FORTINET

РОСТ РИСКОВ И СНИЖЕНИЕ ЭФФЕКТИВНОСТИ В РЕЗУЛЬТАТЕ РАЗДЕЛЕНИЯ NOC И SOC

ИССЛЕДОВАНИЕ

АННОТАЦИЯ

Несомненно, иногда у руководителей по безопасности возникает ощущение, что они вынуждены подниматься по эскалатору, идущему вниз. Мы живем в эпоху стремительной цифровой трансформации, которая приводит к появлению новых направлений атак, увеличивает нагрузку и усложняет управление безопасностью. Наряду с этими проблемами возникают и другие: по мере появления новых угроз защититься от них становится все сложнее. Ограниченность ресурсов приводит к сужению охвата и эффективности систем безопасности. Сотрудники отделов информационной безопасности и обслуживания сетей попали в сердце этого шторма — они вынуждены решать противоположные друг другу задачи. Операторы сетевых операционных центров (NOC) стремятся к максимальному увеличению пропускной способности, времени бесперебойной работы и доступности, в то время как сотрудники центров выполнения операций безопасности (SOC) для определения эффективности своей деятельности используют показатели выявления и блокировки угроз.

Однако реальность такова, что в условиях обособленности подходов система не поддерживает гибкое масштабирование в целях блокировки новых направлений атак, упрощения управления безопасностью и противодействия современным продвинутым угрозам. Команды NOC испытывают затруднения в процессе борьбы с угрозами безопасности, а сотрудники SOC не могут адаптировать решение к требованиям сетей и успешно противостоять стремительным атакам и меняющимся угрозам. Кроме того, изолированность центров NOC и SOC, отсутствие систем и средств взаимодействия и обмена данными об угрозах и состоянии сети приводит к снижению эффективности работы и росту рисков безопасности.

УСЛОЖНЕНИЕ ЗАЩИТЫ КОРПОРАТИВНЫХ СЕТЕЙ В СВЯЗИ С ПОЯВЛЕНИЕМ НОВЫХ НАПРАВЛЕНИЙ АТАК

Почти все организации нашли себе место на «скором поезде» цифровой трансформации. Внедрение цифровых технологий практически во все области бизнеса принципиально изменило бизнес-операции и модель предоставления услуг клиентам. Цифровая трансформация создает все предпосылки для коммерческого успеха: в частности, это повышение гибкости, ускорение внедрения инноваций и рост прибыли.

Однако новые бизнес-возможности сопряжены с трудностями. Цифровая трансформация требует соответствующей модернизации системы безопасности, в противном случае организация станет уязвима для атак. Согласно недавнему исследованию Cybersecurity Ventures, по итогам четырехлетнего периода, заканчивающегося в 2021 г., объем рынка информационной безопасности превысит 1 трлн долл. США.[1] Однако, несмотря на все предосторожности и рациональное распределение ресурсов, киберугрозы по-прежнему представляют собой реальную опасность, и их количество продолжает расти. Согласно прогнозу, приведенному в другом исследовании Cybersecurity Ventures, к 2021 г. ущерб от деятельности киберпреступников достигнет 6 трлн долл. США.[2]

Часть проблемы заключается в росте количества уязвимых *пользователей*. В настоящее время более половины населения мира имеют доступ к сети,[3] растет и число пользователей, которые не помнят время до появления Интернета. Таким образом, организации вступают в процесс цифровой трансформации в целях удовлетворения потребностей клиентов и сотрудников в доступе к цифровым технологиям. Эти потребности обширны и разнообразны. К примеру, более дальновидные организации предоставляют клиентам и сотрудникам доступ к данным в режиме реального времени, непрерывно разрабатывают и развертывают новые приложения и создают возможности для совместной работы при поддержке цифровых технологий.

Другим аспектом проблемы является рост количества векторов атак. Быстрое распространение устройств с подключением к Интернету вещей (IoT), рост объема трафика приложений и больших данных, появление сложных и высокоэластичных многооблачных сред, а также увеличение количества мобильных пользователей, нуждающихся в доступе к сети в любое время, — все эти факторы приводят к перегрузке ресурсов безопасности. Результатом стало появление так называемых «лишенных границ сетей».

Распространение технологии IoT служит одним из самых ярких примеров назревающих проблем безопасности. За счет свободного доступа к сетям эта технология создает уязвимости, которым сложно противостоять в рамках традиционных подходов к безопасности. Некоторые устройства IoT лишены собственных средств управления, что делает недоступными такие традиционные методы защиты, как обновления и исправление уязвимостей. Киберпреступники осведомлены об этой проблеме и стремятся использовать уязвимости в своих интересах. Чтобы проиллюстрировать масштабы проблемы, хакеры на конференции по вопросам безопасности DEF CON 2016 выявили 47 новых уязвимостей, затрагивающих 23 устройства от 21 производителя.[4] В ходе четырехдневной конференции, помимо других возможных вариантов использования технологий в противоправных целях, хакеры нашли способы дистанционно разблокировать замки с поддержкой IoT, физически повреждать солнечные батареи и шпионить за людьми.

Угроза со стороны IoT более чем реальна. Например, целью трех из десяти наиболее успешных атак в последнем квартале 2017 г. были устройства IoT. Новые IoT-ботнеты, такие как Reaper и Hajime, способны одновременно поражать миллионы уязвимостей. Круг целевых устройств необычайно широк. В качестве лишь одного примера из многих можно отметить то, что частота поражения Wi-Fi камер эксплойтами возросла в четыре раза.[5]

Другая технология, размывающая периметр корпоративной сети, — это программно-конфигурируемая глобальная сеть (SD-WAN). Технология SD-WAN снижает совокупную стоимость владения (TCO), поэтому наиболее активно ее внедряют организации с разветвленной сетью филиалов, ведущие свою деятельность в разных местоположениях. Решения SD-WAN устраняют необходимость в дорогостоящих процедурах обратной передачи трафика филиалов в сеть за счет использования более дешевых интернет-подключений между местоположениями одновременно с повышением пропускной способности и скорости.

Тем не менее, несмотря на преимущества решения SD-WAN, оно также создает риски безопасности. Существует множество различных систем SD-WAN. Организациям необходимо внимательно изучить варианты и убедиться в том, что выбранное решение повышает эффективность сети без ущерба для безопасности благодаря балансу функций защиты и сетевых функций. В частности, в результате развертывания SD-WAN в среду безопасности, и без того состоящую из специализированных решений, нередко внедряются новые изолированные продукты. Это усложняет управление безопасностью и выполнение анализа, приводя к образованию новой области безопасности, задача управления которой ложится на обслуживающий персонал центров NOC и SOC.

УПРАВЛЕНИЕ СООТВЕТСТВИЕМ НОРМАТИВНО-ПРАВОВЫМ АКТАМ, ОТРАСЛЕВЫМ СТАНДАРТАМ И ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ

Организации сталкиваются с ростом количества нормативных требований, большая часть которых направлена на повышение уровня безопасности и обеспечение защиты конфиденциальных данных. Тем не менее, необходимость соблюдения дополнительных требований приводит к появлению новых проблем безопасности. Например, стандарт безопасности данных индустрии платежных карт (PCI DSS) требует от организаций обеспечения безопасной среды обработки и хранения данных кредитных карт. Тем не менее, практика показывает, что «соответствие стандарту PCI» не всегда гарантирует безопасность данных. Существует длинный список предприятий розничной торговли и электронной коммерции, которые при *заявленном* соблюдении стандарта PCI стали жертвами утечки данных.

По сути, соответствие деятельности компании стандарту PCI до определенной степени свидетельствует о внимательном отношении к правилам. Однако следует учитывать, что процесс обеспечения ИТ-безопасности не сводится к доскональному выполнению шаблонных рекомендаций. Проблема заключается в том, что требования к безопасности, такие как PCI, разработаны в рамках традиционного мышления и, как правило, реализуются в изолированной среде.

Принятые в Европейском союзе «Общие положения о защите данных» (GDPR) также значительно усложняют задачу обеспечения безопасности данных. В документе GDPR сформулированы глобальные требования к конфиденциальности данных и жесткие санкции за их несоблюдение. Организации обязаны внедрить средства контроля личных данных на уровне отдельных пользователей. Сложности, возникающие в процессе обеспечения соответствия GDPR, связаны с трудностью отслеживания всех расположений, где могут находиться личные данные пользователей.

Положение усугубляется мандатом GDPR, обязывающим организации обезличивать эти данные и удалять их по запросу соответствующего лица. Крайне важную роль играют функции отслеживания и ведения отчетности по соблюдению этих и других требований.

НЕДОСТАТОЧНАЯ ЭФФЕКТИВНОСТЬ ТРАДИЦИОННЫХ СИСТЕМ БЕЗОПАСНОСТИ

В последнее время задача противодействия угрозам стала как никогда сложной. С одной стороны, растет скорость атак. Например, в последнем квартале 2017 г. среднее количество эксплойтов на фирму составило 274, что на 82% больше, чем в предыдущем квартале.[6] Часто эти атаки проходят по нескольким направлениям одновременно, что затрудняет защиту от них без обмена данными об угрозах в режиме реального времени.

С другой стороны, растут разнообразие и изощренность атак. Злоумышленники используют концепцию «вредоносное ПО как услуга» (MaaS) для получения доступа к изощренным вредоносным программам, которые отличаются быстродействием и простотой. Многие из услуг MaaS поддерживают автоматизированные функции сбора информации и выявления уязвимостей на стороне клиента. Затем технология искусственного интеллекта (ИИ) на стороне сервера выполняет анализ полученной информации и сопоставляет огромные объемы данных в целях определения и проработки векторов атак. Полиморфное вредоносное ПО использует технологию машинного обучения для уклонения от средств управления безопасностью и репликации на скорости машины (ежедневно создаются миллионы копий). Традиционная архитектура безопасности может быть оснащена лучшими в своем классе продуктами, однако если эти продукты размещены в изолированных средах, а инструменты управления и анализа отсутствуют, такая архитектура не сможет эффективно противодействовать современным продвинутым угрозам.

УСУГУБЛЕНИЕ ПРОБЛЕМ БЕЗОПАСНОСТИ, ОБУСЛОВЛЕННОЕ НЕХВАТКОЙ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Процесс управления безопасностью существенно усложнился за последнее десятилетие. Это обусловлено ростом киберпреступности, появлением новых поставщиков услуг безопасности и взрывным увеличением числа оповещений служб безопасности (и требующихся в связи с этим действий). Все это, безусловно, способствует увеличению расходов на обеспечение безопасности, хотя темпы роста бюджетов по-прежнему отстают от темпов усложнения администрирования систем безопасности. (*См. рис. 1, на котором представлен экспоненциальный рост показателей.*[7])

	2007	2017
Злоумышленники	<50	>1000
Поставщики услуг безопасности	<100	>2300
Среднее количество оповещений в день	<1000	>1 000 000
Расходы на обеспечение безопасности	<3 млрд долл. США	>80 млрд долл. США

РИС. 1. ПОВЫШЕНИЕ КОЛИЧЕСТВА УГРОЗ.

Описанные выше изменения не коррелируют с динамикой роста количества специалистов в сфере информационной безопасности. Руководители по безопасности не только сталкиваются с ограничениями в процессе расширения штата отделов безопасности, но и испытывают трудности с поиском, наймом и удержанием квалифицированных профессионалов, владеющих востребованными навыками.

Эта острая нехватка специалистов по информационной безопасности усугубляет проблемы, связанные с ростом количества векторов атак и усложнением угроз. На сегодняшний день зафиксировано более миллиона незанятых должностей в сфере безопасности, и к 2021 г. этот показатель, согласно прогнозам, вырастет до 3,5 миллиона.[8] К тому же развертывание дополнительных специализированных средств защиты в целях противодействия новым угрозам приводит к росту степени фрагментарности корпоративных архитектур безопасности.

Число организаций, заявивших о недостаточном количестве сотрудников по информационной безопасности.[9]	
Мировой уровень	66%
Северная Америка	68%
Латинская Америка	67%
Европа	66%
Ближний Восток и Африка	67%
Азиатско-Тихоокеанский регион	61%

РИС. 2. НЕДОСТАТОК СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГЛОБАЛЬНОМ МАСШТАБЕ.

Нехватка ресурсов информационной безопасности является фактором повышенного риска. По свидетельствам 22% респондентов, в число причин инцидентов безопасности, с которыми они столкнулись в прошлом, входит и недостаточная численность штата отделов безопасности.[10] 70% специалистов по информационной безопасности сообщают, что нехватка квалифицированных кадров отрицательно сказывается на деятельности организаций и приводит к увеличению нагрузки, найму неопытных сотрудников и преобладанию аврального режима работы над обучением.[11]

В связи с растущей нехваткой квалифицированного персонала привлечение специалистов высокого уровня требует повышения окладов и ввода бонусов. По этой причине многие мелкие организации нередко не имеют возможности привлечь специалиста в условиях ограниченности количества профессионалов. Даже крупные компании сталкиваются с проблемой недостаточной квалификации кандидатов, что делает корпоративные сети более уязвимыми для атак.

РАЗРЫВ МЕЖДУ NOC И SOC

Решения NOC и SOC играют важную роль в обеспечении эффективности работы и упреждающем управлении рисками безопасности. NOC способствует повышению эффективности за счет координации и автоматизации таких процессов, как управление ресурсами, версиями, пользователями и полномочиями, подключениями и доступом. Также это решение реализует функции аудита и обеспечения соответствия требованиям. SOC действует в рамках упреждающей концепции безопасности и отвечает за поддержку таких функций, как выявление и предотвращение атак, администрирование и реагирование на инциденты и события, управление рисками и смягчение их последствий.

Цели каждого из решений также отличаются. NOC выполняет функцию измерения показателей, связанных с пропускной способностью и доступностью. SOC служит для регистрации показателей выявления и блокировки угроз (см. рис. 3).

Решения NOC и SOC совместно используются во многих организациях. Однако они выполняют разные функции и фиксируют разные показатели. Таким образом, эти решения передают данные о состоянии сети и угрозах независимо друг от друга. Устранение угроз и сетевых проблем требует взаимодействия решений NOC и SOC, так как событие безопасности может стать причиной сбоя сети, а уязвимость в системе безопасности может быть связана с сетевым событием. Однако технологии NOC и SOC не всегда поддерживают согласованное решение проблем. Кроме того, изолированность систем мониторинга, оповещения и отправки запросов затрудняет взаимодействие центров NOC и SOC в процессе совместного принятия мер противодействия и повторной категоризации уже прошедших анализ событий. Например, если операторы NOC обнаруживают проблему и впоследствии приходят к выводу, что это результат нарушения безопасности, они могут столкнуться с отсутствием эффективного способа передачи собранной информации коллегам в отделе SOC.

Кроме того, ранее упомянутая в статье проблема нехватки специалистов по информационной безопасности оказывает существенное влияние на центры NOC и SOC. Отсутствие у сотрудников надлежащей квалификации препятствует взаимодействию решений с разными функциями и повышает потенциальные риски.

Операционные технологии… Повышение эффективности	**Технологии безопасности… Более оперативное выявление угроз**
Повышение эффективности согласования и автоматизации операций. Сюда входят следующие направления.	**Выявление атак и нарушений с последующим принятием мер противодействия. Сюда входят следующие направления.**
■ Ресурсы и управление версиями	■ Атаки и уязвимости
■ Пользователи и полномочия	■ Зараженные пользователи и серверы
■ Подключения и доступ	■ Реагирование на инциденты и устранение последствий
■ Аудит и обеспечение соответствия требованиям	■ Управление рисками и смягчение их последствий

РИС. 3. ТРАДИЦИОННО СУЩЕСТВУЮЩЕЕ РАЗДЕЛЕНИЕ МЕЖДУ NOC И SOC.

ЗАКЛЮЧЕНИЕ

Успешное противодействие современным угрозам требует внедрения превентивной стратегии безопасности. Операционные центры NOC и SOC эффективны в рамках предписанных им функций, однако в силу изолированности им недостает таких характеристик, как гибкость и масштабируемость. Только эти свойства при поддержке актуальных данных об угрозах могут обеспечить защиту от современных продвинутых угроз. В связи с такими тенденциями, как появление новых векторов атак, усложнение процесса управления соответствием требованиям и возникновение продвинутых угроз, потребность в комплексном подходе становится все более настоятельной. В силу ограниченности бюджетных средств, выделяемых на обеспечение безопасности и управление сетевыми ресурсами, а также нехватки специалистов по информационной безопасности попытки руководителей устранить описанные недостатки путем найма новых сотрудников могут оказаться бесплодными.

Вместо этого необходимо ликвидировать разрыв между центрами NOC и SOC. Устранить границы можно за счет подбора и интеграции соответствующих средств управления безопасностью и инструментов анализа, поддерживающих комплексное отслеживание и автоматизацию процессов корреляции данных.

[1] Стив Морган (Steve Morgan), «2018 Cybersecurity Market Report», Cybersecurity Ventures, 31 мая 2017 г.

[2] Стив Морган (Steve Morgan), «Cybercrime Damages $6 Trillion By 2021», Cybersecurity Ventures, 16 октября 2017 г.

[3] Саймон Кемп (Simon Kemp), «The global state of the internet in 2017», TNW, 11 апреля 2017 г.

[4] Люсьен Константин (Lucian Constantin), «Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON», CSO, 13 сентября 2016 г.

[5] «Threat Landscape Report: Q4 2017», Fortinet, февраль 2018 г.

[6] «Fortinet Threat Landscape Report Reveals Attacks Per Firm Increased by 82%», Fortinet, 20 февраля 2018 г.

[7] Дэйв ДеУолт (Dave DeWalt) и Дэвид Петреус (David Petraeus), «The Cyber Security Mega Cycle Aftermath», Optiv, 7 сентября 2017 г.

[8] Джим Кеннеди (Jim Kennedy), «Cybersecurity skills shortage», CSO, 1 марта 2018 г.

[9] «2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk», Frost & Sullivan, июнь 2017 г.

[10] Джон Олтсик (Jon Oltsik), «Cybersecurity skills shortage creating recruitment chaos», CSO, 28 ноября 2017 г.

[11] Джон Олтсик (Jon Oltsik), «Research suggests cybersecurity skills shortage is getting worse», CSO, 11 января 2018 г.

Fortinet
Смоленская площадь 3,
Регус, офис 610,
121099 Москва
Тел.: +7 (499) 955-24-99

ГЛАВНЫЙ ОФИС
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
США
Тел.: +1.408.235 7700
www.fortinet.com/sales

ОТДЕЛ ПРОДАЖ В ЕБВА
905 rue Albert Einstein
06560 Valbonne
Франция
Тел.: +33 4 8987 0500

ОТДЕЛ ПРОДАЖ В АТР
300 Beach Road 20-01
The Concourse
Сингапур 199555
Тел.: +65 6513 3730

ЛАТИНСКАЯ АМЕРИКА
ГЛАВНЫЙ ОФИС
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Тел.: +1 954 368 9990

© Fortinet, Inc., 2018. Все права защищены. Fortinet®, FortiGate®, FortiCare®, FortiGuard® и другие знаки являются зарегистрированными товарными знаками компании Fortinet, Inc.; иные названия Fortinet, упомянутые в данном документе, также могут быть зарегистрированными и/или охраняемыми нормами общего права товарными знаками компании Fortinet. Все иные названия продуктов и компаний являются товарными знаками соответствующих владельцев. Показатели производительности и иные показатели, приведенные в данном документе, были получены в ходе внутренних лабораторных испытаний при идеальных условиях; фактические показатели производительности и другие результаты могут отличаться. На показатели производительности могут оказать влияние сетевые переменные, различия сетевых сред и иные обстоятельства. Данный документ не следует рассматривать как твердое обязательство компании Fortinet; компания Fortinet отказывается от обязательств по всем гарантиям, как явным, так и подразумеваемым, за исключением обязательств по соглашениям с покупателями, заключенным в письменной форме за подписью главного юрисконсульта Fortinet, и в явной форме гарантирующим получение в ходе использования указанного продукта результатов, соответствующих зафиксированным в соглашении показателям производительности — в данном случае компания Fortinet берет на себя исключительно обязательства по обеспечению указанных в письменном соглашении результатов. Для полной ясности любая гарантия относится к применению продукта в идеальных условиях, аналогичных условиям проведения внутренних лабораторных испытаний Fortinet. Компания Fortinet полностью отказывается от каких-либо договоренностей, представлений и гарантий, связанных с данным документом, как явных, так и подразумеваемых. Компания Fortinet сохраняет за собой право изменять, перемещать или иными способами исправлять данную публикацию без уведомления; актуальной является последняя версия публикации.

208268-A-1-RU