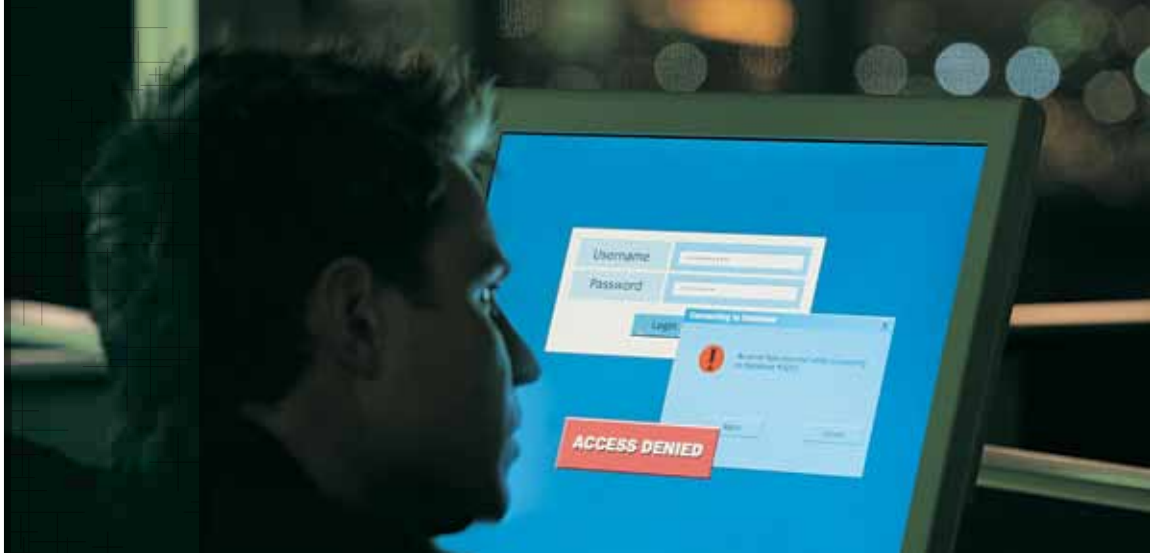
McAfee
An Intel Company

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ И РИСКОМ

Руководство по решению



Security Connected

Разработанный компанией McAfee подход Security Connected позволяет интегрировать друг с другом большое количество разных продуктов, услуг и партнерских отношений, создавая возможность централизованно, эффективно и надежно снижать уровень риска. Основанный на мерах безопасности, проверенных на практике на протяжении более двадцати лет, подход Security Connected позволяет организациям любого размера, в любом регионе мира и в любой отрасли повысить свой уровень безопасности, оптимизировать систему защиты, снижая расходы на нее, и выполнить стратегическую интеграцию системы безопасности и бизнес-процессов организации. В эталонной архитектуре McAfee Security Connected предлагаются конкретные шаги от идей до их воплощения. С их помощью концепцию Security Connected можно адаптировать к конкретным рискам, инфраструктуре и коммерческим целям вашей организации. Компания McAfee непрерывно ведет поиск новых путей защиты своих клиентов.

Все новые материалы доступны для загрузки по адресу www.mcafee.com/ru/enterprise/reference-architecture/index.aspx.

Необходимость упреждающего подхода к управлению риском

Проблемы

Прежде основными целями, которые преследовали компании при управлении безопасностью и риском, были обеспечение нормативно-правового соответствия и сокращение финансового риска. Аудиты и процессы управления были предсказуемыми событиями, которые ИТ-отдел стремился минимизировать и автоматизировать. Риск был довольно статичным понятием. Теперь же темпы распространения угроз — медленных и незаметных, как целенаправленные атаки, или молниеносных, как вспышки кибератривизма и эпидемии вредоносных программ, — требуют от руководителей компаний и ИТ-администраторов уделять больше внимания происходящим в текущий момент событиям и принимать быстрые решения по устранению уязвимостей на основе анализа рисков.

Соответственно и требования, касающиеся обеспечения нормативно-правового соответствия и сокращения финансового риска, тоже приобрели динамический характер. Так, в мире существует более двухсот нормативных директив, и по мере изменения экономической ситуации, рождающей новые возможности для бизнеса, создавшие их регулирующие органы независимо друг от друга вносят в них соответствующие изменения. Прежде статичная картина риска теперь непрерывно меняется словно узоры в калейдоскопе.

«Большие данные» в сфере безопасности

Сегодня управление риском связано с анализом большего количества данных, чем прежде. К этим данным относятся результаты проверок на наличие уязвимостей, журналы событий приложений и баз данных, потоки, журналы доступа и сеансов, предупреждения и результаты анализа трендов. Потоки данных сегодня поступают от множества разных систем, предназначенных для защиты большего числа пользователей, использующих большее число устройств и посещающих большее число мест, чем прежде.

Классическим примером сложностей, возникающих при обработке данных из такого огромного числа разных источников, являются аудиты, как внутренние, так и внешние. ИТ-администраторам приходится находить и упорядочивать потоки данных, а затем представлять их на проверку аудитору в удобном для него формате. Аудиты по определению являются ретроспективной и статичной оценкой прошлого риска. Они отнимают у организации ресурсы и отвлекают ее от упреждающего управления риском, т. е. от возможности смотреть в будущее, анализировать и смягчать меняющиеся риски до того, как они приведут к возникновению ущерба.

Вычисление риска

Мы живем в мире «больших данных», и эти «большие данные» важны для обеспечения безопасности. Иногда для того, чтобы разобраться в изощренной угрозе безопасности, могут потребоваться дни или даже месяцы. При обработке данных большинство аналитиков безопасности сталкивается с проблемами, похожими на те, с которыми сталкиваются ИТ-администраторы при выполнении аудиторских требований: наличие огромного числа независимых друг от друга потоков данных сильно усложняет задачу получения точной и непротиворечивой картины событий. Чем больше объем собираемых и анализируемых данных, тем более хаотичным кажется их скопление, и тем больше времени занимает процесс реконструкции событий. Лишь после получения полной картины события (т. е. когда само событие уже довольно долго в прошлом) появляется возможность изменить политики и средства защиты таким образом, чтобы подобное событие больше не повторилось.

Но что если мы имеем дело с молниеносной атакой — атакой типа «отказ в обслуживании» или быстро распространяющимся червем? Если на диагностирование проблемы будут уходить дни или месяцы, то компании может быть нанесен огромный (и возможно даже фатальный) ущерб с точки зрения нормативно-правового соответствия и финансового риска. Какие активы действительно затрагивает данная угроза и в отношении каких активов действуют компенсирующие средства управления или иные меры противодействия? Чтобы ответить на этот вопрос, администраторам необходимо иметь информацию о степени защищенности всего спектра систем, включая набирающие популярность мобильные и личные устройства, имеющие доступ к их сетям.

Реагирование на события

За пониманием проблемы следует расстановка приоритетов и устранение риска. Какие активы самые важные? С какими можно повременить? Администраторы нередко мечутся от одной консоли управления к другой, выполняя сканирование систем, запуская скрипты, редактируя политики, устанавливая обновления или помещая системы в карантин. Каждый новый продукт, массово появляющийся на рынке средств защиты, влечет за собой дополнительные расходы и новые проблемы: это и другой пользовательский интерфейс, и иной формат данных, и новый стандарт политик и отчетности. В результате неизбежно возникают бреши в защите и ошибки, подвергающие организацию и ее активы ненужному (и, как правило, неучтенному) риску.

Нельзя больше управлять риском, смотря в зеркало заднего вида. Вы должны вооружиться широкоугольным объективом и смотреть вперед, чтобы обнаруживать риск и управлять им по мере его изменения. Ситуативный сбор данных о риске позволяет получить доступ к динамическому контексту, в котором учтена информация о глобальной ситуации с угрозами и информация об активах и степени защищенности вашей компании. Технологии автоматизированного управления риском используют этот контекст для того, чтобы вы всегда имели возможность связать факты в единое целое, чтобы при необходимости выполнить настройку политик и средств защиты.

Решения

Проблема «больших данных» в сфере безопасности и связанные с ней оперативные вопросы усложняют процесс управления безопасностью и риском. Упорядочить этот хаос поможет комплексная стратегия в сочетании с современной технологией. В контексте процессов управления нормативно-правовым соответствием и финансовым риском это означает, что вам необходимо в режиме реального времени учитывать все возможные риски, связанные с внешними и внутренними событиями. Использование единого подхода к решению этих задач позволяет оптимизировать процессы и обеспечить автоматическое реагирование на события, что ведет к сокращению расходов и повышению скорости реагирования. В результате руководители компаний получают информацию о потенциальном воздействии тех или иных событий на уровень риска, а администраторы получают возможность сбора информации и управления средствами защиты для упреждающего снижения уровня риска.

Современные системы управления информацией о безопасности и событиями безопасности (Security Information And Event Management — SIEM) тесно взаимосвязаны со средствами управления безопасностью и обеспечением нормативно-правового соответствия устройств, серверов, сетей, приложений и баз данных. Подобная платформа для управления безопасностью может выполнять функции командно-контрольного центра, позволяющего собирать информацию о ситуации и оперативно реагировать на события. Чем теснее эти системы интегрированы друг с другом, с системами сбора информации о рисках и с системами безопасности, тем легче вам будет анализировать риск и управлять им. Использование концепции «платформы» позволяет согласовать и объединить друг с другом отдельные разрозненные процессы, политики, задачи и отчеты. Возможность получения актуальной информации об угрозах позволяет поместить данные в контекст меняющихся рисков и повысить точность, эффективность и скорость реагирования с целью снижения уровня риска.

Оценка уязвимостей

Большинство организаций, деятельность которых регулируется нормативными правовыми актами, проверяют свои системы на наличие уязвимостей в соответствии с нормативно-правовыми требованиями. Однако, если сканирование проводится по графику, то существует опасность не учесть удаленные системы, находящиеся в спящем режиме, или пропустить критически важные для компании активы: приложения, базы данных и т. п. Незамеченными могут остаться вышедшие из-под контроля системы, несущие в себе неустраненные уязвимости. Ответственный подход к задаче управления уязвимостями всех подключенных к сети активов позволяет охватить все эти разнородные системы и устранить бреши в нормативно-правовом соответствии. Сканирование систем и внедрение компенсирующих средств управления следует проводить на основе динамично получаемых данных о рисках, анализе ценности активов и информации об имеющихся возможностях для принятия мер противодействия.

Улучшение уровня ситуативной осведомленности

Сталкиваясь с кибератаками и брешами в периметре, большинство организаций хочет иметь возможность лучше понимать характер меняющихся рисков и лучше реагировать на них. Здесь самое важное — найти нужные данные, пока они не устарели. Системы SIEM имеют уровень быстродействия и пропускные способности, достаточные для обработки «больших данных» в сфере безопасности, поэтому они могут осуществлять мониторинг приложений и баз данных, управлять журналами событий и нормализовать события для вывода на взаимосвязанные панели мониторинга. Некоторые из них также имеют функции, позволяющие в режиме реального времени проводить анализ угроз, пользователей, систем, данных, рисков и мер противодействия. Наличие богатой контекстной информации дает вам возможность быстро анализировать действия, связанные с безопасностью компании (включая действия, имевшие место в прошлом). Использование надежных аналитических инструментов позволяет предсказывать и выявлять атаки, а также устранять угрозы не за часы и дни, а за считанные минуты.

Анализ сетевого трафика

Сети одновременно являются объектами критически важной инфраструктуры и каналами связи, по которым может происходить утечка конфиденциальных данных, подлежащих нормативно-правовому регулированию. Путем мониторинга и регулирования сетевого трафика (включая зашифрованный трафик), администраторы могут сократить число случаев использования Интернета и приложений в нежелательных и рискованных целях, а также обеспечить применение политик, касающихся содержимого трафика. Интеграция средств сетевой защиты следующего поколения с системами SIEM и средствами системной защиты может помочь администраторам, занимающимся управлением риском, в деле применения политик, обеспечения защиты от угроз «нулевого дня», мониторинга и анализа состояния нормативно-правового соответствия и генерирования необходимых отчетов.

Оптимизация управления журналами событий

В журналах событий содержится огромное количество данных, помогающих вам выполнять нормативно-правовые требования (представление документов в электронной форме, аудиты и т. п.) при условии, что вы можете извлечь из потоков данных необходимые вам факты. Благодаря интегрированному, безопасному и быстрому решению для управления журналами событий, вы можете в режиме реального времени собирать данные из всех необходимых источников и хранить журналы событий в соответствии с надежным стандартом обеспечения сохранности документов. Наличие средств контроля за приложениями не позволяет злоумышленникам вносить изменения в системы ведения журналов событий с целью сокрытия своих следов. Совмещение функций управления журналами с другими функциями защиты и анализа рисков позволяет передавать данные журналов в руки тех, кто может наилучшим образом использовать их для управления риском.

Факторы, способствующие применению оптимальных методов работы

- Согласование и объединение разрозненных процессов и средств управления
- Автоматизация сбора данных, сопоставления угроз, оценки рисков, реагирования на события и мониторинга действий
- Использование динамических данных о рисках, прогнозного анализа и мер реагирования на основе политик для упреждающего обнаружения и блокирования угроз
- Охват всех устройств, данных и всей ИТ-инфраструктуры системой защиты и противодействия рискам
- Сведение сбора всей информации о безопасности и рисках в масштабе предприятия в единую платформу управления, что позволит повысить эффективность и продуктивность управления
- Непрерывный и упреждающий мониторинг ситуации с целью обнаружения риска, реагирования на изменения уровня риска, поддержки нормативно-правового соответствия и предотвращения повторения событий в будущем

Обеспечение вручную процессов безопасности и управления рисками служит самым вероятным источников сбоев и главным фактором высоких расходов на поддержание безопасности и соответствия требованиям.

Факторы успеха

Наличие комплексной стратегии управления безопасностью и риском, реализуемой посредством автоматизированной платформы управления безопасностью на основе анализа рисков, поможет вашей организации:

- обеспечить существенный уровень ситуативной осведомленности путем создания насыщенного контекста и анализа данных;
- за считанные секунды диагностировать инциденты и реагировать на них, тем самым сокращая размер ущерба, предотвращая несанкционированный доступ к данным и снижая расходы на восстановление систем;
- сократить количество инцидентов, связанных с безопасностью и нормативно-правовым соответствием, и снизить расходы в пересчете на один инцидент;
- упростить процессы обеспечения нормативно-правового соответствия и ведения отчетности с целью повышения эффективности работы;
- сократить количество платформ, аппаратных устройств и программных продуктов от разных поставщиков, используемых для управления безопасностью;
- сократить время на обучение и эксплуатационные расходы.

Сопутствующие материалы по теме эталонной архитектуры McAfee Security Connected

Уровень II

- Мониторинг и контроль за изменениями
- Защита центров обработки данных
- Преимущества соответствия стандарту PCI

Уровень III

- Оценка уязвимостей
- Улучшение уровня ситуативной осведомленности
- Анализ сетевого трафика
- Оптимизация управления журналами событий
- Расследование случаев несанкционированного доступа к данным
- Жизнь с социальными медиа
- Защита интеллектуальной собственности

Дополнительную информацию об эталонной архитектуре McAfee Security Connected можно получить, посетив страницу www.mcafee.com/ru/enterprise/reference-architecture/index.aspx.

Об авторе

Барбара Г. Кей (Barbara G. Kay), сертифицированный специалист по безопасности информационных систем (Certified Information Systems Security Professional — CISSP), является старшим отраслевым аналитиком Secure By Design Group. Специализируется в области средств защиты информации для распределенных и мобильных компаний, а также на обучении пользователей приемам безопасной работы в сети Интернет. В 2006 году основала Secure By Design. До этого занимала должность директора по маркетингу в проекте Security and Privacy Initiative компании Sun. Выпускница Дартмутского колледжа.

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru