Официальный документ

Интегрированная архитектура безопасности сети: межсетевой экран нового поколения, ориентированный на предотвращение угроз

Автор: Джон Олтсик (Jon Oltsik), ведущий аналитик

Сентябрь 2014 г.

Настоящий официальный документ ESG был подготовлен по заказу Cisco Systems и распространяется под лицензией ESG.

Содержание

Обзор

В большинстве крупных организаций задачи по обеспечению безопасности сети решаются с использованием целой «армии» инструментов, таких как межсетевые экраны, VPN-шлюзы, системы обнаружения и предотвращения вторжений (IDS и IPS), прокси-серверы, среды тестирования вредоносного ПО, интернет-шлюзы и шлюзы эл. почты, а также многое другое. Этот хаотичный набор независимых друг от друга технологий считался нормой во времена десятилетней давности, однако сегодня он приводит к возникновению большого количества сложных задач, связанных с эксплуатацией, контролем соблюдения политики и мониторингом. В еще большей степени усугубляет ситуацию тот факт, что средства защиты теряют свою эффективность в борьбе с целенаправленными и усовершенствованными угрозами и новейшими атаками вредоносного ПО.

Насколько ухудшилась ситуация, и что следует предпринять руководителям служб информационной безопасности в сложившихся условиях?

- **Сегодня для обеспечения безопасности сети требуется большее количество знаний и усилий.** Специалистам по безопасности приходится ежедневно сталкиваться с несметным числом сложных задач, связанных с параллельно работающими процессами и элементами управления, слишком большим количеством узконаправленных инструментов и процессов, выполняемых вручную, а также недостатком навыков и умений. Принимая во внимание все эти новые и уже исторически сложившиеся трудности, состояние систем обеспечения безопасности далеко не всегда отвечает требованиям современных предприятий.
- **Инструментов обеспечения безопасности, которые используются сегодня, недостаточно.** Многие организации охотно внедряют новые средства обеспечения безопасности, например межсетевые экраны нового поколения (NGFW). Такие решения, как NGFW действительно способны улучшить работу системы обеспечения безопасности, однако они зачастую ограниченны узким спектром элементов управления и не обеспечивают комплексную защиту от угроз кибербезопасности. Кроме того, отдельные инструменты, например тестовые среды для анализа вредоносного ПО, носят тактический характер, поскольку с их помощью невозможно обеспечить защиту или усилить безопасность в пределах сети или облака.
- **Крупные организации нуждаются в совместимой с имеющимися решениями архитектуре, обеспечивающей безопасность сети.** Предприятиям требуется интегрированная архитектура безопасности сети, которая отличается более высокой ориентированностью на предотвращение угроз, предлагает возможности масштабируемости, позволяет автоматизировать выполняемые вручную процессы и заменяет узконаправленные инструменты совместимыми услугами обеспечения безопасности. Архитектура безопасности сети должна включать средства централизованного управления и контроля, распределенного применения, а также интегрированные средства сбора ценной оперативной информации.

Задачи обеспечения безопасности сети

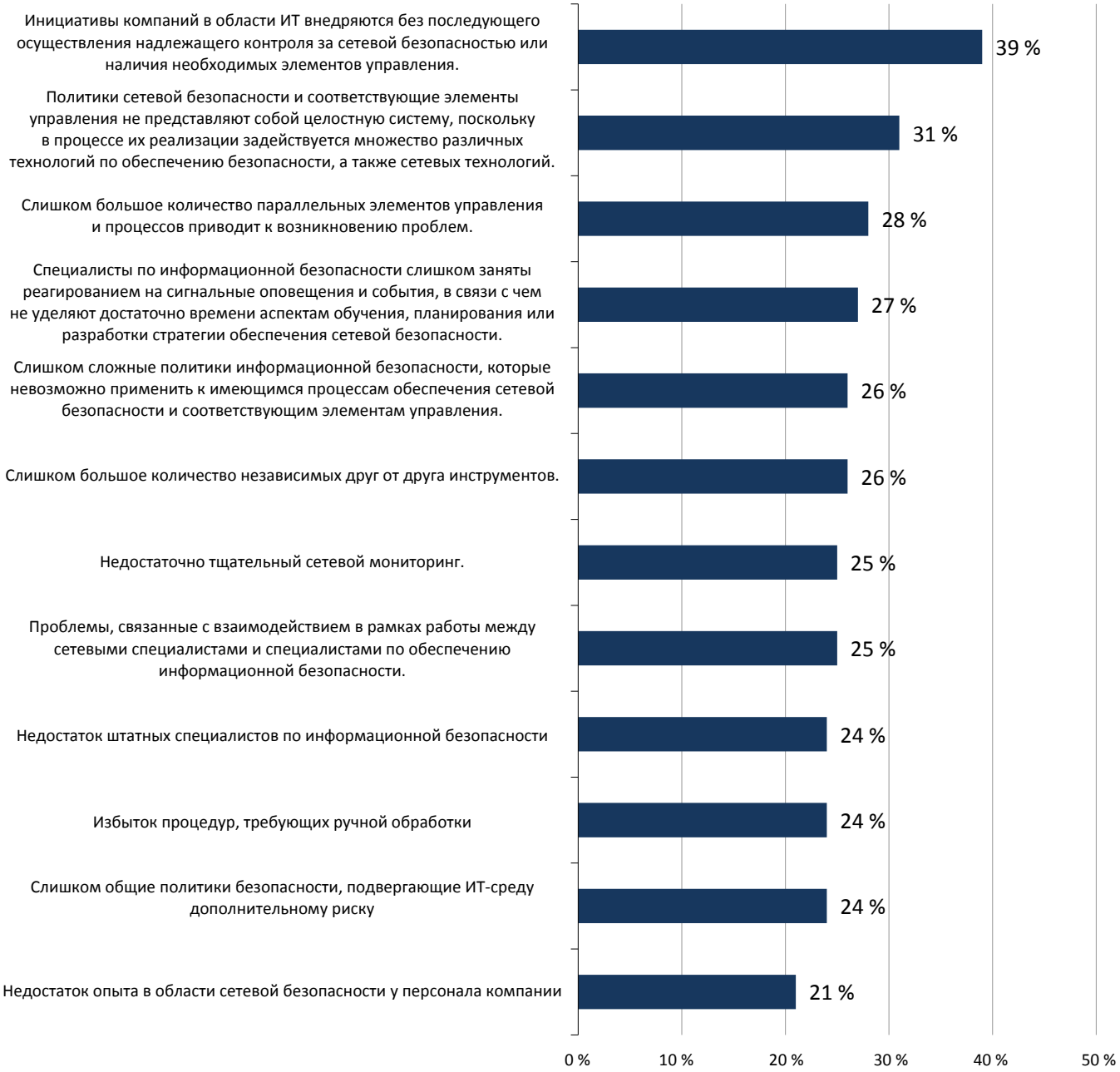
Крупные организации стремительно преобразуют свои устаревшие ИТ-инфраструктуры, внедряя новые инициативы, как, например, приложения на базе облачных вычислений, средства анализа больших данных, а также возможности, предоставляемые мобильностью и Всеобъемлющим Интернетом. Все внедряемые изменения приводят к возникновению ряда задач, связанных с обеспечением сетевой безопасности для структур организации (см. рисунок 1)[1]. Руководителям служб информационной безопасности зачастую приходится сталкиваться с рядом трудностей в рамках обеспечения безопасности, что вызвано следующими факторами:

- **Слишком большое количество разрозненных технологий и приложений, не совместимых с другими аналогичными решениями.** Около одной трети (31 %) организаций сталкиваются с проблемами, вызванными недостаточной совместимостью политик и элементов управления сетевой безопасностью, используемых в рамках одной сети. 28 % организаций приходится решать задачи, возникающие в результате большого количества частично перекрывающихся политик и элементов управления, а у 26 % организаций возникают сложности ввиду использования большого числа независимых друг от друга инструментов. Этот несвязный набор не совместимых друг с другом решений и технологий усложняет решение задач по предотвращению, обнаружению и ликвидации последствий вторжений.
- **Большое количество процессов, выполняемых вручную.** Согласно данным ESG, в большинстве случаев специалисты по безопасности «тушат пожар» вместо внедрения упреждающих политик и процедур в систему безопасности сети. Помимо прочего, 24 % организаций говорят о сложностях, вызванных слишком большим количеством процессов, выполняемых вручную. Методы «тушения пожара» в сочетании с выполняемыми вручную процессами едва ли могут помочь в обеспечении соответствия требованиям по управлению рисками и реагированию на события, имеющим крайне важное значение для обеспечения безопасности современных сетей.
- **Нехватка квалифицированных специалистов по обеспечению безопасности.** По результатам исследований ESG, 24 % организаций испытывают затруднения по причине нехватки сотрудников, отвечающих за вопросы обеспечения безопасности, в то время как 21 % организаций видят причину проблем безопасности в нехватке специализированной подготовки сотрудников. Учитывая глобальную нехватку специалистов по кибербезопасности, можно рассмотреть следующий путь к спасению.

[1] Источник: отчет об исследовании ESG, *Тенденции в области обеспечения сетевой безопасности в эпоху облачных и мобильных вычислений*. Август, 2014 г.

Рисунок 1. Задачи обеспечения безопасности сети

Какие из предложенных ответов можно рассматривать в качестве наиболее серьезных вызовов в отношении обеспечения безопасности сети вашей компании? (Количество ответивших на вопрос (в процентах), N = 397, принимается пять ответов.)



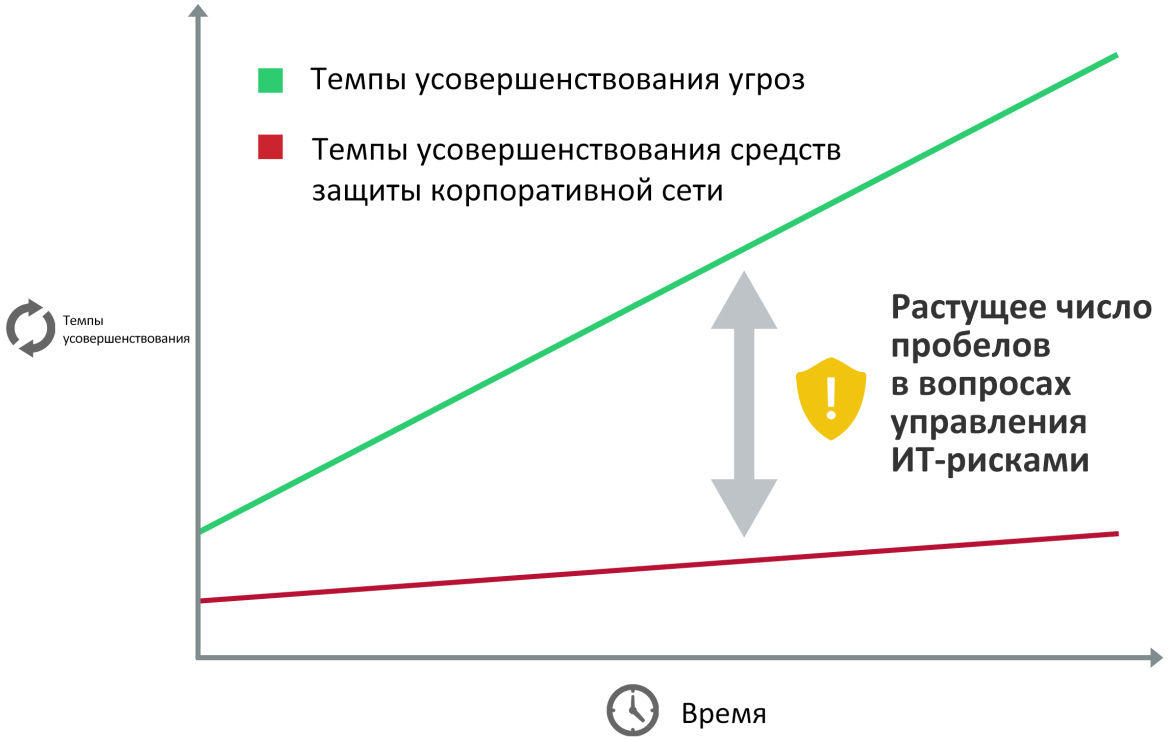
Источник: Enterprise Strategy Group, 2014 г.

«Пробелы» в области обеспечения безопасности сети

Исполнительные и корпоративные директоры должны понимать, что сложные задачи, связанные с обеспечением безопасности, являются составной частью проблемы большего масштаба — проблемы управления рисками кибербезопасности. Устаревшие системы обеспечения безопасности сети, построенные на технологиях и приложениях, не совместимых с их аналогами и выполняемых вручную процессах, не способны противостоять объему, разнообразию и высочайшему уровню современных киберугроз. Использование не связанных между собой решений приводит к образованию «мертвых зон», которые используют в своих целях злоумышленники. Это является одной из причин, по которым в организациях происходят нарушения безопасности: киберпреступники с легкостью используют слабые места системы безопасности, оставаясь вне поля видимости и с легкостью обходя контроль системы безопасности. После захвата «территории» активность хакеров может оставаться незамеченной на протяжении месяцев, в течение которых злоумышленники могут свободно перемещаться по сети, получая доступ к важным для бизнеса системам и, в конечном счете, осуществляя запланированную кражу конфиденциальных данных.

В прошлом руководители отделов безопасности пытались справиться с угрозами кибербезопасности путем постепенного внедрения различных технологий, процессов, а также привлечения дополнительного персонала. Однако сегодня применение подобной стратегии может не принести желаемых результатов. Говоря простым языком, количество и качество кибератак увеличивается экспоненциально вместе с появлением новых технологий и разработкой новых эксплойтов. Альтернативный вариант — постепенное инвестирование в сферу обеспечения безопасности сети приводит к незначительному росту безопасности, особенно в свете описанных выше задач. Данная ситуация приводит к образованию «пробелов» в системе безопасности сети, что, в свою очередь, провоцирует возрастание ИТ-рисков на ежедневной основе (см. рисунок 2).

Рисунок 2. Тактические методы обеспечения безопасности сети провоцируют рост ИТ-рисков



Источник: Enterprise Strategy Group, 2014 г.

Крупные организации нуждаются в интегрированной архитектуре обеспечения безопасности сети, ориентированной на предотвращение угроз

Крупные организации находятся в парадоксальной ситуации: корпоративные сети должны демонстрировать доступность, масштабируемость и готовность к привязке новых ИТ- и бизнес-процессов, однако именно это привело к чрезвычайному росту рисков в области кибербезопасности. Устаревшие элементы управления безопасностью сети не вписываются в стремительно развивающуюся среду ИТ и не менее стремительно укрепляющую свои позиции деятельность киберпреступников.

Каким образом следует действовать? Специалисты ESG полагают, что требования к обеспечению безопасности сети следует рассмотреть в рамках нового подхода к безопасности сети. Делая шаги вперед, руководители отделов информационной безопасности должны рассмотреть безопасность сети в контексте новой архитектурной модели, охватывающей весь «диапазон», от периметра до ядра, а затем — до облака. Специалисты ESG дают следующее определение интегрированной архитектуры безопасности сети:

Интегрированная система, состоящая из аппаратного и программного обеспечения сети, в рамках которой любую услугу обеспечения безопасности можно применить в любой точке внутренней или расширенной сети, как в физическом, так и в виртуальном формфакторе. Помимо прочего, архитектура безопасности сети должна предоставлять возможность внутренней коммуникации, позволяющей всем услугам и компонентам обеспечения безопасности обмениваться и реагировать на информацию в режиме реального времени в целях выполнения точной настройки элементов управления обеспечением безопасности, обнаружения событий, связанных с обеспечением безопасности, а также восстановления скомпрометированных систем.

В основе ориентированной на угрозы архитектуры безопасности сети используются известные современные технологии, а именно межсетевые экраны (межсетевые экраны нового поколения и стандартные межсетевые экраны), системы предотвращения и обнаружения вторжений (IDS и IPS) и другие технологии обеспечения безопасности. Основное отличие заключается в том, что отдельные устройства обеспечивают более высокую степень совместимости и взаимодействия в пределах сети, обмениваясь данными телеметрии и, как следствие, информируя друг друга и действуя сообща. Кроме того, такие функции обеспечения безопасности как межсетевое экранирование, предотвращение и обнаружение вторжений можно рассматривать в качестве услуг, которые могут применяться в пределах локальной сети, корпоративного центра обработки данных или сети поставщика облачной среды — там, где они требуются, и в нужное время.

Для обеспечения интеграции, комплексного покрытия и совместимости ориентированная на угрозы архитектура безопасности сети должна опираться на три ключевых компонента.

1. **Централизованное управление и контроль.**
2. **Распределенное применение.**
3. **Сбор ценной оперативной информации.**

Централизованное управление и контроль

Одна из первоначальных задач, связанных с устаревшими технологиями обеспечения безопасности сети, относится к аспектам управления и выполнения технологических операций. Каждое устройство обеспечения безопасности сети оснащено собственным механизмом обработки политик, выделения ресурсов, настройки и отчетности, что приводит к возникновению проблем, связанных с решением излишних служебных задач. Более того, вам будет крайне трудно (если вообще возможно) сделать выводы о состоянии системы безопасности, исходя из набора отчетов о работе тактических инструментов.

Для смягчения и устранения подобных проблем интегрированная архитектура обеспечения безопасности сети должна перейти к этапу централизованного командования и управления, что позволит решить следующие задачи:

- **Управление сервисами.** Услуги выделения ресурсов, настройки и замены в рамках системы обеспечения безопасности сети требуют централизованного управления с поддержкой интуитивного графического интерфейса пользователя (GUI) и модуля управления рабочими процессами. Кроме того, предоставляемые услуги должны быть совместимы с другими инструментами ИТ. Например, специалисты по безопасности должны иметь возможность выделять ресурсы и выполнять настройку правил межсетевого экранирования, сетей VLAN, ACL-списков маршрутизаторов и коммутаторов, используя один графический интерфейс пользователя. Решение только этой задачи позволит в значительной степени упростить использование элементов управления, отвечающих за обеспечение безопасности сети, повысить уровень защиты и ускорить выполнение технологических операций по обеспечению безопасности сети.
- **Совместимость с виртуализацией серверов и оркестрацией облачных решений.** Высококлассные инструменты, предназначенные для настройки виртуальных рабочих нагрузок для VMware, Hyper-V, OpenStack или AWS, требуют поддержки со стороны соответствующих элементов управления обеспечением безопасности. Наряду с функцией централизованного управления и контроля архитектура безопасности сети предлагает пользователям API-интерфейсы, позволяющие объединить преимущества облачных решений, такие как быстрое выделение ресурсов и самообслуживание, с соответствующими уровнями системы обеспечения безопасности.
- **Мониторинг и создание отчетов.** Помимо функций управления и выполнения операций интегрированная архитектура безопасности сети должна предоставлять возможности централизованного мониторинга и создания отчетов, согласованные с другими видами деятельности, например с управлением событиями. Аналитики по вопросам безопасности должны иметь возможность переходить от одного отчета к другому или сопоставлять несколько отчетов в кратчайшие сроки, чтобы получить четкое представление о состоянии системы безопасности. Для устранения «мертвых зон» в рамках централизованного мониторинга и создания отчетов наряду с физическими устройствами должны контролироваться виртуальные и облачные элементы управления.
- **Расширенный контроль.** Помимо мониторинга аналитиками по вопросам безопасности требуется возможность проведения углубленного контроля сред в целях выявления многовекторных угроз и наблюдения за пользователями, приложениями, контентом и устройствами, присутствующими в сети, а также их поведением, направленным на повышение эффективности политики безопасности и, как следствие, оптимизации выявления угроз и применения ответных действий.

Распределенное применение

Благодаря централизованному управлению и контролю руководители служб информационной безопасности могут создавать глобальные политики безопасности. Однако для их реализации и соблюдения требуются услуги обеспечения безопасности, доступные в пределах сети. Интегрированная архитектура безопасности сети обеспечивает возможность соответствия вышеописанному требованию благодаря такой функции, как:

- **Поддержка для любого формфактора, в любом местоположении.** Услуги обеспечения безопасности сети должны быть доступны в любом местоположении, для любого формфактора и любой комбинации. Это позволяет специалистам по безопасности применять детализированные политики обеспечения безопасности к сегментам сети, потокам, приложениям или отдельным группам пользователей. К примеру, компании розничной торговли могут использовать комбинацию физических и виртуальных элементов управления обеспечением безопасности для того, чтобы POS-системы могли подключаться к устройствам с определенными IP-адресами, используя набор межсетевых экранов, систем обнаружения и предотвращения вторжений, а также усовершенствованных инструментов обнаружения вредоносного ПО. Альтернативный вариант — для пользователей корпоративной локальной сети могут быть настроены другие политики доступа, нежели для сотрудников, работающих из дома и использующих общедоступные сети.

- **Портфель услуг обеспечения безопасности.** Архитектура безопасности сети должна справляться с задачами L2-7, а также поддерживать все типы фильтрации пакетов в любой точке локальной сети, сети WAN или облака. Здесь под «фильтрацией пакетов» подразумевается широкая категория, включающая в себя проверку на наличие угроз, например: вирусов, программных червей, распределенных атак типа «отказ в обслуживании», спама, фишинговых атак, интернет-угроз, утечек контента и атак уровня приложений. Возможность комбинирования различных формфакторов и услуг позволяет предприятиям создавать превосходные многоуровневые стеки, соответствующие различным сетевым потокам, группам пользователей, а также требованиям мобильности, с возможностью быстрой настройки для обнаружения новых типов угроз.
- **Интеграция средств обеспечения безопасности сети и конечных точек.** В прошлом управлением аспектами обеспечения безопасности сети и конечных точек зачастую занимались разные группы специалистов, использующие в корне различающиеся между собой процессы и инструменты. Однако сегодня характер и поведение угроз стали непредсказуемыми, и подобный подход неприемлем. Для решения этой задачи архитектура безопасности сети должна обеспечивать тесную интеграцию между элементами управления безопасностью сети и конечных точек и аналитическими средствами обнаружения угроз. К примеру, элементы управления приложениями, используемые в рамках NGFW и конечных точек, должны быть единообразными, что позволит защитить конфиденциальные данные при подключении пользователей к сети через корпоративную локальную сеть или удаленные общедоступные сети по всему миру. Для оптимизации обнаружения вторжений тестовые аналитические среды должны быть совместимыми с агентами конечных точек, что позволит согласовывать подозрительный аномальный трафик с аномальным поведением системы.

Интегрированные средства сбора ценной оперативной информации

В то время как функционирование ряда технологий обеспечения безопасности сети, например, устройств обнаружения интернет-угроз, систем обнаружения и предотвращения вторжений, а также антивирусных шлюзов обусловлено обновлениями баз данных и подписей, выполняемых из облака, многие другие технологии обеспечения безопасности сети зависят от сотрудников отдела безопасности, которые вносят необходимые изменения или прописывают новые правила для блокировки сетевых подключений. Альтернативный вариант — интегрированная архитектура безопасности сети изначально была задумана как решение «с развитыми логико-информационными возможностями», которое:

- **Работает с использованием нескольких различных источников данных.** В то время как системы на базе платформ для управления событиями и информацией по безопасности (SIEM) производят анализ системы безопасности, исходя из зарегистрированных событий, архитектура безопасности сети предлагает широкий набор данных для анализа. К ним относятся такие основные элементы, как NetFlow и полный захват пакетов, а также детализированные данные технической экспертизы и профилирования конечных точек, схемы доступа устройств или пользователей и аудит облачных приложений. В результате объединения, сопоставления и надлежащего анализа эти новые данные могут помочь организациям оптимизировать систему управления рисками, а также ускорить процессы обнаружения и реагирования на угрозы.
- **Интегрируется с интеллектуальными облачными средствами мониторинга угроз.** Архитектура безопасности сети должна включать интеллектуальные облачные средства мониторинга угроз, предоставляя сведения об уязвимостях программного обеспечения, «плохих» IP-адресах, компрометирующих URL, известных CC-каналах, вредоносных файлах, индикаторах компрометации и быстро изменяющихся схемах атак.
- **Создано для автоматизации.** В конечном итоге, архитектура безопасности сети использует внутренние и внешние интеллектуальные средства обнаружения угроз в целях оказания поддержки организациям в вопросах автоматизации защитных функций и операций системы безопасности. Например, обнаружение аномального трафика в центре обработки данных может инициировать создание правила межсетевого экранирования, согласно которому будут заблокированы потоки, отвечающие ряду таких критериев, как IP-адрес, порт, протокол источника и действия службы доменных имен (DNS). Альтернативный сценарий — при обнаружении вредоносного ПО сеть

выполняет проверку загруженных файлов, а затем выявляет и выполняет восстановление на конечных точках, выполнивших загрузку подозрительных файлов с конкретных URL-адресов. Подобные функции автоматизированного восстановления способствуют непрерывной оптимизации элементов управления системы обеспечения безопасности сети и помогают систематизировать результаты проверок для более быстрого реагирования на угрозы.

В общей сложности, архитектура безопасности сети не только помогает справиться с существующими задачами, но также предоставляет ряд преимуществ для бизнеса, ИТ и обеспечения безопасности (см. таблицу 1).

Таблица 1. Характеристики архитектур обеспечения безопасности сети

Свойство архитектуры обеспечения безопасности сети	Сведения	Функциональность	Преимущества
Централизованное управление и контроль	Управление сервисами, совместимость с виртуализацией серверов и оркестрацией облачных решений, централизованный мониторинг и отчетность.	Централизованное управление политиками, выделение ресурсов, управление процедурами настройки, управление внесением изменений, управление событиями и пр.	Ускоренное выполнение процедур по обеспечению безопасности, простота эксплуатации, централизованный мониторинг и контроль всех элементов системы обеспечения безопасности сети независимо от местоположения и формфактора.
Распределенное применение	Любая услуга обеспечения безопасности сети, в любом местоположении, для любого формфактора, интеграция систем обеспечения безопасности сети и конечных точек.	Согласование услуг в пределах сети, расширение области мониторинга соблюдения политики безопасности до границ облака.	Соответствующая требованиям многоуровневая система обеспечения безопасности для различных сценариев защиты пользователей, устройств и приложений может быть с легкостью усовершенствована или модифицирована с появлением новых типов угроз.
Интегрированные средства сбора ценной оперативной информации	Многообразные источники данных, включая интеллектуальные облачные средства мониторинга угроз.	Предоставляет подробные сведения о трафике приложений, сетевом трафике, поведении конечных точек и появлении новых угроз.	Позволяет сотрудникам отдела безопасности принимать решения, исходя из оперативной информации, полученной в режиме реального времени, автоматизирует процессы восстановления.

Источник: Enterprise Strategy Group, 2014 г.

Архитектура безопасности сети Cisco: межсетевой экран нового поколения, ориентированный на предотвращение угроз

Поскольку Cisco Systems получила признание в области продукции для обеспечения безопасности сети, компания была вынуждена совершенствовать свое представление о технологиях, чтобы предлагаемые решения могли соответствовать растущим требованиям организаций и укрепляющей свои позиции киберпреступности. Для достижения данной цели в 2013 г. Cisco объединила свои усилия с компанией-инноватором в области обеспечения безопасности Sourcefire.

Несмотря на то что в результате слияния Cisco и Sourcefire были объединены усилия и возможности двух гигантов в области обеспечения безопасности, компаниям предстояло выполнить большой объем работы по объединению технологий с целью создания архитектуры обеспечения безопасности сети корпоративного класса. О том, что приложенные усилия начали давать свои плоды, стало понятно, когда было анонсировано появление на рынке многофункционального устройства защиты Cisco ASA с сервисами Firepower.
В результате объединения возможностей межсетевого экрана Cisco ASA, системы предотвращения вторжений Sourcefire нового поколения и расширенных функций защиты от вредоносного ПО в рамках одного устройства корпорация Cisco представила набор услуг обеспечения безопасности, направленный на решение следующих задач:

- **Детальный мониторинг и контроль приложений.** Как и другие межсетевые экраны нового поколения (NGFW), решение Cisco способно выявлять и предоставлять отчеты о подключении приложений и применять политики детального контроля на основе пользователей, групп, устройств и пр. Теперь благодаря сервисам FirePOWER решение Cisco дополняют расширенные возможности мониторинга и контроля приложений в пределах сети наряду с интеграцией этих возможностей с такими ресурсами Cisco, как TrustSec и Identity Services Engine (ISE).
- **Защита по всей сети и конечным точкам, ориентированная на предотвращение угроз.** Архитектура безопасности сети Cisco предоставляет функции комплексной защиты от угроз, обнаружения и предотвращения вредоносного ПО с использованием FirePOWER для обеспечения безопасности сети и FireAMP — для защиты конечных точек. Функции обнаружения и предотвращения угроз дополнены возможностями FirePOWER NGIPS, фильтрации URL-адресов по категории и репутации, а также широким набором интеллектуальных средств мониторинга угроз. FireAMP также имеет функцию отслеживания поведения конечных точек с целью проведения анализа статистических данных. После обнаружения файла с вредоносным ПО FireAMP может применить ретроспективные политики безопасности, чтобы выявить и восстановить конечные точки, которые «сталкивались» с этим файлом в прошлом. И, наконец, решение Cisco объединяет события IPS, интеллектуальные средства мониторинга угроз и события, связанные с вредоносным ПО с целью предоставления детализированных индикаторов вторжения, с помощью которых специалисты отдела безопасности смогут усовершенствовать и автоматизировать проверки, выполняемые системой обеспечения безопасности, а также процедуры восстановления.
- **Широкий набор услуг обеспечения безопасности в сочетании с комплексным контролем состояния сети.** Сегодня Cisco предлагает полноценный портфель физических и виртуальных услуг обеспечения безопасности для межсетевого экранирования, мониторинга приложений, обнаружения и предотвращения вторжений, фильтрации URL-адресов, расширенного обнаружения и предотвращения новейших вредоносных программ и многого другого. Данный портфель услуг позволяет предприятиям настроить свою многоуровневую систему обеспечения безопасности для защиты пользователей, приложений, сегментов сети, а также сетевых потоков с использованием различных формфакторов и полной доступности в пределах сети. Cisco также предоставляет возможности мониторинга и контроля по всем доступным услугам и точкам с целью устранения «мертвых зон».

- **Оценка воздействия.** Архитектура безопасности Cisco разработана для возможности установления взаимосвязи между событиями вторжения и потенциальным воздействием атаки на конкретный объект. Cisco демонстрирует эту взаимосвязь посредством набора из пяти «флажков воздействия». Флажок воздействия под номером один указывает на событие, соответствующее уязвимости, соотнесенной с конкретным узлом, что говорит о необходимости принятия незамедлительных мер. Флажки воздействия под другими номерами имеют более низкий приоритет. Таким образом, Cisco помогает и без того загруженным специалистам отдела безопасности определять участки, в большей степени нуждающиеся в ресурсах, и тем самым оптимизировать работу системы защиты и повышать производственную эффективность.

Специалисты Cisco считают, что объединение возможностей ASA и FirePOWER может оптимизировать защиту на протяжении всего цикла атаки — до ее возникновения, во время ее проведения и по ее завершении. На первом этапе цикла архитектура безопасности Cisco может быть использована для определения сетевых ресурсов, применения политик безопасности и усиления функций элементов управления с целью оптимизации защиты. На протяжении второго этапа цикла атаки возможности ASA и FirePOWER могут оказать поддержку в обнаружении подозрительного поведения (в сети и на конечных точках), блокирования сетевых подключений и, как следствие, обеспечения безопасности сети в целом. И, наконец, в рамках третьего этапа цикла атаки, т. е. по ее завершении архитектура безопасности сети Cisco может помочь аналитикам в вопросах безопасности в определении масштабов воздействия атаки, внесения корректировок в работу элементов управления и использования данных технической экспертизы на новом уровне с целью ускорения процессов восстановления.

Специалисты Cisco знают, что впереди еще много работы — в планах компании на период 12—18 месяцев помимо прочего обозначено внедрение дополнительных функций в архитектуру безопасности. Специалисты Cisco понимают, что многим руководителям отделов информационной безопасности понадобится помощь в оценке имеющихся средств обеспечения безопасности сети и создании плана относительно развертывания архитектуры безопасности. Компания Cisco подготовила ряд предложений по предоставлению специализированных услуг в рамках оказания подобной поддержки организациям.

Проливая свет

Существует ряд общепризнанных фактов относительно кибербезопасности.

1. ИТ становятся все более сложными ввиду привлечения возможностей виртуализации, мобильности и облачных вычислений.
2. Угрозы приобретают более серьезный характер, в то время как целенаправленные атаки все труднее предотвратить, выявить и ликвидировать.
3. Устаревшие средства обеспечения безопасности сети сегодня уже недостаточно эффективны.
4. Многим организациям не хватает имеющихся знаний, вследствие чего в системе обеспечения безопасности образуются пробелы.

В конечном итоге, перед нами стоит достаточно ужасающая картина, в то время как риски кибербезопасности возрастают с каждым днем.

Альберт Эйнштейн однажды сказал: «Безумием является проделывать то же самое снова и снова, каждый раз ожидая иного результата». Мудрое изречение, которое очень точно описывает то, чем занимаются большинство руководителей служб информационной безопасности, когда речь заходит об обеспечении безопасности сети. Руководители направлений, связанных с решением бизнес-задач, ИТ и информационной безопасностью должны осознать, что они ведут обреченную на провал битву. Киберпреступники используют новые типы оружия и тактик, поэтому предприятия должны отвечать на них новыми типами средств защиты, непрерывно совершенствуя инструменты обеспечения безопасности, обнаружения и реагирования.

Специалисты ESG убеждены в том, что наращивание возможностей с помощью устаревших средств защиты не принесет желаемых результатов. Предприятиям необходимо сделать уверенный шаг вперед, используя более стратегический подход, например прибегнув к возможностям интегрированной архитектуры безопасности сети. В результате объединения усилий Cisco и Sourcefire в 2013 г. мы получили решение с непревзойденными возможностями. Теперь, когда Cisco интегрировала ключевые функции межсетевого экрана ASA, FirePOWER NGIPS, усовершенствованной защиты от вредоносного ПО и интеллектуальных средств мониторинга угроз в интегрированную архитектуру безопасности сети, она может рассчитывать на укрепление своих лидерских позиций в отрасли.

Enterprise Strategy Group | **Проливая свет на мир технологий**

Асилум-стрит, 20 | 01757 Милфорд, Массачусетс | Телефон: 508 482 0188 Факс: 508 482 0218 | www.esg-global.com