Защита инфраструктуры и данных компании Cisco — это общая задача наших отделов ИТ и ИБ

Безопасность — это надежные люди, процессы, политики и технологии

КРАТКОЕ СОДЕРЖАНИЕ

ЗАДАЧА

- Защита инфраструктуры и данных
- Обеспечение того, чтобы средства безопасности не осложняли выполнение бизнес-процессов

РЕШЕНИЕ

- Интеграция средств безопасности по всей нашей инфраструктуре
- Внедрение политик и процессов
- Воспитание у сотрудников сознательного отношения к безопасности

РЕЗУЛЬТАТЫ

- Сокращение числа уязвимостей на 65 % в первый год
- Повышение процента закрытия заявок на устранение уязвимостей с 15 до 84 %
- Проведение онлайн-обучения для более чем 25 000 сотрудников с целью воспитания у них ответственного и сознательного отношения к безопасности

РЕКОМЕНДАЦИИ

- Включение экспертов по безопасности в работу ИТ-отделов
- Внедрять политики и технологии везде, где это возможно
- Измерять успех, отслеживая и публикуя показатели по безопасности

ДАЛЬНЕЙШИЕ ШАГИ

- Регулярное обучение сотрудников мерам выявления угроз безопасности и противодействия им
- Внедрение новых технологий по мере развития ландшафта угроз

Исходные данные

Заказчики часто спрашивают нас, как мы в Cisco обеспечиваем защиту нашей международной компании. Для ответа на этот вопрос мы подготовили этот пример внедрения.

Цель компании Cisco — быть не только первой в мире ИТ-компанией, но и лучшей компанией в сфере кибербезопасности. Для защиты инфраструктуры и данных необходимо тесное сотрудничество между нашим отделом ИТ и отделом информационной безопасности (ИБ или InfoSec). В ИБ-отделе работает более 350 сотрудников. ИБ-отдел входит в организацию Cisco Security and Trust Organization (STO) и работает вместе с ИТ-отделом Cisco над задачей обеспечения безопасности создаваемых нами продуктов и используемой нами инфраструктуры. Наша главная цель — защита инвестиций наших заказчиков и нашего собственного бизнеса.

«Мы стремимся работать надежно, прозрачно и понятно», — говорит Мишель Гюэль (Michele Guel), заслуженный инженер и главный архитектор по безопасности компании Cisco. «Это значит, что мы делаем все возможное и невозможное, чтобы найти и обезвредить то, что угрожает нашей инфраструктуре и данным».

Задача

В современном мире организации должны подстраиваться под быстро меняющийся ландшафт угроз. Атаки становятся все более масштабными, сложными, вредоносными и частыми. Проще стало и проводить атаки: программы, в которых достаточно указать на уязвимость в ОС и приложениях и просто щелкнуть мышью, теперь доступны уже спустя несколько дней после обнаружения этой уязвимости.

Защита корпоративной инфраструктуры Cisco® — это сложная система, в которой задействовано 122 000 сотрудников в 170 странах, 3 миллиона IP-адресов, более 40 000 маршрутизаторов, около 26 000 удаленных офисных подключений и 75 миллионов веб-транзакций ежедневно (Годовой отчет Cisco по безопасности за 2016 г.). Задача усложняется еще и тем, что год за годом растет число устройств, подключенных к нашей сети, что обусловлено развитием Интернета вещей (IoT) и нашей программой «принеси на работу свое устройство» (BYOD). По прогнозам, к 2020 году к Интернету будет подключено уже 50 миллиардов устройств.

Все большее число взаимодействий и рост проблем с кибербезопасностью заставляют Cisco и другие организации переосмысливать свой подход к безопасности.

Решение

Комплексный подход

ИТ-отдел и отдел информационной безопасности компании Cisco работают вместе, чтобы обеспечить высокую производительность нашего бизнеса, одновременно защищая наши системы и данные от внутренних и внешних угроз. Мы не фокусируемся только лишь на аппаратном или программном обеспечении для безопасности, мы применяем комплексный, всеобъемлющий подход:

- Воспитание сознательного и ответственного отношения к вопросам безопасности для уменьшения площади атаки и обеспечения надежных механизмов защиты
- Внедрение политик и процессов, ориентированных на безопасность
- Обеспечение безопасности по всей нашей инфраструктуре

Мы стараемся, чтобы эти меры никоим образом не мешали нашим сотрудникам выполнять свою работу. «Некоторые люди воспринимают ИТ-отдел как тех, кто всегда говорит «нет», а отдел по информационной безопасности — как тех, кто говорит «нет» даже тогда, когда ИТ говорит «да», — говорит Мариса Ченселлор (Marisa Chancellor), старший директор по информационной безопасности в компании Cisco. — Нам бы не хотелось, чтобы наши сотрудники думали, что им придется все время спрашивать разрешения у ИТ- и ИБ-отделов на выполнение своих рабочих задач».

Наш комплексный подход к безопасности объединяет людей, процессы, политики и технологии.

Люди

Наши люди — это первая и важнейшая линия обороны во всей защите компании Cisco. Мы привлекаем консультантов по безопасности и работаем над воспитанием ответственного и сознательного отношения к вопросам безопасности во всей компании.

Консультанты по безопасности

В нашем ИТ-отделе работают консультанты по безопасности двух типов:

- Ведущие специалисты по услугам безопасности (Security Service Primes, SSP), которые отвечают за комплексную безопасность одной или нескольких из наших 200 ИТ-услуг, как, например, совместная работа или «данные как услуга». По существу, эти ведущие специалисты — главные лица, которые отвечают за безопасность этой услуги.
- Архитекторы-партнеры по безопасности (Partner Security Architects, PSA), которые, играя роль ведущих сотрудников по техническим вопросам безопасности, отвечают за оценку архитектуры безопасности ИТ-проектов и приложений.

Несмотря на то, что консультанты по безопасности напрямую не работают в отделе информационной безопасности, они проходят обучение основам безопасности (25 часов) и регулярно повышают свою квалификацию, проходя отдельные курсы (1 час). «Ведущие специалисты по услугам безопасности и архитекторы по безопасности помогают команде информационной безопасности встроить процессы безопасности в структуру ИТ-отдела и масштабировать эти процессы необходимым образом», — говорит Суджата Рамомурти (Sujata Ramamoorthy), директор по информационной безопасности ИБ-отдела.

Культура ответственного отношения к вопросам безопасности

Ответственное отношение сотрудников к вопросам кибербезопасности и своей роли в защите своей организации позволяет значительно уменьшить возможные уязвимости или вовсе устранить их. ИТ- и ИБ-отделы вместе работают над воспитанием такого ответственного и осознанного подхода. Программа состоит из следующих частей.

- Программа онлайн-обучения кибербезопасности: более 25 000 сотрудников и подрядчиков Cisco по всему миру приняли участие в программе онлайн-обучения Cisco Security Ninja. Пройдя серию 20-минутных модулей, разработанных экспертами Cisco, сотрудники получали сертификаты с присвоением белого, зеленого, коричневого или черного пояса. Обучение доступно для менеджеров, инженеров по программному или аппаратному обеспечению и нетехнических сотрудников. На сегодняшний день около 60 % сотрудников Cisco прошли обучение и получили белый пояс.
- Обучение противодействию фишинговым атакам: каждый квартал мы отправляем тестовое письмо с фишинговой атакой 130 000 нашим сотрудникам и подрядчикам, у которых есть адреса электронной почты Cisco. Сотрудники, которые щелкают на ссылку из письма, видят веб-страницу с сообщением о том, что если бы эта ссылка оказалась реальной, этот сотрудник мог бы поставить под угрозу безопасность всей компании Cisco. Далее на этом сайте приводится подробное объяснение, как распознать электронное письмо с фишинговой атакой. Спустя три недели после теста сотрудники, которые щелкнули на ссылку в первый раз, получают еще одно тестовое письмо. Некоторые фишинговые электронные письма очень убедительны, и по нашей ссылке в первом тестовом письме щелкали многие. Но обучение помогло. «Если брать все компании, то в среднем число щелчков по ссылкам в фишинговых электронных письмах составляет 30 %, —

говорит Дейв Вандер Мейр (Dave Vander Meer), менеджер по услугам ИБ-отдела Cisco. — Мы же значительно сократили это число среди наших сотрудников».

- Кодекс корпоративной этики: каждый год сотрудники Cisco подписываются под документом «Кодекс корпоративной этики». Защита данных — это такая же важная часть этого кодекса, как этическое поведение и ответственное использование корпоративных ресурсов. Соглашаясь с правилами корпоративного поведения, сотрудники обязуются со всей ответственностью относиться к данным, с которыми они работают, кому бы ни принадлежали эти данные — заказчикам, партнерам или самой компании.

Процессы

В качестве примеров процессов, которые мы используем для защиты нашей инфраструктуры, можно привести публикацию унифицированных показателей безопасности (Unified Security Metrics, USM) и регулярное проведение тестов на возможность проникновения.

Ежеквартальные унифицированные показатели безопасности

Без полных статистических данных об оценке состояния безопасности услуг, владельцы ИТ-услуги и руководители могут ошибочно считать, что их услуга безопасна и надежно защищена. Отдел информационной безопасности ежеквартально публикует показатели USM (см. таблицу 1). Эти показатели рассчитываются с использованием данных из разных источников, например, ИТ-журналов и результатов тестов на возможность проникновения. Для каждого показателя мы указываем число уязвимостей и процент своевременно решенных проблем, связанных с уязвимостями, о которых было сообщено в предыдущем квартале.

Таблица 1. Унифицированные показатели безопасности, передаваемые ИБ-отделом владельцам ИТ-услуг и руководителям

Унифицированные показатели безопасности	Что измеряет
Соответствие стеку	Уязвимости, найденные в сетевых устройствах, операционных системах, серверах приложений и промежуточном ПО.
Соответствие средствам защиты от вредоносных программ	Проверка правильности установки и актуальности ПО для защиты от вредоносных программ.
Базовая оценка уязвимости приложений	Проверка автоматического выполнения сканирования системы на уязвимость. Проблемы безопасности, которые остаются после сканирования.
Глубокая оценка уязвимости приложений	Проводится ли тест на возможность проникновения для критически важных для бизнеса приложений в соответствии с политикой Cisco. Проблемы безопасности, которые остаются после сканирования.
Отклонения от проекта	Количество открытых проблем безопасности, определяемых как отклонение от установленных стандартов и практических рекомендаций по обеспечению безопасности.

Цель публикации показателей USM — помочь владельцам ИТ-услуг быстро диагностировать, локализовать и устранить проблемы, связанные с безопасностью. «Когда по результатам USM выяснилось, что только 15 % выявленных уязвимостей устраняется вовремя, и, по сути, в остальное время Cisco подвергается угрозе, владельцы ИТ-услуг вызвались увеличить эту цифру до 84 % в течение года», — говорит Рамамурти.

> «Когда по результатам USM выяснилось, что только 15 % выявленных уязвимостей устраняется вовремя, и, по сути, в остальное время Cisco подвергается угрозе, владельцы ИТ-услуг вызвались увеличить эту цифру до 84 % в течение года»,
>
> — Суджата Рамамурти (Sujata Ramamoorthy), директор по информационной безопасности ИБ-отдела Cisco

Cisco направляет атаки на собственную компанию

Мы регулярно атакуем нашу собственную компанию, чтобы выявить пробелы с безопасностью, пока их не нашли злоумышленники. Благодаря такому проактивному подходу ИБ-отдел получает аналитические данные об уязвимостях операционной системы и приложений. Мы регулярно сканируем сеть, чтобы находить и устранять уязвимости. Области повышенного риска сканируются ежедневно, а вся компания — ежемесячно.

Отчет об уязвимостях, генерируемый в результате этих сканирований, автоматически отправляется владельцу ИТ-услуги. ИБ-отдел и владелец услуги вместе оценивают полученные результаты, так как ИТ-отдел Cisco владеет активами, подвергающимися риску. «Мы смотрим, какие системы и данные уязвимы и насколько они важны

для Cisco, — говорит Дэвид Белл (David Bell), менеджер команды по управлению уязвимостями ИБ-отдела. — Затем мы сообщаем ИТ-отделу, в какие системы необходимо внести исправления сегодня, а не, скажем, через 30 дней».

Менеджеры по ИТ-услугам входят в систему сканирования ИБ-отдела и смотрят, какие уязвимости были обнаружены в их зоне ответственности, например в настольных ПК или маршрутизаторах. Владелец услуг использует инструмент управления активами ИТ-отдела Cisco для выявления всех устройств с уязвимостями, например системы хранения или определенной операционной системы. Затем владелец услуги самостоятельно закрывает заявку, не привлекая к этому ИБ-отдел. Скорость решения вопроса по заявке отражается в USM.

Политики

Согласно нашему подходу, ориентированному на людей и процессы, мы внедряем и политики, ориентированные на обеспечение безопасности. В таблице 2 представлены политики, которые ИБ-отдел применяет для защиты нашей инфраструктуры и данных.

Таблица 2. Комплексный подход к безопасности включает политики безопасности

Политика	Содержание
Допустимое использование	Требования к допустимому использованию информации, электронных и вычислительных устройств и сетевых ресурсов в соответствии с нашей культурой этического и законопослушного поведения, открытости, доверия и честности.
Управление доступом	Требования к управлению доступом пользователей и администраторов к информационным ресурсам и информационным системам с использованием соответствующих инструментов для аутентификации, авторизации и учета.
Защита приложений	Требования, которым должно соответствовать приложения, чтобы уменьшить риск для критически важной инфраструктуры и информационных ресурсов, связанный с уязвимостями в проекте, коде и инфраструктуре приложения.
Аудит	Требования к аудиту и оценке рисков, которые должны проводиться, чтобы гарантировать соответствие политикам безопасности, целостности данных, расследованию инцидентов или мониторинга активности пользователей/систем, если это применимо.
Безопасность облака	Минимальные требования к безопасности облаков, которые мы используем для ведения бизнеса Cisco или для создания собственных облаков (услуг на хостинге).
Управление инцидентами, связанными с компьютерной безопасностью	Требования к управлению инцидентами, связанными с компьютерной безопасностью, включая, но не ограничиваясь, обнаружение атак, реагирование на атаки, проведение расследований, мониторинг и создание журналов.
Криптографические средства управления	Требования к использованию криптографических средств управления для защиты конфиденциальности, целостности и доступности информационных ресурсов.
Защита данных	Требования к классификации, маркировке и защите данных. Определение относительной конфиденциальности информации и того, как следует обращаться с этой информацией и раскрывать ее сотрудниками Cisco и другим сторонам.
Информационная безопасность	Требования к управлению информационной безопасностью и к конфиденциальности, целостности и доступности информационных ресурсов.
Защита интеллектуальных активов	Требования к защите интеллектуальных активов Cisco.
Защита лабораторных исследований	Требования к информационной безопасности для управления и защиты лабораторных ресурсов и сетей Cisco за счет минимизации угроз для критически важной инфраструктуры и информационных ресурсов, которые могут быть связаны с незащищенными хостами и неавторизованным доступом
Доступ к сети	Требования к авторизованным пользователям и устройствам для доступа к корпоративным сетям.
Пароль	Требования к созданию, защите и управлению учетными данными для надежной аутентификации.
Безопасность сервера	Требования к серверному оборудованию для минимизации угроз для критически важной инфраструктуры и информационных ресурсов Cisco, которые могут быть связаны с незащищенными хостами и неавторизованным доступом.

Политики, приведенные в таблице 2, соответствуют проверенным лучшим практическим методикам и отраслевым сертификатам ISO 27001. «ИБ-отдел отвечает за эти политики и вместе с ИТ-отделом и другими отделами Cisco мы внедряем нужные средства управления и контроля», — говорит Уандер Мейер (Vander Meer). Например, ИБ-отдел устанавливает требования к паролю. ИТ-отдел Cisco применяет эту политику, настраивая процессы сброса пароля и управления устройствами таким образом, что все пароли, не соответствующие заданным критериям, будут отклоняться. Другой пример — доступ к сети. ИБ-отдел определяет требования к устройствам, включая требования к защите от вредоносного ПО, к операционной системе и разным другим настройкам. ИТ-отдел Cisco готовится к использованию системы Identity Services Engine (ISE) для автоматического внедрения этой политики. Например, устройство сотрудника получает полный доступ к сети, если оно удовлетворяет всем требованиям. В противном случае доступ будет ограничен или заблокирован.

В 2005 году Cisco совместно с компанией SANS, крупнейшим в мире центром по обучению и сертификации в области информационной безопасности, создали универсальные версии большинства политик безопасности Cisco, доступных в виде шаблонов на веб-сайте SANS Security Policy Resource. Заказчики могут воспользоваться этими шаблонами в качестве основы для создания собственных политик безопасности.

Технологии

Мы используем технологии Cisco и третьих сторон для защиты данных и систем на всем протяжении атаки, как показано в таблице 3.

Таблица 3. Технологии Cisco для обеспечения безопасности, используемые на всем протяжении атаки

Стратегия	Наша технология
ДО АТАКИ: ВНЕДРЕНИЕ ПОЛИТИК И СРЕДСТВ УПРАВЛЕНИЯ	
Защита от вредоносного ПО	Cisco Web Security Appliance (WSA)[1] Cisco Email Security Appliance (ESA)[2] Cisco Advanced Malware Protection (AMP) Cisco Intrusion Prevention System (IPS)
Политики, соответствие нормативным правилам и управление устройствами	Cisco Identity Services Engine Cisco ASA Adaptive Security Appliances Cisco Application Centric Infrastructure Cisco Prime Infrastructure
Управление уязвимостями	Qualys Инструменты анализа кода третьих фирм Инструменты управления уязвимостями третьих фирм
Предотвращение утечки данных	Решение третьих фирм
Защита веб-приложений	Решение третьих фирм
ВО ВРЕМЯ АТАКИ: ОПРЕДЕЛЕНИЕ И БЛОКИРОВАНИЕ	
Сбор данных и обнаружение	Cisco Intrusion Prevention System Cisco FireSIGHT® Management Center Cisco AMP ThreatGrid Appliance Cisco Stealthwatch
Подавление	Cisco ISE для внедрения политик Security Group Tagging Cisco Application-Centric Infrastructure
Анализ угроз, с помощью которого WSA и ESA блокируют вредоносные веб-сайты и сообщения электронной почты	Группа Talos по аналитике и исследованиям безопасности SenderBase®, крупнейшая в мире сеть мониторинга веб-трафика и электронной почты
ПОСЛЕ АТАКИ: АНАЛИЗ И ВОССТАНОВЛЕНИЕ	
Создание отчетов и обработка инцидентов	Аналитика Cisco Stealthwatch с данными NetFlow
Расследования и анализ	Cisco AMP ThreatGrid Appliance Cisco FireSIGHT Management Center.

1. Устройство защиты веб-трафика (WSA) ежедневно блокирует 1,2 миллиона из 75 миллионов веб-транзакций.
2. Устройство защиты электронной почты (ESA) блокирует 94 % входящей электронной почты на периметре сети.

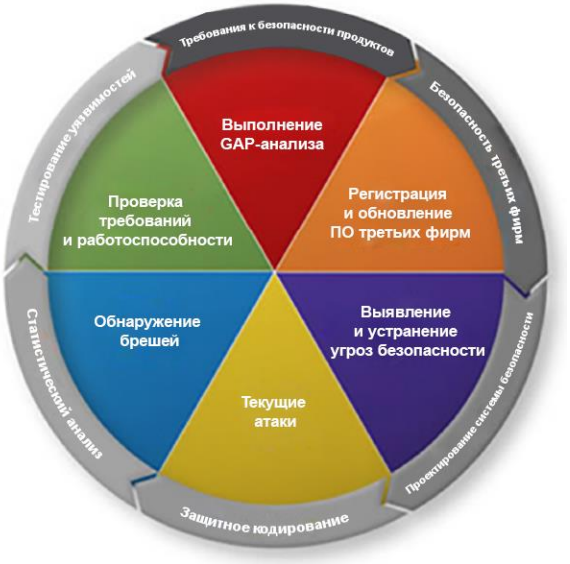
Надежные, заслужившие доверие продукты и инфраструктура

Основа безопасности предприятия — надежные и заслужившие доверие продукты и инфраструктура. «ИТ-отделы должны закупать полный набор технологий (инфраструктура, вычислительные ресурсы, системы хранения и приложения) у поставщиков, которые выполняют необходимые процессы, гарантирующие, что их решениям можно доверять», — говорит Стив Мартино (Steve Martino), директор Cisco по информационной безопасности. Начиная с 1995 года компания Cisco встраивает технологии обеспечения безопасности в продукты, которые мы производим для наших заказчиков и нас самих (см. рис. 1).

Рисунок 1. Этапы построения интегрированной модели безопасности

Для дальнейшего снижения числа уязвимостей и повышения надежности в 2008 году мы внедрили жизненный цикл разработки решений по безопасности (Secure Development Lifecycle, SDL). SDL — это обязательный, повторяемый и измеряемый процесс для разработки безопасных, надежных и заслуживающих доверия продуктов (см. рис. 2). Согласно этому процессу, безопасность должна стать основным фактором при создании продуктов и решений. Процесс удовлетворяет требованиям методологии разработки продуктов Cisco Product Development Methodology (PDM) и ISO 9000, а также поддерживает среды разработки Agile и Waterfall. Благодаря процессу SDL в основе нашего портфеля продуктов и глобальной инфраструктуры лежат фундаментальные технологии обеспечения безопасности, такие как защита при запуске и во время выполнения программы.

Рисунок 2. Жизненный цикл разработки решений Cisco по обеспечению безопасности



Результаты

Для оценки результативности наших операций по безопасности мы используем следующие показатели.

Своевременное решение проблем с уязвимостями

ИТ- и ИБ-отделы Cisco согласовывают условия соглашений об уровне обслуживания (SLA) для решения проблем, связанных с уязвимостями. Целевое время выполнения заявки зависит от серьезности уязвимости. «В первый год после внедрения показателей USM нам удалось сократить число уязвимостей на 65 %, — говорит Мартино. — Показатель своевременного закрытия заявок по уязвимостям вырос с 15 до 84 %».

Ежегодные убытки: ожидаемые и реальные

Ожидаемые ежегодные убытки (Annual Loss Expected,ALE), связанные с инцидентами по безопасности, основываются на отраслевых исследованиях. Мы сравниваем показатели ALE с нашими собственными реальными ежегодными убытками (Annual Loss Realized,ALR), включающими затраты на оплату труда, оборудование, ПО, ремонт аппаратуры, утечку данных и ущерб репутации бренда. Наша главная задача — добиться, чтобы реальные убытки стали ниже ожидаемых. Наша бизнес-цель — четко и ясно продемонстрировать, как хорошо мы защищаем нашу собственную компанию, и тем самым завоевать доверие наших заказчиков и партнеров.

Основные контрольные показатели

В 2014-м и 2015 годах мы измеряли, насколько наши внутренние процессы и средства управления соответствуют основным контрольным показателям Центра информационной безопасности (Center for Internet Security, CIS). Центр CIS утвердил 20 категорий контрольных показателей, включая защиту от вредоносного ПО, управление беспроводным доступом, непрерывную оценку уязвимостей и их устранение, а также учет авторизованного и неавторизованного ПО. Измерение основных контрольных показателей отражает, насколько сильны наши механизмы защиты в заданный момент времени, и помогает нам эффективно выявлять проблемы. В 2016 году мы планируем внедрить контрольные показатели версии 6.0, в которой используется метод измерения на основе повторяемости и согласованности.
Каждая категория контрольных показателей имеет четыре уровня достижимости, которые показаны на вертикальной оси на рис. 3:

- Уровень 1: быстрые победы
- Уровень 2: улучшение мониторинга и атрибуции
- Уровень 3: конфигурация и очистка
- Уровень 4: продвинутый уровень

Наша таблица основных контрольных показателей состоит из 80 ячеек (20 контрольных показателей x 4 уровня). В 2016 году мы хотим присвоить каждой ячейке одну из пяти оценок: «соответствует», «в большей степени соответствует», «в процессе», «не относится к культуре Cisco» или «пропуск без дальнейших планов по корректировке». (Примеры контрольных показателей, не относящихся к культуре Cisco, включают неработающие USB и оконечные устройства из белого списка.) ИБ-отдел присваивает оценки, руководствуясь информацией, полученной от специалистов SSP и PSA ИТ-отдела Cisco.

На рис. 3 представлен пример таблицы основных контрольных показателей, посмотрев на которую, наш совет директоров и наши заказчики сразу могут составить себе ясное представление о ситуации с обеспечением безопасности в нашей компании. Эта таблица также помогает принять решение о том, инвестиции в какие области важнее всего в данный момент.

Рисунок 3. Ежеквартальная оценка 20 основных контрольных показателей

Число угроз

В ежедневном отчете команды CSIRT представлено число угроз, которые были предотвращены нашими решениями по безопасности, например число DNS-атак, предотвращенных на уровне межсетевого экрана. Система анализа больших данных команды по реагированию на инциденты, связанные с компьютерной безопасностью (Computer Security Incident Response Team, CSIRT), создает отчет. «Проанализировав число угроз, которые удалось предотвратить, мы можем понять, какие решения по безопасности оказались наиболее эффективными, — говорит Гюйель. — И, соответственно, принять решение об инвестициях».

> «Проанализировав число угроз, которые удалось предотвратить, мы можем понять, какие решения по безопасности оказались наиболее эффективными. И, соответственно, принять решение об инвестициях».
>
> — Мишель Гюйель (Michele Guel), главный архитектор по безопасности, Cisco

Время на обнаружение/локализацию инцидентов

Еще один способ, с помощью которого мы измеряем эффективность наших решений по безопасности, — это контроль времени обнаружения (Time to Detect, TTD) и времени локализации (Time to Contain, TTC) инцидентов безопасности. В апреле 2015 года среднее время TTD было 6 часов, а среднее время TTC — 168 часов. В феврале 2016 года наше среднее время TTC уже составило почти 24 часа.

Мы относим событие к «инцидентам», только если нарушение безопасности связано с вредоносным ПО, неавторизованным доступом или неправомочным использованием. Если наши системы блокируют события, мы не рассматриваем их как инциденты. «Мы ежедневно блокируем миллионы потенциальных событий нарушения безопасности», — говорит Мартино. «Из-за того что мы не включаем эти блокируемые события в наши измерения, мы можем сфокусироваться на борьбу с теми угрозами, которые прорвали наш первый уровень обороны».

Сравнивая время TTD и TTC с эталонным временем, мы можем:

- Подстраивать возможности измерений и обнаружения инцидентов
- Сотрудничать с поставщиками на предмет повышения производительности
- Постоянно совершенствовать наши возможности сдерживания атак, например атрибуцию и помещение в карантин

Дальнейшие шаги

Ландшафт угроз продолжает развиваться быстрыми темпами. Защита наших данных и систем требует комплексного подхода, пристального внимания и постоянного обеспечения безопасности. «Мы продолжаем внедрять инновации, используя людей, процессы, политики и технологии, чтобы соответствовать быстро меняющимся бизнес-требованиям и ландшафту угроз, — говорит Мартино. — Мы создали прочную основу для проведения политики безопасности Cisco и обеспечения ее надежности и постоянного совершенствования».

Наши планы:

- Интеграция безопасности в наши среды разработки и непрерывная реализация стратегии
- Масштабирование нашей архитектуры безопасности в соответствии с ростом и развитием Интернета вещей
- Улучшение мониторинга и контроля использования облачных решений третьих сторон в соответствии с положениями нашей статьи Обеспечение безопасности облачных приложений третьих сторон

Рекомендации

ИТ- и ИБ-отделы Cisco предлагают организациям, заинтересованным в реализации механизмов безопасности, воспользоваться следующими рекомендациями.

- Тщательно выбирайте политики. Проще и эффективнее внедрять и управлять 10 политиками, чем 30. Если ваши политики сложны для понимания и трудновыполнимы, пользователи будут стараться найти способы их обойти.
- Попробуйте взять за образец шаблоны политик на веб-сайте SANS Security Policy Resource. Там представлены обобщенные версии политик Cisco.
- Дайте владельцам ИТ-услуг возможность контролировать состояние их безопасности, регулярно публикуя показатели безопасности.
- Внедряйте ответственный и сознательный подход к безопасности среди сотрудников, проводя онлайн-обучение. Модули не должны быть длинными — лучше не дольше 10 минут. Безопасность должна ассоциироваться с конкретными людьми — приглашайте экспертов по безопасности для разработки и записи материалов курсов. Ищите способы мотивации сотрудников для прохождения обучения.

- Поощряйте финансирование стратегических инициатив по безопасности, дополнительно к тактическим проектам. Наши директора по ИТ и ИБ вместе выступают спонсорами программы Pervasive Security Accelerator. Кроме того, в рамках этой программы финансируются программы с привлечением специалистов Security Service Primes и измерения показателей USM.

Дополнительная информация

В 2016 году на конференции RSA компания Cisco стала победителем в номинациях «Лучшая компания в области информационной безопасности» и «Лучший отдел по информационной безопасности». Дополнительную информацию см. на сайте http://blogs.cisco.com/security/cisco-security-leadership-at-2016-rsa-conference.

Для получения дополнительной информации об управлении рисками кибербезопасности посетите страницу нашего центра Trust and Transparency Center.

Для получения дополнительной информации о жизненном цикле разработки решений по безопасности посетите сайттwww.cisco.com/web/about/security/cspo/csdl/.

Годовой отчет Cisco по безопасности за 2016 год

Для ознакомления с примерами внедрения различных бизнес-решений ИТ-отделом Cisco посетите сайт Cisco: работа ИТ-отдела Cisco изнутри www.cisco.com/go/ciscoit

Примечание

В этой публикации рассказывается о том, какие преимущества компания Cisco получает от развертывания собственных продуктов. На результат и описываемые преимущества могут влиять самые разные факторы. Компания Cisco не гарантирует получение аналогичных результатов в других случаях.

КОМПАНИЯ CISCO ПРЕДОСТАВЛЯЕТ ДАННУЮ ПУБЛИКАЦИЮ БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, КАК ПРЯМЫХ, ТАК И КОСВЕННЫХ, ВКЛЮЧАЯ КОСВЕННЫЕ ГАРАНТИИ КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КОНКРЕТНЫХ ЦЕЛЕЙ.

В соответствии с законодательством отдельных стран или территорий отказ от прав в явном или подразумеваемом виде не допускается, следовательно, настоящее заявление об ограничении ответственности может к вам не относиться.

Россия, 121614, Москва,
ул. Крылатская, д.17, к.4 (Krylatsky Hills)
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru, www.cisco.com

Казахстан, 050059, Алматы, бизнес-центр «Самал Тауэрс», ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, «Лэндмарк» здание III, 3 этаж
Телефон: +994 (12) 437 4820, факс: +994 (12) 437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998 (71) 140 4460, факс: +998 (71) 140 4465