FORTINET

Стратегии снижения сложности и упрощения операций безопасности

Содержание

FORTINET

Аннотация

Два показателя в сфере кибербезопасности, которые в последние годы растут быстрее всех остальных, — это разнообразие угроз и количество разрозненных средств безопасности, разработанных для противодействия им. Проблемой для разработчиков архитектур безопасности становится растущая сложность, которая затрудняет операции безопасности. Однако есть три стратегии, позволяющие существенно сократить эту сложность: 1) централизация и приоритизация угроз, 2) упрощение аудита и контроля соответствия требованиям и 3) автоматизация для более быстрого реагирования. Эти ключевые стратегии существенно улучшают операции безопасности и защитную инфраструктуру организации.

До 40% новых вредоносных программ, обнаруживаемых в отдельно взятый день, представляют собой угрозу «нулевого дня» или относятся к ранее неизвестным.[1]

Среднее предприятие использует одновременно 75 разных инструментов обеспечения безопасности.[2]

На сегодняшний день количество незакрытых вакансий в области безопасности во всем мире составляет почти 3 миллиона.[3]

Введение: слишком много полезных данных о безопасности

Для профессионала в сфере безопасности статистика выглядит обескураживающе: количество и сложность киберугроз растут, и организациям уже не хватает специалистов, чтобы с ними справляться.

Проблема состоит не в том, что у служб кибербезопасности нет инструментов для защиты или ценных данных для эффективного применения этих инструментов. Данных просто слишком много. Слишком много файлов журналов, которые нужно сопоставлять, консолей, в которых нужно управлять, оповещений, которые нужно оценивать. Неудивительно, что 79% отделов безопасности считают, что перегружены потоком оповещений.[4]

Все это означает, что разработчикам архитектур безопасности следует рассмотреть ряд стратегий по снижению сложности и упрощению операций безопасности.

01 Централизованное отслеживание и приоритизация угроз

Мониторинг безопасности должен быть централизован. Отделам безопасности требуется подход, который обеспечит отображение всех данных в едином окне на предоставленном портале или возможность интегрировать защитные решения с одним из популярных инструментов отслеживания.

Решение должно обеспечивать обзор аномалий во всей цифровой организации, включая локальные и облачные компоненты, Интернет вещей (IoT) и системы эксплуатационных технологий (OT). Инструменты обеспечения безопасности на основе аналитических функций и управления журналами сопоставляют данные от различных устройств и защищают от избыточного количества оповещений, выполняя критическое исследование угроз. Оно точно определяет случаи, требующие немедленного реагирования, и позволяет оперативно принять ответные меры.

Решение должно также предусматривать автоматическое развертывание конфигураций безопасности во всей организации, минимизируя риск ошибок, связанных с человеческим фактором, и неправильной настройки конфигурации. Оно должно детализировано представлять индикаторы компрометации (IOC) специалистам по безопасности и эксплуатационным группам, используя машинное обучение (ML) для определения стандартного поведения, выявления аномалий и идентификации индикаторов компрометации. Также оно должно поддерживать получение новых данных об индикаторах компрометации, полученных посредством автоматизированного или человеческого анализа других сред во всем мире и предоставляемых службой информирования об угрозах.

Наличие единого канала аналитики угроз важно и действительно повышает уровень безопасности. Например, в двух недавних случаях глобальных взломов специалисты по безопасности просмотрели предупреждения в результате усталости из-за избыточного количества оповещений.[5]

02 Упрощение аудита и контроля соответствия требованиям

Когда компании слишком медлят с внедрением критически важных мер безопасности для защиты своих данных, на сцену выходят органы власти государственного, регионального и местного уровня. Во всем мире принимается все больше регламентов по кибербезопасности, и они становятся все более строгими.[6] Наиболее значительным из таких документов на сегодня является «Общий регламент по защите данных» (GDPR) Европейского союза, предусматривающий строгие наказания и штрафы.[7] А с учетом скорого вступления в силу Закона Калифорнии о защите конфиденциальности потребителей (CCPA) аспекты конфиденциальности данных становятся для разработчиков архитектур безопасности еще более актуальными.[8]

Специалистам по безопасности требуется аналитическое решение, которое предоставит инструменты для организации операций в соответствии с лучшими отраслевыми методиками, основанными на стандартах безопасности таких организаций, как Национальный институт стандартов и технологий (NIST) и Центр интернет-безопасности (CIS). Решение должно также создавать отчеты, которые будут подтверждать соблюдение регламентов, например стандарта безопасности данных индустрии платежных карт (PCI DSS).

В дополнение к этому руководителям отделов безопасности рекомендуется проанализировать свою ситуацию, ответив на три важных вопроса, касающихся надзора за использованием данных:

1. Правильно ли настроена сеть? Есть ли возможность выявлять проблемы конфигурации до того, как они приведут к инциденту?
2. Каково общее состояние безопасности? Ответом на этот вопрос должно быть единое измерение. Это показатель, демонстрирующий влияние решений по обеспечению безопасности за определенный период, который можно использовать в отчетах об общих тенденциях для высшего руководства и совета директоров.
3. Что доказывает соответствие требованиям? Одно решение может заменить сотни часов ручного анализа, если оно способно анализировать изменения топологии сети и составлять соответствующие отчеты. Оно должно облегчать выявление и устранение устройств с высоким уровнем риска или не соответствующих требованиям и предоставлять планы действий и отчеты о ходе выполнения как для технических специалистов, так и для руководства.

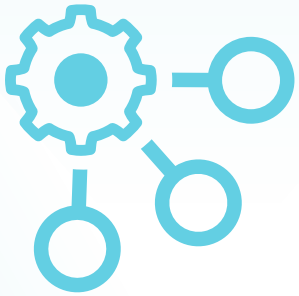
Ответы на эти вопросы могут быть сформулированы в форме объективной оценки риска, которая должна включать сравнение с принятыми эталонами и аналогичными организациями, а также практические рекомендации по улучшению управления рисками.[9] Соответствующая оценка безопасности в баллах позволяет разработчикам архитектур безопасности определять и приоритизировать необходимые компоненты системы безопасности, а специалистам отделов безопасности — распределять ресурсы с учетом выявленных уязвимостей и устойчивости к рискам. Более того, специалисты по безопасности могут использовать удобное отслеживание проблем безопасности и мер по снижению рисков, чтобы управлять рисками профилактически.[10]

«Технологические метрики рисков контролируют достижение целей путем количественной оценки внедрения и эффективности мер безопасности, анализа адекватности действий в рамках программы информационной безопасности и определения возможных мер по улучшению».[11]

03 Автоматизация для более быстрого реагирования

Специалисты центра операций сети (NOC) и центра операций безопасности (SOC) преследуют общую цель — обеспечение доступности и защиты служб — однако рассматривают задачу с разных точек зрения и используют разные инструменты. Чтобы помочь им эффективно сотрудничать друг с другом, разработчики архитектур безопасности должны рассмотреть подход к обеспечению безопасности и управлению журналами на основе анализа, который обеспечит консолидированное представление операций и безопасности. Это позволит специалистам центров NOC и SOC найти общий язык и рассматривать интегрированные данные NOC и SOC в их взаимосвязи. Анализ выявляемых угроз дает возможность определить для них высокий, средний или низкий уровень риска. Более того, чтобы ускорить расследование угрозы, события на временной шкале инцидента должны сопровождаться контекстом.

Такое решение должно также поддерживать интеграцию с технологиями управления информационной безопасностью и событиями (SIEM) и решениями по управлению IT-службами (ITSM), автоматизируя утверждение рабочих процессов между отделами безопасности и обслуживания сети при реагировании на события, а также предлагать рекомендации по политикам и настройкам. Инциденты безопасности автоматически передаются в решение ITSM, причем аналитики могут выбирать из каталога ответов подходящие варианты, которые можно внедрить автоматически из центрального расположения. Такие возможности сокращают время реагирования на инциденты с нескольких дней до нескольких минут и позволяют обойтись меньшим числом специалистов, задачей которых становится принятие решений на экспертном уровне, а не мониторинг и перенаправление информации.[12]



Автоматизация процессов обеспечения безопасности не только снижает риски организации, сокращая время реагирования с нескольких дней или недель до нескольких минут, но и помогает повысить эксплуатационную эффективность.[13]

Заключение: киберугрозы определяют нашу эпоху

Компания может иметь оборудование на миллиарды долларов, размещенное на нескольких объектах в разных точках мира и хорошо охраняемое физически. Но в наступившую цифровую эпоху операции глобального масштаба могут быть полностью остановлены за несколько минут в результате тихой кибератаки, которая поставит под угрозу безопасность сотрудников, прибыли и клиентские операции, а также подорвет репутацию компании и доверие клиентов, завоеванное, возможно, в течение нескольких десятилетий. Например, вредоносное ПО NotPetya на несколько дней остановило деятельность тысяч бизнесов во всем мире, включая одну транспортную компанию с глобальным охватом и одну фармацевтическую компанию, также глобального уровня. Потери во всем мире были оценены в 10 миллиардов долларов.[14]

В свете такой картины продвинутых угроз разработчики архитектур безопасности должны рассматривать архитектурные изменения, касающиеся реагирования на инциденты и управления событиями. Риск подвергнуться взлому в ближайшие 24 месяца для организаций составляет сейчас примерно один к трем.[15] Однако событие взлома не обязательно должно приводить к ущербу. Как отметил один андеррайтер компании, страхующей от специализированных рисков: «Сам по себе взлом — еще не катастрофа. Катастрофа — неверная реакция на него».[16]

Именно на этот аспект и может существенно повлиять разработчик архитектуры безопасности, сведя к минимуму время, необходимое для обнаружения взлома и устранения последствий. Функции обеспечения безопасности и управления журналами на основе анализа — ключевой элемент в достижении этой цели. Они позволяют приоритизировать риски, ускорить расследование инцидентов и быстрее получать ответы в случае взлома. В частности, важно обеспечить возможность унифицировать и сопоставлять данные от различных решений по обеспечению безопасности и автоматизировать рабочие процессы устранения последствий.

За один год в 65 странах:[17]

2 216
сообщений об утечке данных

53 000
сообщений об инцидентах кибербезопасности

Средние затраты в случае взлома составляют 3,86 миллиона долл. США, однако организации, в которых системы безопасности полностью автоматизированы, могут сократить эти затраты на 1,55 миллиона долл. США.[18]

[1] По внутренним данным FortiGuard Labs.

[2] Кейси Цуркус (Kacy Zurkus), «Defense in depth: Stop spending, start consolidating», CSO, 14 марта 2016 г.

[3] «Cybersecurity Skills Shortage Soars, Nearing 3 Million», (ISC)², 18 октября 2018 г.

[4] Грег Мастерс (Greg Masters), «Crying wolf: Combatting cybersecurity alert fatigue», SC Magazine, 9 июня 2017 г.

[5] Там же.

[6] Джадзия Пирс (Jadzia Pierce), «Privacy and Cybersecurity: A Global Year-End Review», Inside Privacy, 21 декабря 2018 г.

[7] Джульетт Ризкалла (Juliette Rizkallah), «The Cybersecurity Regulatory Crackdown», Forbes, 25 августа 2017 г.

[8] Мэри К. Пратт (Mary K. Pratt), «State data privacy laws, regulations changing CISO priorities», TechTarget, апрель 2019 г.

[9] Исследование «Proactive, Actionable Risk Management with the Fortinet Security Rating Service», Fortinet, 5 апреля 2019 г.

[10] Исследование «Bridging the NOC-SOC Divide: Understanding the Key Architectural Requirements for Integration», Fortinet, 23 августа 2018 г.

[11] Мукул Парик (Mukul Pareek), «Standardized Scoring for Security and Risk Metrics», ISACA Journal, 2017 г.

[12] Исследование «Purpose-built Integrated NOC-SOC Management and Analytics», 11 сентября 2018 г.

[13] Марина Мартин (Marina Martin), «How Inefficiency Negatively Impacts Your Business», Dummies.com, по состоянию на 21 июня 2019 г.

[14] Энди Гринберг (Andy Greenberg), «The Untold Story of NotPetya, the Most Devastating Cyberattack in History», WIRED, 22 августа 2018 г.

[15] Исследование «2018 Cost of a Data Breach Study», Ponemon Institute, по состоянию на 18 октября 2018 г.

[16] Статья «Phrases to help us think about cyberattacks…», The Cyber Rescue Alliance, по состоянию на 25 апреля 2019 г.

[17] Джил Пресс (Gil Press), «60 Cybersecurity Predictions For 2019», Forbes, 3 декабря 2018 г.

[18] Исследование «2018 Cost of a Data Breach Study», Ponemon Institute, по состоянию на 18 октября 2018 г.

www.fortinet.com/ru

402438–0–0–RU

ноября 22, 2020 1:06 ПП

eb-cybersecurity-architect-fortianalyzer_RU