее, является наилучшим подходом к снижению рисков, которые создает вредоносное ПО, использующее недавно обнаруженные уязвимости. Решение BigFix обеспечивает автоматическое упрощенное и эффективное применение исправлений ко всем конечным точкам, как подключенным, так и не подключенным к корпоративной сети, для различных операционных систем и приложений. Применение исправлений с помощью BigFix может существенно сократить время выполнения этого процесса, а также способствует существенному уменьшению операционных издержек.

В отношении уязвимостей, для устранения которых еще нет доступных исправлений (уязвимостей нулевого дня), решение BigFix предоставляет функциональную возможность удаленного карантина, чтобы изолировать от сети уязвимые конечные точки и таким образом защитить их от атак и заражения других конечных точек, пока не будет выпущено соответствующее исправление или средство для устранения уязвимости.

Устранение пробелов в управлении уязвимостями

Чтобы защититься от угроз для безопасности, организациям необходим комплексный подход для идентификации и устранения рисков с высоким приоритетом в постоянно изменяющейся ИТ-среде. В рамках такого подхода должны выполняться следующие задания:

- понимание актуального статуса разнообразных конечных точек;
- идентификация уязвимостей каждой конечной точки;

- выработка приоритета для устранения уязвимостей;
- быстрое выполнение действий по устранению высокоприоритетных уязвимостей конечных точек или уменьшению создаваемой ими угрозы либо постановка устройств на карантин;
- проверка успешного применения корректирующего действия и более безопасного состояния конечной точки.

Многие решения для управления уязвимостями могут идентифицировать уязвимости и устанавливать приоритет для их устранения, однако при этом не обладают интеллектуальными и функциональными возможностями для эффективного устранения таких уязвимостей с заданным приоритетом. При совместном использовании BigFix с платформой QRadar Security Intelligence Platform эти решения IBM способны помочь организациям в устранении пробелов в системе управления уязвимостями. Благодаря этому интегрированному решению организация может идентифицировать и ранжировать по приоритетам уязвимости в операционных системах и прикладном ПО, которые могут использовать злоумышленники, а затем устранить такие уязвимости, чтобы предотвратить возможность атаки или минимизировать ее последствия для организации.

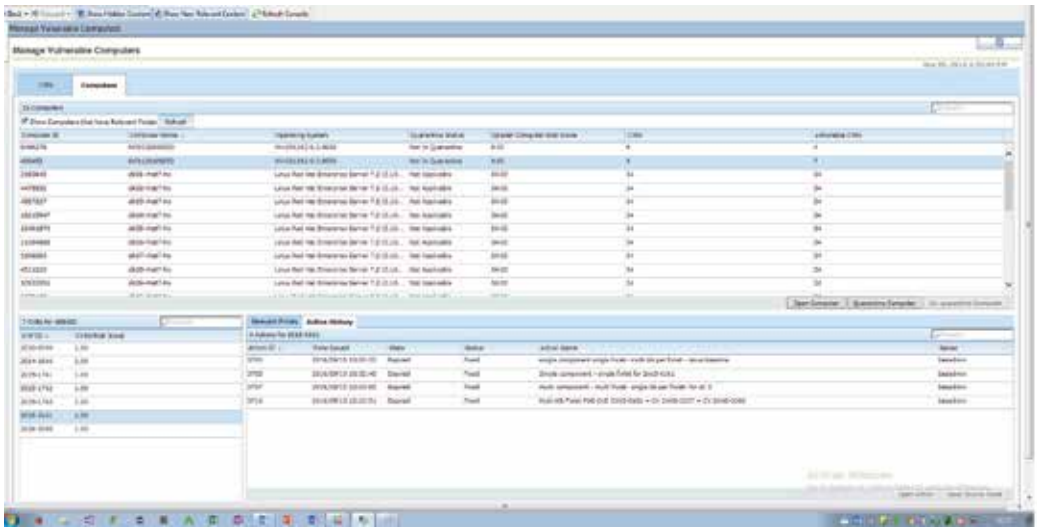
Установление замкнутого управления рисками с применением интеллектуальных решений для конечных точек

По мере того как современные высокоразвитые угрозы становятся более опасными, динамичными и разрушительными, наблюдается все большая потребность в интегрированных, интеллектуальных и автоматизированных средствах для борьбы с такими угрозами. Использование интегрированного решения, в котором сочетается и платформа QRadar Security Intelligence Platform, и решение BixFix, дает возможность ИТ- и ИБ-специалистам совместно работать над защитой активов от атак, которые становятся все более изощренными.

Решение BigFix способно предоставлять подробные сведения о статусе конечных точек практически в реальном времени, создавать отчеты о применении исправлений, недавних изменениях конфигурации и т. д. и передавать их на платформу QRadar Security Intelligence Platform для повышения точности аналитики, связанной с системными рисками. В частности, агент BigFix, работающий на конечной точке, подключенной или не подключенной к корпоративной сети, постоянно оценивает ее конфигурацию и выполнение политики применения исправлений и отправляет сведения об актуальном статусе в QRadar, с тем чтобы платформа QRadar смогла сопоставить статус конечной точки с другими событиями в области безопасности или сетевыми действиями для выявления подозрительных инцидентов.

Решение IBM BigFix передает актуальный статус конечных точек в IBM QRadar для сопоставления этого статуса с другими событиями безопасности и назначения приоритетов подозрительным инцидентам.

Диспетчер уязвимостей QRadar Vulnerability Manager можно использовать для сканирования уязвимостей или сбора сведений о них от BigFix или других сканеров уязвимостей конечных точек, назначения оценки риска каждому активу на основании сопоставления с расширенным контекстом, предоставляемым QRadar Risk Manager, который включает данные о топологии сети и коммуникационных действиях, и последующей передачи оценок уязвимостей и рисков для активов в BigFix. В отношении каждой выявленной с помощью QRadar уязвимости решение BigFix может порекомендовать ИТ-специалистам подходящее действие по устранению (применение исправления или помещение в карантин). Более того, ИТ-персонал получает возможность использовать оценку риска для активов, сведения о количестве уязвимостей на каждой конечной точке или доступные методы устранения в целях составления приоритета таким образом, чтобы в первую очередь устранить наиболее критичные уязвимости.



Решение IBM BigFix способно эффективно устранять уязвимости, выявленные диспетчером уязвимостей QRadar Vulnerability Manager, и предоставляет различные метрики, помогающие ИТ-специалистам заказчика назначать приоритеты усилиям по обеспечению безопасности.

После устранения уязвимости актуальный статус конечной точки передается в QRadar и повторно сопоставляется с другими событиями безопасности или сетевыми действиями, что может привести к обновлению сведений о ранее выявленных подозрительных инцидентах. Сочетая предоставляемые решением BigFix интеллектуальные возможности и средства управления конечными точками и имеющиеся в QRadar возможности для обеспечения безопасности всей корпоративной ИТ-среды, организации могут выработать непрерывно выполняемую программу замкнутого управления рисками для эффективной борьбы с угрозами для безопасности.

- Повышение точности сведений в базе данных активов
- Улучшение оценки рисков
- Улучшение отчетности по соблюдению нормативных требований
- Ускорение выработки приоритетов устранения угроз и уязвимостей с точки зрения рисков
- Расширение оценки уязвимости на конечные точки, не подключенные к сети

IBM BigFix и IBM QRadar при совместном использовании образуют интегрированную систему закрытого управления рисками, в которой используется формируемая в реальном времени аналитика состояний конечных точек и аналитика состояния безопасности всей ИТ-инфраструктуры компании.

Заключение

Для более эффективного управления уязвимостями организациям необходим интегрированный подход, сочетающий как интеллектуальные возможности для анализа конечных точек, так и сетевой контекст. Для соблюдения приоритета при устранении уязвимостей ИТ-персоналу необходимо знать, какие уязвимости исправит по графику система управления конечными точками, а какие необходимо исправить вручную. Кроме того, ИТ-персоналу нужна возможность быстрого реагирования на основании полученного анализа безопасности и быстрой установки обновлений на все конечные точки, использующиеся в организации.

При совместном использовании решений QRadar и BigFix организации могут с упреждением реагировать на сложные угрозы безопасности. Стратегическое преимущество такого интеллектуального, автоматизированного и интегрированного подхода состоит в обеспечении консолидированного управления и эффективного использования ресурсов в области безопасности. Оперативность реагирования на инциденты, в том числе время с момента возникновения уязвимости до ее выявления, можно оптимизировать, сочетая получаемые от BigFix практически в реальном времени сведения о статусе конечных точек с интеллектуальным анализом безопасности, который осуществляют решения QRadar. В результате такого сочетания миллионы событий безопасности можно свести в управляемый список уязвимостей с назначением приоритетов. Соответственно, организации могут использовать проактивный подход к укреплению своих средств для защиты ИТ-инфраструктуры от наиболее постоянных угроз и существенно сократить риски.

Для национальной безопасности необходимо обеспечение соответствия конечных точек нормативным требованиям в реальном времени

Тот факт, что безопасность ИТ-систем федеральных агентств подвергается многочисленным угрозам, обусловил принятие законодательных актов, требующих внедрения решений, для непрерывного мониторинга уязвимостей, управления ими и их устранения. Интеграция решений QRadar и BigFix приносит огромную пользу федеральным агентствам.

Корпоративное решение для обеспечения безопасности компьютерных систем способно помочь правительственным органам эффективнее бороться с угрозами и устранять уязвимости. В качестве одного из примеров можно указать на тот факт, что свыше 50 федеральных агентств в США стандартно используют решение BigFix для управления и обеспечения безопасности более чем трех миллионов рабочих станций, серверов (как физических, так и виртуальных) и других конечных точек, работающих под управлением самых разнообразных операционных систем. Такие решения в реальном времени и непрерывно обеспечивают безопасность конечных точек и соответствие их состояния нормативным требованиям благодаря использованию библиотек, содержащих несколько тысяч проверок.

Более подробная информация

Для получения дополнительных сведений об IBM QRadar Security Intelligence Platform, IBM BigFix или других решениях IBM Security обратитесь к представителю или бизнес-партнеру IBM либо посетите веб-сайт **ibm.com**/security

О решениях для обеспечения безопасности IBM Security

IBM Security предлагает один из наиболее совершенных и интегрированных портфелей продуктов и услуг в области обеспечения корпоративной безопасности. Входящие в данный портфель продукты, разрабатываемые всемирно известным научно-исследовательским центром IBM X-Force, предоставляют сведения по безопасности, которые помогают организациям целостно защищать своих сотрудников, инфраструктуры, данные и приложения и содержат функциональные возможности для управления учетными записями и доступом, обеспечения безопасности баз данных, разработки приложений, управления конечными устройствами, безопасностью сетей и многое другое. Данные решения позволяют организациям эффективно управлять рисками и внедрять интегрированные системы безопасности для мобильных и облачных вычислительных сред, социальных сетей и других архитектур, используемых коммерческими предприятиями. IBM управляет одной из крупнейших в мире организаций по исследованию, разработке и поставке решений для обеспечения безопасности; корпорация отслеживает 15 миллиардов событий безопасности в день в более чем 130 странах и владеет более чем 3000 патентов в области обеспечения безопасности.

Кроме того, IBM Global Financing предоставляет различные варианты оплаты, чтобы помочь вашей компании приобретать технологичные решения по мере развития вашего бизнеса. Мы предоставляем услуги по управлению полным жизненным циклом ИТ-продуктов и услуг от приобретения до вывода из эксплуатации. Дополнительную информацию см. на веб-сайте по адресу: **ibm.com**/financing

IBM Восточная Европа/Азия
123112, Москва
Пресненская наб., 10

Тел.: +7 (495) 775-8800, +7 (495) 940-2000
Факс: +7 (495) 940-2070

IBM Ireland зарегистрирована в Ирландии, регистрационный номер 16226.

[1] “2015 Data Breach Investigations Report,” *Verizon*, April 2015. https://msisac.cisecurity.org/whitepaper/documents/1.pdf

Пожалуйста, утилизируйте.

WGW03051-RURU-02