Пробел в кибербезопасности медицинских устройств, скрывающийся на виду

Источник: MedTech Intelligence

Оригинал: https://medtechintelligence.com/feature_article/the-medical-device-cybersecurity-gap-hiding-in-plain-sight/

инфраструктура здравоохранения | кибербезопасность | медицинские устройства | управление рисками

Слепое пятно в клинической сети

Здравоохранение годами укрепляло защиту электронной почты, идентификационных данных и конечных точек, в то время как огромная поверхность атаки остается у постели больного, в диагностических средах и в кабинетах визуализации. Подключенные медицинские устройства теперь делают больше, чем просто обеспечивают терапию или собирают данные; они также работают на распространенных операционных системах, полагаются на удаленное обслуживание, обмениваются защищенной медицинской информацией (PHI) и все чаще участвуют в рабочих процессах, которые нельзя просто приостановить при возникновении подозрений. Эта реальность делает риск, связанный с медицинскими устройствами, отличным от обычного ИТ-риска. Если выходит из строя рабочая станция, падает производительность. Если выходит из строя или подвергается манипуляциям критически важное клиническое устройство, оказание помощи может быть задержано, ухудшено или стать небезопасным. Тем не менее, многие организации до сих пор оценивают киберриски устройств с помощью инструментов, созданных в первую очередь для общего ИТ, а не для клинических сред.

Идея, лежащая в основе этой статьи, указывает на более практичный путь. Вместо того чтобы начинать только с абстрактных фреймворков, она начинается с того, что многие больницы уже просят поставщиков предоставить во время закупок и внедрения: **Manufacturer Disclosure Statement for Medical Device Security** (MDS2 — Заявление производителя о раскрытии информации по безопасности медицинских устройств). Простыми словами, MDS2 — это структурированная форма раскрытия информации о безопасности. Она сообщает покупателям, поддерживает ли устройство такие функции, как установка исправлений (патчинг), ведение журналов (логирование), шифрование, аутентификация, усиление защиты (hardening) и средства контроля удаленного доступа. Сама по себе эта информация полезна, но неполна. Анализ в данной статье заключается в том, чтобы дополнить её данными об угрозах **MITRE ATT&CK** и оценкой по шкале **CVSS 4.0**, включая метрику безопасности. Результатом является метод, предназначенный не просто для описания состояния устройства, а для ранжирования того, где действия организаций, предоставляющих медицинские услуги, наиболее срочны.

Рисунок 1.

Почему текущие подходы часто не достигают цели?

Это важно, потому что текущее состояние оценки рисков устройств все еще остается хаотичным. Некоторые подходы в значительной степени полагаются на опубликованные **CVE** (Common Vulnerabilities and Exposures — общеизвестные уязвимости). Другие опираются на экспертные панели, пользовательские рубрики или длинные опросники. Третьи больше фокусируются на корпоративной инфраструктуре вокруг устройства, чем на самом устройстве. Эти методы могут быть полезными, но они часто медленны, дороги, непоследовательны или их трудно поддерживать в актуальном состоянии. Они также склонны рассматривать безопасность пациентов как нечто, добавляемое позже. Для профессионалов отрасли, балансирующих между сроками закупок, бэклогом уязвимостей и циклами замены капитальных средств, это является плохим решением. Руководителям нужен метод, который будет понятным, повторяемым и достаточно динамичным, чтобы развиваться вместе с ландшафтом угроз.

Операционную сложность легко недооценить. Крупные системы здравоохранения могут управлять тысячами подключенных устройств в отделениях интенсивной терапии, амбулаторного лечения, лабораториях, отделениях визуализации и средах домашнего мониторинга. Многие из них

являются долговечными активами. Некоторые имеют слабую техническую оснащенность с точки зрения безопасности. Некоторые используются совместно различными отделениями, которые используют разные рабочие процессы и пути эскалации. В таком контексте метод оценки рисков, зависящий от созыва экспертных комиссий для каждого актива или от длительных пользовательских опросников, будет иметь трудности с масштабированием. Индустрии нужны не просто лучшие баллы; ей нужен процесс, соответствующий темпу и сложности современных клинических операций.

Исследование оценило подход на примере шести различных медицинских устройств от разных производителей: дефибриллятор/монитор/кардиостимулятор, автоматизированный шкаф для выдачи лекарств, монитор показателей жизнедеятельности, электрокардиографическая система, госпитальный глюкометр и мобильное рентгеновское устройство. Вместе они представляли системы на базе **Windows** и **Linux**, а также различные клинические роли. Методология переводила ответы MDS2 в потенциальные уязвимости, сопоставляла эти уязвимости с методами **ATT&CK**, актуальными для здравоохранения, сравнивала результаты со моделью **STRIDE** и затем оценивала серьезность с помощью **CVSS 4.0**. Также использовались данные **CISA** (Cybersecurity and Infrastructure Security Agency — Агентство по кибербезопасности и защите инфраструктуры) о частоте угроз для расчета технических баллов риска. Целью было не создание идеального универсального балла, а создание более быстрого, ориентированного на здравоохранение способа приоритизации действий.

Упускаемый из виду актив, скрывающийся на виду.

Одним из самых четких выводов является то, что MDS2 заслуживает гораздо большего внимания, чем обычно получает. Во многих организациях к MDS2 относятся как к форме для закупок: собрать, подшить в папку и забыть. Исследование утверждает обратное: она может служить основой для живого процесса оценки рисков. Это значимо, потому что MDS2 уже знакома производителям и все чаще ожидается системами здравоохранения. Крупные организации, такие как **VA** (Department of Veterans Affairs — Министерство по делам ветеранов США), **Mayo Clinic**, **Johns Hopkins** и **University of California**, использовали MDS2 в процессах проверки или внедрения устройств. Другими словами, индустрии не нужны совершенно новые стандарты данных, чтобы начать. Она может извлечь больше пользы из стандарта, который уже признает.

Этот момент имеет стратегическое значение для руководителей по закупкам. Лучшее время, чтобы обнаружить, что устройству не хватает надежной аутентификации, возможности установки исправлений, ведения журналов или ограничений удаленного доступа, — это до того, как заказ будет окончательно оформлен, а не после того, как оборудование будет развернуто в отделении интенсивной терапии. MDS2 дает организациям поставщикам возможность задавать более информированные вопросы на более ранних этапах жизненного цикла. При правильном использовании она может улучшить формулировки контрактов, решения по сегментации, обработку исключений и планирование обновления парка оборудования. При неправильном использовании она становится еще одним PDF-файлом, который никто больше не открывает. Настоящий вызов исследования заключается не в том, что больницам нужно больше форм, а в том, что им нужно внедрить в операционную деятельность ту форму, которая у них уже есть.

Исследование также показало, что анализ на основе MDS2 выявил больше проблем, чем только поиск по **CVE**. Только два из шести устройств имели опубликованные **CVE** в период исследования, однако метод, основанный на MDS2, выявил дополнительные потенциальные уязвимости во всем наборе устройств. Это важный операционный момент. **CVE** необходимы, но они не дают полной картины подверженности угрозам. Устройство может не иметь публичного **CVE**, но при этом представлять реальную угрозу безопасности из-за слабой аутентификации, ограниченного логирования, недостаточного усиления защиты, неполных возможностей резервного копирования или зависимостей от удаленного обслуживания. Для **CISO** (Chief Information Security Officer — директор по информационной безопасности), руководителей отделов **HTM** (Healthcare Technology Management — управление медицинскими технологиями) и архитекторов безопасности это является убедительным аргументом в пользу использования данных о раскрытии информации и характеристик проектирования, а не только публичных фидов уязвимостей, для руководства приоритизацией.

Почему ATT&CK добавляет необходимый реализм.

Сравнение с **ATT&CK** не менее показательно. В совокупности метод на основе **ATT&CK** сопоставил 71% выявленных уязвимостей устройств с соответствующими угрозами, по сравнению с 60% при использовании **STRIDE**. Этот разрыв не огромен, но он значим. **STRIDE** остается полезным как классическая линза моделирования угроз, особенно в дискуссиях по проектированию, но по своей природе он слишком широк. **ATT&CK** дал

исследованию более приземленный взгляд на то, как реальные злоумышленники атакуют здравоохранение. Не менее важно то, что **ATT&CK** регулярно обновляется. Это дает программам безопасности встроенный способ обновления оценок по мере изменения активности угроз. Для отрасли, сталкивающейся с постоянным давлением программ-вымогателей, злоупотреблением учетными данными, фишинговыми кампаниями и проблемами цепочки поставок, «живая» модель угроз более ценна, чем статичная.

Эта разница также важна для доверия со стороны высшего руководства. Аргумент о риске, построенный на абстрактных категориях, часто звучит теоретически. Аргумент о риске, привязанный к методам, используемым злоумышленниками, нацеленными на здравоохранение, звучит операционно. Советы директоров, аудиторские комитеты и исполнительные команды все чаще хотят знать не только то, существует ли пробел в контроле, но и то, соответствует ли он реалистичному поведению атакующих. **ATT&CK** помогает ответить на этот вопрос. Он сужает разговор от «что могло бы произойти в теории» до «что атакующие делают на самом деле». Этот сдвиг облегчает защиту приоритизации в условиях ограниченных бюджетов и персонала.

Результаты оценки баллов риска подтверждают этот тезис. Среди шести проверенных устройств дефибриллятор/монитор/кардиостимулятор показал самый низкий совокупный технический балл риска — 4,78, в то время как госпитальный глюкометр показал самый высокий — 9,48. Самым важным драйвером для всех устройств было не экзотическое поведение «нулевого дня» (zero-day), а первоначальный доступ, особенно через валидные учетные записи. Это должно быть знакомо каждому защитнику здравоохранения. Злоупотребление учетными данными остается одним из самых надежных способов проникновения в сеть и, как следствие, в экосистемы устройств, которые зависят от идентификации, удаленного доступа и использования учетных записей по умолчанию или общих учетных записей. Для читателей отрасли вывод практический: кибербезопасность устройств — это не только вопрос биомедицинской инженерии. Это также вопрос идентификации, доступа и операционной дисциплины.

Рисунок 2.

Множитель безопасности пациентов

Однако, пожалуй, самым важным бизнес-инсайтом стало то, что произошло, когда безопасность пациентов рассматривалась как часть логики оценки, а не как отдельная тема для обсуждения. Используя необязательную метрику безопасности в **CVSS 4.0**, исследование показало, что несколько уязвимостей стали более срочными, когда учитывалось потенциальное воздействие на пациента. Из шести устройств 29 из 95 общих уязвимостей были помечены как имеющие последствия для безопасности пациентов. У госпитального глюкометра была самая высокая доля: 9 из 17 уязвимостей имели флаг безопасности. За ним следовал дефибриллятор/монитор/кардиостимулятор — 5 из 12. Такой уровень видимости меняет дискуссию в залах заседаний и комитетах по закупкам. Проблема безопасности больше не является просто пробелом в контроле; она может стать риском для оказания медицинской помощи.

Такое переосмысление важно, потому что организации здравоохранения часто с трудом согласовывают приоритеты кибербезопасности и клинической инженерии. Традиционная ИТ-оценка может упустить то, что клиницисты понимают интуитивно: не каждый сбой актива одинаков. Компрометация административной системы с низким уровнем критичности серьезна, но компрометация устройства, участвующего в управлении лекарствами, мониторинге или экстренном реагировании, несет в себе иной операционный и этический вес. Включая безопасность в оценку серьезности, исследование дает руководителям более обоснованный способ распределения дефицитных ресурсов. Это помогает ответить на вопрос, который возникает в каждой зрелой программе: что нам следует исправить в первую очередь, когда кажется, что срочно всё?

Это также меняет язык инвестиций. Когда команды безопасности говорят только о вредоносном ПО, патчах и возможности эксплуатации, им может быть трудно конкурировать с другими операционными приоритетами. Когда они могут связать уязвимость с прерыванием терапии, небезопасным мониторингом или сценариями причинения вреда пациенту, разговор становится проще для понимания нетехническими руководителями. Это не означает, что каждая уязвимость становится кризисом. Это означает, что организация получает более четкий способ отличить рутинную кибергигиену от клинически значимого риска. В секторе, где маржа ограничена, а время простоя дорого стоит, такая ясность имеет значительную бизнес-ценность.

Сводка устройств на основе источников.

Рисунок 3.

Что профессионалам отрасли делать дальше?

Результаты исследования можно переложить в практический план действий на ближайшее время.

- **Во-первых**, относитесь к MDS2 как к операционным данным, а не как к бумажной работе. Внедряйте его в процессы закупок, внедрения, сегментации, управления уязвимостями и периодических проверок.
- **Во-вторых**, обновляйте модели рисков устройств с использованием актуальных данных **ATT&CK**, а не полагайтесь только на статические списки угроз.
- **В-третьих**, сделайте **CVSS 4.0** с метрикой безопасности частью обсуждения для соответствующих устройств, особенно тех, которые используются в условиях высокой интенсивности лечения или напрямую связаны с терапией и мониторингом.
- **В-четвертых**, тщательно проверяйте аутентификацию, управление учетными записями, удаленное обслуживание и пути установки исправлений. Исследование неоднократно возвращает нас к этим основам, потому что злоумышленники делают то же самое.
- **Наконец**, сделайте заинтересованных лиц из областей **HTM**, безопасности, инфраструктуры и клиники совладельцами процесса. Киберриск медицинских устройств живет на стыке команд.

Для многих организаций правильным первым шагом будет не амбициозная программа «прыжка к луне», а дисциплинированный 12-месячный операционный план. Начните со стандартизации того, как документы MDS2 собираются, проверяются и хранятся. Установите минимальный набор контрольных точек для каждого нового устройства: модель идентификации, возможность ведения журналов, путь установки исправлений, средства контроля удаленного доступа, требования к сегментации и документированные исключения. Затем определите ограниченный набор классов устройств, где оценка с учетом безопасности будет использоваться последовательно, например, системы, связанные с лекарствами, мониторингом и жизнеобеспечением. Незначительные изменения в процессах могут принести огромную пользу, если они повысят последовательность и уменьшат количество ситуативных решений.

Производители также должны играть свою роль. Исследование отмечает, что предоставление MDS2 остается добровольным, что является ограничением. Тем не менее, давление рынка меняет ситуацию. Поставщики, предоставляющие актуальные и полные данные, облегчают жизнь организациям-поставщикам услуг и укрепляют свои конкурентные позиции. На практике это означает своевременные обновления после существенных изменений в устройстве, более четкую документацию по усилению защиты и сторонним компонентам, а также прозрачные ответы о патчинге, удаленном доступе и аутентификации. По мере того как системы здравоохранения формализуют проверку безопасности устройств, качественное раскрытие информации будет все чаще становиться частью ведения бизнеса, а не просто приятным бонусом. Ничего из этого не означает, что методология идеальна, но профессионалам отрасли не нужно совершенство, чтобы извлечь пользу из этого урока. Им нужен процесс, который лучше, чем сегодняшняя мозаика из форм, электронных таблиц и разовых суждений. По этому критерию данная работа выглядит убедительно.

Лучшая операционная модель для подключенного ухода

Более широкий посыл заключается в том, что здравоохранение больше не может позволить себе отделять киберустойчивость от безопасности пациентов или управление устройствами от корпоративной безопасности. Подключенные устройства являются частью клинической миссии. Это означает, что оценка рисков должна быть достаточно быстрой для операций, достаточно специфичной для закупок и достаточно достоверной для руководства. Соединяя раскрытие информации поставщиками, поведение реальных противников и оценку с учетом безопасности, это исследование направляет дискуссию в этом направлении. Как для больниц, так и для производителей, следующий этап кибербезопасности медицинских устройств будет выигран не за счет увеличения объема бумажной работы, а за счет превращения правильных данных в действия.

Избранные ссылки

- Manufacturer Disclosure Statement for Medical Device Security. (2019). National Electrical Manufacturers Association (NEMA).
- MITRE ATT&CK. MITRE Corporation. https://attack.mitre.org/
- Common Vulnerability Scoring System Version 4.0: Specification Document Version 1.1. FIRST. https://www.first.org/cvss/v4.0/specification-document
- CISA Analysis: Fiscal Year 2023 Risk and Vulnerability Assessments. Cybersecurity and Infrastructure Security Agency.
- (2023). Multi-Source Analysis of Top MITRE ATT&CK Techniques.

Отказ от ответственности: Мнения, выраженные в статье, принадлежат авторам, а не организациям, которые они представляют.
