ИСПОЛЬЗОВАНИЕ FORTINAC ДЛЯ КОНТРОЛЯ УСТРОЙСТВ IOT В КОРПОРАТИВНОЙ СЕТИ

О.А. Кондрашук, Е.В. Константинова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Число типов и моделей устройств IoT (Internet of Things) стремительно расширяется с развитием рынка «интернета вещей». Если ранее необходимо было контролировать подключения компьютеров и мобильных устройств, то на сегодняшний день ассортимент оборудования, которое необходимо обнаружить и идентифицировать, существенно расширился. Неконтролируемое подключение устройств IoT в сети организации, увеличивают вероятность возникновения инцидентов безопасности. Поэтому необходимо вести учет и контроль каждого устройства в корпоративной сети.

Поскольку модернизация технологий затрагивает практически все отрасли человеческой деятельности, различные предприятия и организации, которые ранее не уделяли большого внимания информационной безопасности, сейчас вынуждены решать проблемы, возникающие в этой сфере. С этой целью была разработана система контроля доступа к сети FortiNAC (Network Access Control). Данная система обеспечивает обнаружение и профилирование всех устройств, подключающихся к корпоративной инфраструктуре, конфигурацию политик безопасности, а также реагирование на различные события и инциденты безопасности.

NAC-система компании Fortinet имеет трехуровневую архитектуру безопасности. На первом уровне происходит идентификация и профилирование всех подключившихся к сети устройств, в том числе IoT-устройств, идентификация установленного на них программного обеспечения. Информация, полученная на данном этапе используется для присвоения подключенному устройству прав доступа в соответствии с политикой безопасности, которая разработана для разных типов устройств с учетом таких параметров, как местонахождение, тип подключения, тип установленного программного обеспечения. Последний уровень архитектуры безопасности FortiNAC предусматривает использование средств, обеспечивающих реагирование на потенциально опасные изменения состояния подключенных устройств. В случае несоответствия параметров устройства установленным правилам, система контроля доступа к сети определяет возможные угрозы и автоматически снижает уровень доступа вплоть до полной блокировки. Такие же действия предпринимаются в случае использования VPN-соединения для доступа в сеть.

Таким образом решение FortiNAC минимизирует риски возникновения угроз безопасности в корпоративных сетях, связанные с незащищенными устройствами, которые осуществляют доступ к сети, обеспечивая полную видимость различных пользователей, устройств и приложений. Кроме того, система контроля доступа к сети FortiNAC является легко масштабируемой, позволяет расширять защиту большого количества устройств и устраняет необходимость ее развертывания на каждом объекте крупных предприятий.

Список литературы

1. Система контроля доступа к сети FortiNAC [Электронный ресурс]. – Режим доступа: https://www.anti-malware.ru/reviews/FortiNAC#part2. – Дата доступа: 27.04.2023.

2. FortiNAC: управление доступом к сети [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/Продукт:FortiNAC. – Дата доступа: 27.04.2023.