Свежий отчёт Forescout выявил самую небезопасную категорию электронных устройств.

Согласно недавнему отчёту компании Forescout Technologies – это компания, которая занимается автоматизированной кибербезопасностью в цифровой среде. Она помогает своим клиентам обнаруживать, оценивать и контролировать соответствие всех подключенных устройств.

 Forescout работает с крупными компаниями и предлагает решения для разных отраслей и сценариев. Forescout была основана в 2000 году и имеет офисы в разных странах." data-html="true" data-original-title="Forescout" >Forescout под названием «Самые рискованные подключенные устройства 2024 года», количество уязвимых устройств Интернета вещей (Интернет вещей (англ. Internet of Things, IoT) – концепция сети передачи данных между физическими объектами («вещами»), оснащёнными встроенными средствами для взаимодействия друг с другом или с внешней средой. Организация таких сетей способна перестроить экономические и общественные процессы, исключить из части действий необходимость участия человека.
 Все большая часть IoT-устройств создается для использования потребителями, включая транспортные средства, системы «Умный дом», умную одежду, медицинские устройства и приборы с возможностями удаленного мониторинга.
" data-html="true" data-original-title="IoT" >IoT) увеличилось на 136% по сравнению с прошлым годом. Исследование охватило данные от почти 19 миллионов устройств и выявило, что доля уязвимых IoT-устройств выросла с 14% в 2023 году до 33% в 2024 году.

Наиболее уязвимыми типами IoT-устройств стали точки доступа Wi-Fi, роутеры, принтеры, устройства VoIP и IP-камеры. Около трети (33%) всех проанализированных IoT-устройств имели уязвимости.

Рик Фергюсон, вице-президент по безопасности Forescout, отметил, что злоумышленники в первую очередь нацелены на IoT-устройства, подключенные к корпоративной инфраструктуре, такие как IP-камеры и системы управления зданиями. Эти устройства предоставляют атакующим возможность проникать в системы организаций и покидать их незамеченными.

Исследователи также отметили значительный риск, связанный с медицинскими IoT-устройствами (Интернет медицинских вещей (IoMT) – это сеть подключенных медицинских устройств и приложений, которые собирают, анализируют и передают данные через интернет.

 IoMT используется для мониторинга состояния здоровья пациентов, улучшения диагностики и лечения, а также для повышения эффективности медицинских процессов." data-html="true" data-original-title="IoMT"

>IoMT). 5% из них содержат уязвимости. Наиболее рискованными оказались системы медицинской информации, электрокардиографы, рабочие станции DICOM, системы архивации и передачи изображений и системы выдачи медикаментов. Атаки программ-вымогателей на последние, к слову, уже не раз фиксировались, что препятствовало нормальному лечению пациентов.

IT-устройства составили большинство уязвимых устройств (58%) в отчёте этого года, хотя эти цифры всё равно значительное ниже прошлогодних 78%. Наиболее рискованными IT-устройствами, в свою очередь, стали устройства сетевой инфраструктуры, включая роутеры и точки доступа Wi-Fi.

Фергюсон отметил снижение в некоторых категориях IT-устройств и рост в других, при этом атакующие сосредотачиваются на устройствах, которые часто остаются без управления, таких как точки доступа Wi-Fi и роутеры. В то время, как в прошлом году наиболее частыми точками входа для крупных компрометаций с использованием программ-вымогателей были гипервизоры.

В категории операционных технологий (Operational Technology (OT) или операционные технологии – это область информационных технологий, которая специализируется на управлении и контроле физическими системами и процессами в реальном времени. OT используется в критически важных отраслях, таких как энергетика, производство и транспорт, для автоматизации и контроля оборудования и производственных процессов. Она включает в себя системы управления, датчики, контроллеры и специализированное программное обеспечение, обеспечивающие безопасность и надёжность в работе критических инфраструктур." data-html="true" data-original-title="OT" >OT) самыми рискованными устройствами оказались источники бесперебойного питания (Источники бесперебойного питания (UPS) – это устройства, которые обеспечивают резервное электропитание в случае перебоев в основной сети. UPS защищают оборудование от потерь данных и повреждений, обеспечивая временное питание от батареи до восстановления основной подачи электроэнергии." data-html="true" data-original-title="UPS" >UPS), распределённые системы управления (Распределённые системы управления (DCS) – это автоматизированные системы, используемые для управления процессами на производственных объектах, таких как нефтеперерабатывающие заводы и химические предприятия. DCS управляют и контролируют сложные процессы, распределяя функции управления между несколькими контроллерами." data-html="true" data-original-title="DCS" >DCS), программируемые логические контроллеры (Программируемые логические контроллеры (Programmable Logic Controllers, PLC) — это специализированные устройства, используемые в автоматизации и управлении производственными

процессами. Они представляют собой цифровые компьютеры, спроектированные для мониторинга и управления различными системами и механизмами в промышленных средах.

 PLC способны мониторить сигналы с датчиков, анализировать данные и принимать решения в реальном времени. Они могут управлять разнообразными задачами, такими как автоматическая сортировка, контроль температуры, управление приводами, системами освещения и другими аспектами производственного процесса." data-html="true" data-original-title="PLC" >PLC), робототехника и системы управления зданиями (Системы управления зданиями (BMS) – это системы, которые автоматизируют управление и мониторинг технических и инженерных систем зданий, включая отопление, вентиляцию, кондиционирование воздуха, освещение и безопасность. BMS повышают эффективность и комфорт в здании, а также снижают затраты на эксплуатацию." data-html="true" data-original-title="BMS" >BMS). В общей сложности 4% всех рассмотренных OT-устройств имели какие-либо уязвимости.

Наибольший средний риск использования устройств по отраслям наблюдается в сфере технологий (8,3), образовании (8,14), производстве (7,98) и финансовом секторе (7,95). Интересно, что здравоохранение, которое было самой рискованной отраслью в 2023 году, теперь, согласно Forescout, имеет самый низкий риск — 7,25. Это связано со значительными инвестициями в безопасность устройств, используемых в этой отрасли, за последний год.

Самый высокий средний риск использования устройств по странам был зафиксирован в Китае (7,32), на Филиппинах (6,97), в Таиланде (6,96), Канаде (6,51) и США (6,44). Великобритания показала самый низкий уровень риска среди проанализированных стран — 6,0.

Для повышения кибербезопасности организациям необходимо уделять первоочередное внимание обновлению устаревшего оборудования, своевременному устранению уязвимостей и внедрению передовых средств защиты для эффективного мониторинга и управления подключенными устройствами.