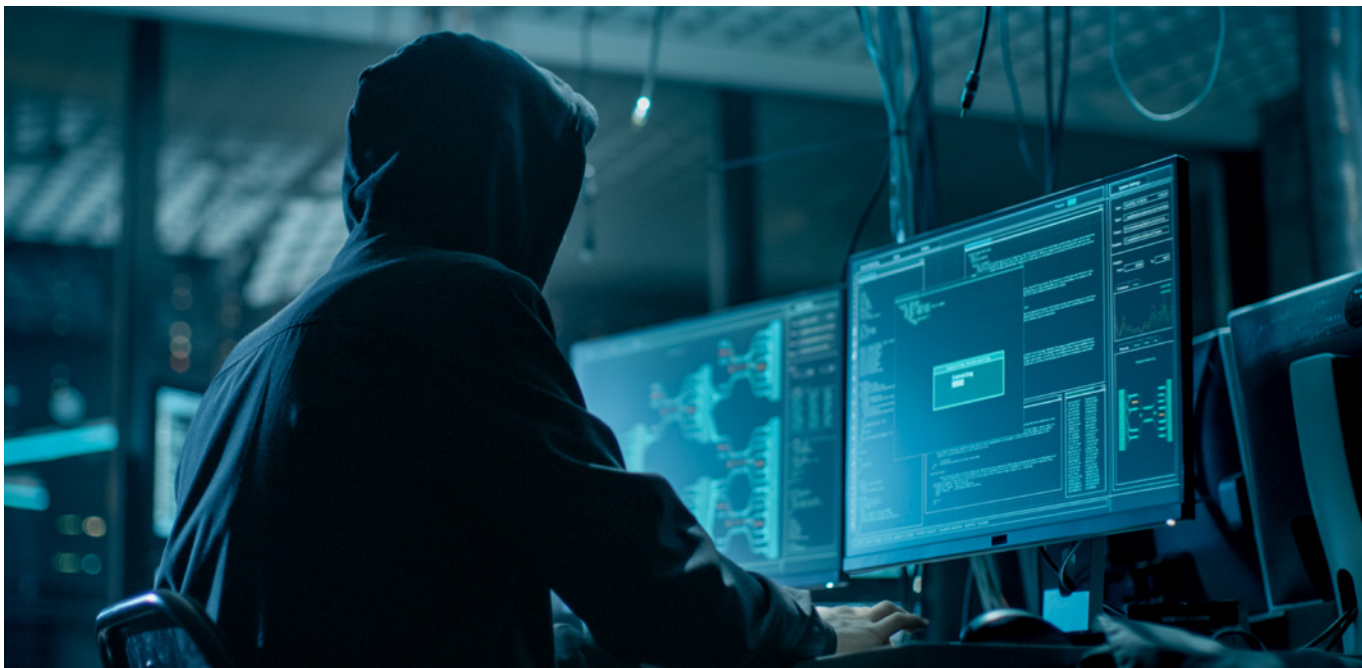


Stay Untouched!

Откройте для себя концепцию «Кактус» MOBOTIX
для защиты охранных видеосистем от кибератак

Представлено:



Вступление – о компании MOVOTIX

Компания MOVOTIX является разработчиком и производителем систем видеонаблюдения и контроля доступа на базе IP-видеокамер, которые видят больше, чем зрение человека. Безопасность — наш приоритет. MOVOTIX является первопроходцем в области технологии децентрализации, объединяющей данные оптического, тепловизионного и звукового датчиков и позволяющей улучшить защиту объектов.

Продукция MOVOTIX разработана для интуитивного управления с поддержкой искусственного интеллекта, что позволяет решать самые сложные задачи видеонаблюдения в области розничной торговли, образования, здравоохранения, транспорта, перевозок и гостинично-ресторанного сектора. Оборудование MOVOTIX не имеет подвижных частей и включает ведущие в отрасли элементы управления кибербезопасностью, что обеспечивает максимальную рентабель-

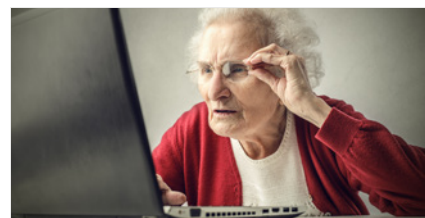
ность инвестиций. Кроме того, гарантируется постоянное обновление программного обеспечения систем.

Почему кибербезопасность так важна для охранных видеосистем?

Видеонаблюдение ежедневно помогает обеспечить безопасность миллиардов людей. От семьи, прогуливающейся по торговому комплексу, безопасность которого обеспечивает бдительное око охранной системы, до обеспокоенных родителей, наблюдающих за спящим ребенком. Видеонаблюдение прочно вошло в жизнь каждого из нас. Примечательно, что по всему миру уже установлено уже более одного миллиона камер MOVOTIX, что стало возможным благодаря нашим сертифицированным партнерам, работающим в 150 странах.

Неудивительно, что охранные видеосистемы, предоставляющие такие важные преимущества, стали потенциальной целью преступников. В прежние времена атаки на сети виде-

онаблюдения были редки в силу замкнутого характера таких систем, которые часто подключались к местным диспетчерским помещениям с помощью прямых кабельных соединений. Однако времена меняются, и современные видеокамеры фактически представляют собой подключенные к видеокамере компьютеры, на которых работает ПО. В связи с развитием Интернета и снижением стоимости камер охранные видеосистемы становятся все более доступными по любой IP-сети и, следовательно, все более уязвимыми для кибератак.



Риск кибератак:

- Чем больше IP-устройств, тем больше целей для атак
- Деактивация устройств и дистанционное управление ими
- Кража данных
- Перехват и использование устройств не по назначению
- Промышленный и государственный шпионаж
- Блокировка из-за атак программ-вымогателей

Возможный ущерб

Успешные кибератаки на охранные видеосистемы и системы контроля доступа могут кончиться человеческими жертвами и нанесением значительного ущерба в результате последующих действий преступников. Кроме того, установка охранных видеосистем все чаще предписывается законом в местах, где разрешена продажа спиртных напитков, или входит в требования страховых компаний. Так, если в результате предотвратимой кибератаки система видеонаблюдения была выведена из строя и преступление не было снято камерой видеонаблюдения, страховые компании могут отказать в выплате страхового возмещения ввиду несоблюдения условий.



Возможный ущерб:

- Финансовые потери, нанесение ущерба деловой репутации
- Меры регулятивного характера, штрафы и преследование по обвинению в халатности
- Расторжение договоров, требования возмещения ущерба
- Человеческие жертвы в результате террористических актов

Защита систем видеонаблюдения также связана с вопросами защиты личных данных. Согласно законам большинства стран, все конфиденциальные личные данные, связанные со здоровьем, финансами, политической принадлежностью и многим другим, должны быть особенно неприкосновенными. Это распространяется и на видеодан-

ные. Например, лица, участвующие в политических митингах, рассчитывают на то, что материалы видеонаблюдения будут храниться в безопасности и не станут всеобщим достоянием. При кибератаках на устройство или сеть видеонаблюдения очень высок риск утечки и кражи личной информации, например, изображений и других данных, позволяющих идентифицировать конкретных лиц. Это нарушило бы права на неприкосновенность частной жизни пользователей, отслеживаемых системой, и могло бы иметь правовые последствия для лица, отвечающего за обработку персональных данных.

Помимо этого, существует серьезная опасность потери деловой репутации, принятия мер регулятивного характера, штрафов и уголовного преследования, если будет доказан факт халатности. В области гражданского права возможно расторжение договоров и подача гражданских и коллективных исков.

Мнение специалистов отрасли

Видеонаблюдение и устройства для контроля доступа являются частью концепции Интернета вещей (IoT). По оценкам Gartner, Cisco и других технологических и исследовательских компаний, к 2020 году количество подключенных к Интернету устройств составит порядка 50 млрд (источник: www.cisco.com). В отличие от радиопередатчиков, телевизионных станций или автотранспортных средств законодательство практически не регулирует устройства, которые можно подключать к Интернету. Не существует никаких утвержденных стандартов, определяющих степень безопасности тех или иных устройств. Однако по мере роста автономности технологии

увеличивается риск того, что незащищенные устройства будут привлекать вирусы, от эпидемий которых страдали пользователи настольных ПК. Подобные вирусы могут появиться, например, в сетях камер видеонаблюдения, а для таких случаев существует довольно мало способов обнаружения и быстрого устранения проблемы.



Атака с помощью ботнета Mirai, 2016 г.

Первый взлом IP-камер

Примеры выведенных из строя серверов:

Сентябрь 2016	Minecraft, OHV
Октябрь 2016	Dyn
Ноябрь 2016	(предвыборная кампания в США): Twitter, Spotify, Amazon
Ноябрь 2016	Интернет в Либерии
Ноябрь 2016	Deutsche Telekom

Атака в реальной жизни

Кибератаки на системы видеонаблюдения зачастую остаются незамеченными или же жертвы не сообщают о них в полицию. Однако если преступникам удастся захватить устройства для видеонаблюдения и затем использовать их в качестве оружия для поражения других интернет-ресурсов, проблема приобретает угрожающие масштабы. Массовая атака осенью 2016 года, затронувшая Twitter, Amazon, Tumblr, Reddit, Spotify и Netflix, была частично порождена сетью устройств видеонаблюдения, захваченных преступниками. Ботнет в основном порастил цифровые устройства записи (DVR) и IP-камеры производства одной китайской компании. Эта компания изготавливает и продает компоненты производи-

телям оборудования, которые используют их в своих собственных про-

дуктах, в результате чего десятки тысяч устройств превращаются в

опасное кибероружие.

Введение в концепцию «Кактус» MOVOTIX

Чтобы противостоять этим угрозам, компания MOVOTIX разработала стратегию кибербезопасности под названием «Кактус», которая представляет собой комплексный подход к защите продукции MOVOTIX от угрозы кибератак.

Кактус символизирует идею, лежащую в основе стратегии кибербезопасности MOVOTIX, где каждое устройство и каждая программа имеют многократную защиту от внешних угроз.

Например, MOVOTIX использует сквозное шифрование без слабых мест, охватывающее источник изображения, цифровые кабели, информационные накопители и систему видеопользователя, — система защищена, как кактус с шипами и прочной кожей. Подобно кактусу, каждый побег которого покрыт шипами, все модули, включая камеру, накопители, кабели и систему управления видео VMS, в системе MOVOTIX оснащены циф-

ровыми «шипами», которые защищают их от несанкционированного доступа.

Однако охранные технологии эффективны лишь настолько, насколько эффективно ими управляет пользователь. Поэтому другая цель концепции «Кактус» состоит в повышении осведомленности потенциальных и существующих клиентов MOVOTIX о важной проблеме безопасности данных в сетевых охранных видеосистемах, а также об интеллектуальных и экономичных методах самозащиты.

Элементы концепции «Кактус»

В отличие от других компаний отрасли видеонаблюдения, MOVOTIX самостоятельно разрабатывает собственное программное обеспечение и не предоставляет лицензий на свои технологии сторонним организациям. Этот инновационный подход дает значительные преимущества в плане безопасности. Контролируя все этапы

разработки программного обеспечения, компания MOVOTIX становится менее уязвимой для таких ситуаций, когда недостаточно хорошо разработанные сторонние программные и аппаратные средства могут привести к проблеме безопасности, что уже случалось с другими компаниями. Концепция «Кактус» отражает принцип «безопасности по определению», заложенной в самой конструкции, которым руководствовалась компания с самого начала и который проявляется во всех областях.



Безопасное программное обеспечение и разработка

Подход MOVOTIX к обеспечению безопасности начинается с разработки операционной системы и стека приложений. Все устройства MOVOTIX созданы на основе модифицированной защищенной ОС Linux, из которой удалены стандартные службы и модули. Критически важные модули Linux, такие как аутентификация, были полностью переработаны инженерами MOVOTIX, чтобы исключить уязвимость этих модулей к стандартным эксплойтам или методам инъекции кода. Это системное



Кактус:

Растет в суровых условиях

Экономичен

Очень устойчивый к вызовам окружающей среды

Долгожитель

Защищен шипами

программное обеспечение не является открытым и защищено дополнительными программными технологиями безопасности. Кроме того, каждое обновление встроенного ПО и элементов программного обеспечения устройства зашифровано и снабжено цифровой подписью, чтобы избежать фальсификации.

Безопасность устройств и безопасная связь

Все созданные камерой записи шифруются самой камерой, начиная с циклического буфера, который использует встроенную SD-карту в каждой камере. Компания MOBOTIX создала безопасную файловую систему. Это означает, что если камера будет физически взломана или украдена, ранее записанное видео, которое все еще находится в камере, невозможно извлечь, не получив предварительно права администратора, защита которых обеспечивается описанными выше процессами безопасной конфигурации. Каждое устройство MOBOTIX можно оснастить средствами защиты от кражи и фальсификации, включая армированные кожухи, видеосенсоры, функции оповещения и сигнализации.

Доступ к интерфейсу конфигурации камеры предоставляется только авторизованным пользователям, а для обеспечения внутренней безопасности каждая система позволяет создавать и применять различные права для разных групп пользователей. На практике это означает, что камеры MOBOTIX никогда не сохраняют пароли пользователей в текстовом виде. Вместо этого пароли хешируются с применением надежного алгоритма одностороннего хеширования (SHA-512). Поэтому даже если файл конфигурации попа-

дет не в те руки, получить пароль в текстовом виде будет чрезвычайно сложно. Неиспользуемые службы ОС Linux отключены, чтобы ограничить возможности потенциальных эксплойтов и предотвратить атаки. Также отсутствует недокументированный мастер-пароль: доступ к камере MOBOTIX и ее настройка осуществляются исключительно через ее собственный веб-интерфейс (графический пользовательский интерфейс).



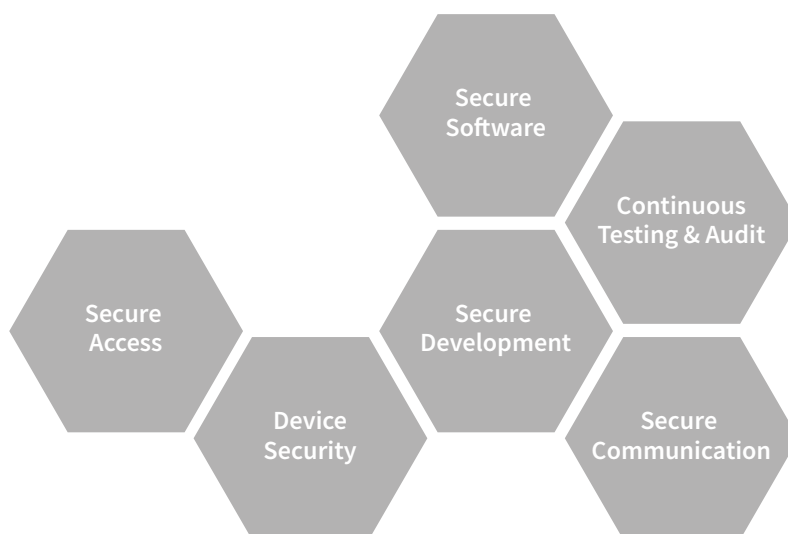
Безопасная сеть и связь между устройствами

Все данные, которыми камеры MOBOTIX обмениваются с другими узлами сети, можно зашифровать и обеспечить таким образом их конфиденциальность и целостность при передаче. Технология HTTPS (SSL/TLS), используемая также для защиты сайтов интернет-банкинга, и цифровые сертификаты поддерживаются в стандартной комплектации. Это обеспечивает соответствие рекомендациям специалистов по защите крупнейших инфраструктур безопасности.

MOBOTIX также предусматривает встроенную поддержку управления уникальными сертификатами X.509 на каждой камере и корневыми центрами сертификации, чтобы организации могли расширять безопасность устройств, охватывая камеры и дверные коммуникаторы, для аутентификации которых используются системы типа OpenVPN. Это означает, что если камера будет физически украдена или взломана, злоумышленник не сможет атаковать остальную сеть камер, используя учетные данные уязвимой камеры.

Постоянное тестирование и аудит

Однако все эти меры безопасности нуждаются в валидации и подтверждении их эффективности. В этих целях MOBOTIX пользуется услугами SySS — авторитетной независимой компании по проверке безопасности, которая тестирует безопасность оборудования и программного обеспечения. Проверка включает тестирование на проникновение, в ходе которого специалисты моделируют действия хакера, пытающегося взломать элементы управления. Это позволяет устранить уязвимости еще до поступления продукции в производство.



Системы MOBOTIX: Stay Untouched

Чем большую популярность завоевывают системы видеонаблюдения, тем чаще они становятся целью кибератак. Устройства MOBOTIX имеют активную защиту от такого рода угроз. Цель концепции «Кактус» состоит в повышении осведомленности потенциальных и существующих клиентов MOBOTIX о чрезвычайно важной проблеме безопасности данных в сетевых охранных видеосистемах.

Компания MOBOTIX предоставляет инструменты, позволяющие клиентам повысить безопасность систем видеонаблюдения. Кроме того, безопасность является фундаментальным преимуществом систем MOBOTIX. Мы рады сотрудничать с другими компаниями нашей отрасли, клиентами и правительственными учреждениями в целях защиты систем и технологий, помогающих сделать общество более безопасным для всех.

Для получения более подробной информации о концепции «Кактус» посетите сайт:

www.cactusconcept.com

Отдел новостей

Выбор продукта

Найти партнера

Login Partner Section

Язык

MOBOTIX

Решения

Продукты

Поддержка

Компания

Партнеры

Q

The MOBOTIX Cactus Concept

Stay Untouched.



Вам знакомы преимущества сетевого защитного решения для видеосистем, в оборудовании и программном обеспечении которой реализована концепция «Кактус»?

Наверное, это очень дорого? Не волнуйтесь. Никто не хочет (да и не должен) чрезмерно тратить на безопасность. К сожалению, мы живем в мире, где многие люди, которые хотят получить идеальную видеосистему, недооценивают значимость ее надежности. И рано или поздно расплачиваются за это. Дело в том, что в наше время ни одну систему нельзя назвать надежной без комплексной сквозной защиты от растущей опасности кибератак международных хакеров.

Компания MOBOTIX разработала уникальную концепцию «Кактус» для надежной и полной защиты комплексных видеосистем от хакерских атак. Защитите себя от будущих атак, когда кто-либо попытается превратить ваш цветущий IT-ландшафт в IT-пустыню. Поставьте заслон серьезным атакам с помощью интеллектуальной видеосистемы, которая не только готова к работе, но может противостоять постоянно меняющимся вызовам нашего мира. Бесперебойно. Без дополнительных расходов.

Видеосистемы MOBOTIX являются одними из самых безопасных в мире. Благодаря необычной децентрализованной технологии они уже в стандартной комплектации оснащаются множеством эффективных средств защиты от хакерских атак. Узнайте больше о концепции MOBOTIX «Кактус» и о преимуществах, которые вы можете получить от защищенной видеосистемы.

[Руководство по киберзащите >](#)

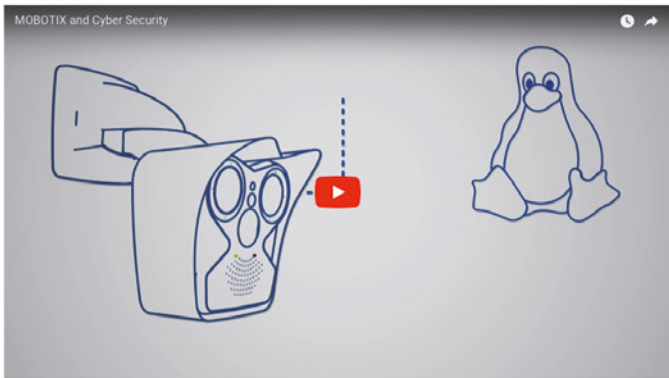
Официальный документ: кибербезопасность

Число кибератак на устройства и инфраструктуру систем видеонаблюдения постоянно растет. В нашем официальном документе вы узнаете об отраслевом лидерстве компании MOBOTIX в борьбе с этой тревожащей тенденцией, а также ознакомитесь с передовым опытом по созданию более устойчивой и безопасной рабочей среды.

Заполните бланк и получите ссылку для скачивания по электронной почте.

Следите за обновлениями прошивок и ПО к вашим камерам MOBOTIX.

[Download >](#)



Подробнее о концепции MOBOTIX «Кактус»

Цель концепции «Кактус»	>
Комплексная безопасность	>
Долговечная конструкция без движущихся частей	>
Исключительная экономность и малая потребность в обслуживании	>
Высокая термо- и погодостойчивость	>
Несомненная польза	>
Впечатляющее концептуальное решение	>
Эволюция без революций	>

Beyond Human Vision

Наше уникальное коммерческое предложение — это больше чем просто предложение отдельных функций или конструктивных элементов.

Уникальное коммерческое предложение MOBOTIX - это полноценный пакет технологий, инноваций и исключительного качества, позволяющий предложить

законченное решение. Это сочетание высокоинженерных инструментов предоставляет гибкость для максимально эффективного и надежного решения

задач современного мира. MOBOTIX выходит за рамки человеческого видения, чтобы помочь вам сегодня быть готовыми к вызовам завтрашнего дня!



RU_05/18

MOBOTIX AG

Kaiserstrasse
D-67722 Langmeil
Tel.: +49 6302 9816-103
Fax: +49 6302 9816-190
www.mobotix.com



MOBOTIX

