Белые страницы

Кибербезопасность Hikvision

www.hikvision.com

О настоящем документе

В данном документе Hikvision, посвященном кибербезопасности, представлен обзор текущей практики Hikvision в отношении кибербезопасности продуктов, а также обеспечен открытый доступ к описанию возможностей кибербезопасности Hikvision.

Hikvision сохраняет за собой право обновлять данный Документ. Последнюю редакцию настоящей Документа можно найти на сайте нашей компании (http://www.hikvision.com/en/).

Белая книга

©2018 Hangzhou Hikvision Digital Technology Co., Ltd.

ВСЕ ПРАВА ЗАЩИЩЕНЫ.

Данный документ не подлежит воспроизведению, изменению, переводу или распространению, частично или целиком, в любой форме или любыми средствами без предварительного письменного разрешения Hikvision.

Торговая марка

海康威视, HIKVISION и другие торговые марки Hikvision и логотипы являются интеллектуальной собственностью Hikvision в различных юрисдикциях. Другие торговые марки и логотипы, содержащиеся в руководстве, являются собственностью их владельцев.

Правовая информация

ДО МАКСИМАЛЬНО ДОПУСТИМОЙ СТЕПЕНИ, РАЗРЕШЕННОЙ ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, СОДЕРЖАНИЕ, ОПИСАННОЕ В НАСТОЯЩЕМ ДОКУМЕНТЕ, ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ», HIKVISION НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ГАРАНТИИ ПРИГОДНОСТИ ДЛЯ ПРОДАЖИ ИЛИ ИНЫХ ЦЕЛЕЙ И ИНОГО ИСПОЛЬЗОВАНИЯ.

HIKVISION НЕ ПРЕДОСТАВЛЯЕТ НИКАКИХ ГАРАНТИЙ В ОТНОШЕНИИ ТОЧНОСТИ ДАННОГО ДОКУМЕНТА И ОСТАВЛЯЕТ ЗА СОБОЙ ПРАВО ИЗМЕНЯТЬ ИЛИ ИСПРАВЛЯТЬ СОДЕРЖИМОЕ БЕЗ КАКОГО-ЛИБО ПРЕДВАРИТЕЛЬНОГО УВЕДОМЛЕНИЯ.

HIKVISION НЕ НЕСЕТ ОТВЕТСТВЕННОСТЬ ЗА ЛЮБЫЕ РЕШЕНИЯ, ПРИНЯТЫЕ В СВЯЗИ С ИСПОЛЬЗОВАНИЕМ ЭТОГО ДОКУМЕНТА, А ТАКЖЕ ЗА ЛЮБЫЕ ВОЗМОЖНЫЕ ПОСЛЕДСТВИЯ.

В СЛУЧАЕ КОНФЛИКТОВ МЕЖДУ НАСТОЯЩИМ РУКОВОДСТВОМ И ДЕЙСТВУЮЩИМ ЗАКОНОДАТЕЛЬСТВОМ, ПОСЛЕДНЕЕ ПРЕВАЛИРУЕТ.

Лист регистрации изменений

Выпуск - январь 2018 года

О компании

Компания Hikvision является ведущим мировым поставщиком инновационных продуктов и решений для видеонаблюдения.

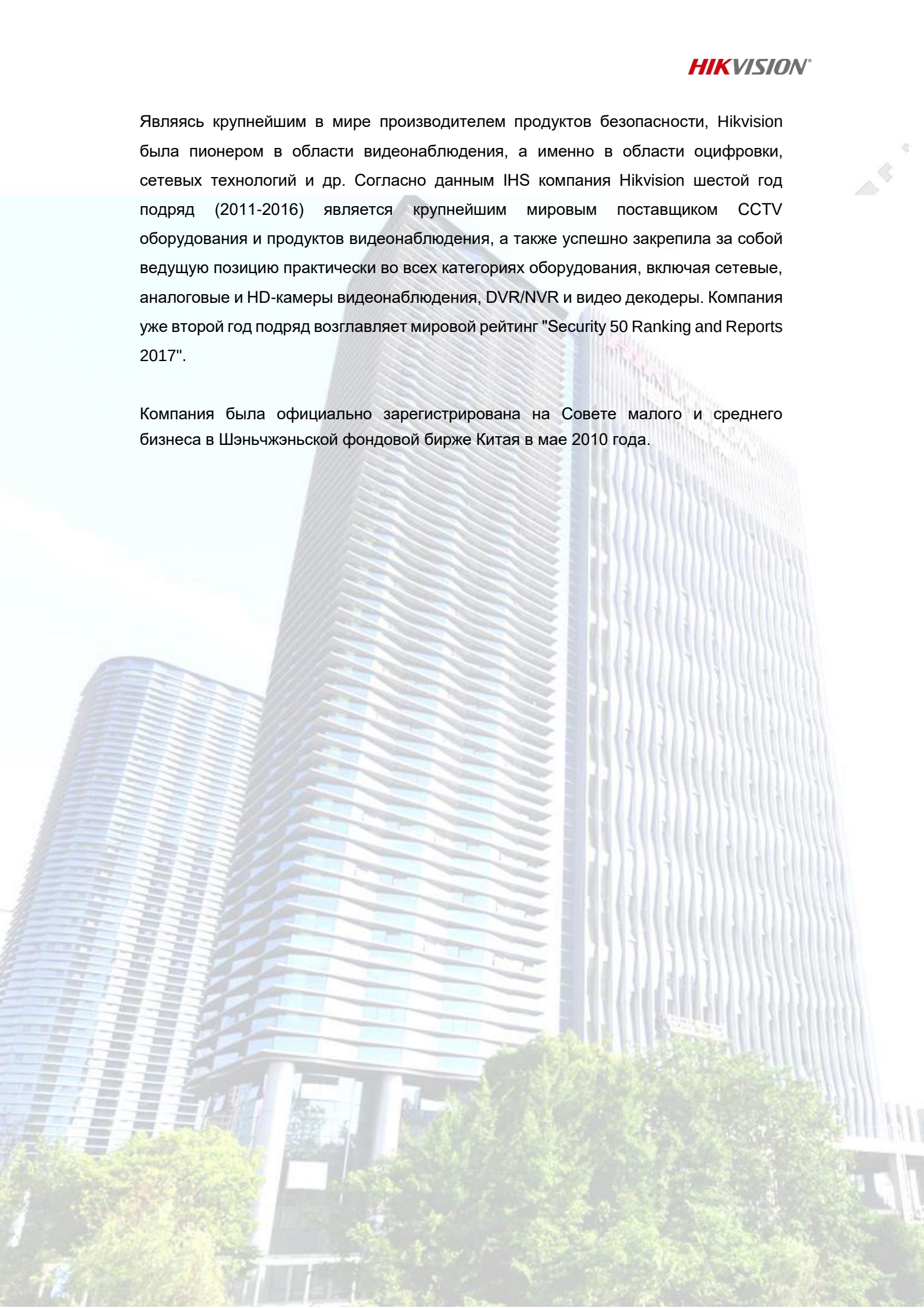
В настоящее время Hikvision насчитывает более 20,000 сотрудников, включая 9,300 инженеров отдела исследований и разработок. Компания ежегодно инвестирует 7-8% своего годового дохода от продаж в исследования и разработки. Hikvision создала замкнутую многоуровневую систему НИОКР, которая включает все этапы от исследования до проектирования, разработки, тестирования, технической поддержки и обслуживания. Команда НИОКР, расположенная в головном офисе в Ханчжоу, осуществляют деятельность по всему миру, включая научно-исследовательские центры в Монреале, Канаде и Кремниевой долине, Калифорнии в Северной Америке, а также в Пекине, Шанхае, Чунцине и Ухане в Китае.

Hikvision продвигает ключевые технологии кодирования аудио и видео, обработки видеоизображения и хранения данных, а также такие перспективные технологии, как облачные вычисления, большие данные и глубинное обучение. За последние несколько лет Hikvision углубила свои знания и получила необходимый опыт в удовлетворении потребностей клиентов на различных вертикальных рынках, включая рынок общественной безопасности, транспорта, торговли, образования, здравоохранения, финансовых учреждений и энергетики, а также рынок умных зданий. Соответственно, компания предоставляет профессиональные и индивидуальные решения, соответствующие самым разным требованиям. Помимо рынка видеонаблюдения Hikvision предлагает решения для умного дома, промышленной автоматизации и робототехники согласно своей долгосрочной стратегии развития.

Hikvision создала одну из наиболее крупных маркетинговых сетей в отрасли, которая насчитывает 33 зарубежных региональных филиала и 35 отделений по всему Китаю, для оперативного удовлетворения потребностей клиентов, пользователей и партнеров. Продукты Hikvision применяются на разнообразных вертикальных рынках, охватывая более 100 стран, например, центр отдыха и развлечений в Филадельфии в США, проект безопасного города в Сеуле в Южной Корее, гавань Дун-Лэаре в Ирландии, аэропорт Мальпенса в Милане, Банк Индии, и это лишь некоторые из них.

Являясь крупнейшим в мире производителем продуктов безопасности, Hikvision была пионером в области видеонаблюдения, а именно в области оцифровки, сетевых технологий и др. Согласно данным IHS компания Hikvision шестой год подряд (2011-2016) является крупнейшим мировым поставщиком CCTV оборудования и продуктов видеонаблюдения, а также успешно закрепила за собой ведущую позицию практически во всех категориях оборудования, включая сетевые, аналоговые и HD-камеры видеонаблюдения, DVR/NVR и видео декодеры. Компания уже второй год подряд возглавляет мировой рейтинг "Security 50 Ranking and Reports 2017".

Компания была официально зарегистрирована на Совете малого и среднего бизнеса в Шэньчжэньской фондовой бирже Китая в мае 2010 года.



СОДЕРЖАНИЕ

О компании 3
1. Письмо генерального директора....7
2. Предисловие 9
3. Угрозы безопасности в интернете вещей....11
Уровень восприятия....11
Сетевой уровень 12
Прикладной уровень 12
4. Сетевая и информационная безопасность в отрасли видеонаблюдения 13
5. Жизненный цикл продукта....15
5.1 Организация 15
Комитет безопасности продуктов 16
Отдел сетевой безопасности 17
Лаборатория сетевой и информационной безопасности....17
HSRC: Центр реагирования на угрозы безопасности Hikvision 17
Отделы управления безопасностью продуктовых линеек 17
Отдел тестирования безопасности....18
Отделы поддержки....18
5.2 Процедуры и стандарты 18
Общие положения для обеспечения безопасности продукта....19
Документы по процедуре обеспечения безопасности продукта....19
Базовые уровни безопасности 19
5.3 Процесс исследований и разработок в области безопасности HSDLC 19
Определение концепции....20
Этап проектирования....20
Этап разработки....21
Этап проверки 21
Управления конфигурацией 22
Спецификации управления сборкой проекта....22
Центр сбора и компиляции....22
Управление компонентами....23
Управление инструментальным и сторонним компонентом 23

Подготовка сотрудников 24
Экстренное реагирование 24
Управление уязвимостями 25
5.4 Безопасность сбытовых цепочек 26
5.5 Соответствие требованиям безопасности 27
ISO/IEC 9001 29
ISO/IEC 27001 29
Сертификация зрелости программного обеспечения CMMI5 29
Ступенчатая защита информационной безопасности 30
Аудит SOC 30
5.7 Обмен и сотрудничество 32
6. Исследование безопасности продукта 34
6.1 Уязвимость при эксплуатации 34
6.2 Осведомленность об угрозах безопасности 35
..... 36
Оценка уязвимости 36
Визуализация безопасности 36
6.3 Система-ловушка для хакеров 37
7. Обязательства в отношении обеспечения безопасности 38

1. Письмо генерального директора

«Интернет всего» становится реальностью. В преддверии реализации проекта «интернета всего», технология видеонаблюдения стремительно развивалась за прошедшие 10 лет. Преодолев путь от аналоговой эры к цифровой, а затем и к сетевой эре, видеонаблюдение переходит на новый уровень, эру умного видеонаблюдения. Усовершенствования технологий могут способствовать развитию человеческого общества, но они также могут стать причиной возникновения новых проблем. Например, развитие интернет-технологий в значительной степени приносит пользу человеческому обществу, но оно также порождает проблемы, связанные с угрозами кибербезопасности. То же самое относится к технологии интернета вещей (IoT), которая разработана на основе интернета, и схожа с ним в том плане, что значительно улучшает жизнь человека. Однако она также порождает новые проблемы для общества и кибербезопасность - одна из таких проблем.

Индустрия видеонаблюдения вошла в цифровую эру позже ИТ-индустрии, а осведомленность о кибербезопасности остается относительно слабым местом данной отрасли. В 2014 Hikvision основала «Центр реагирования на угрозы безопасности» для создания централизованного внешнего интерфейса с целью решения вопросов кибербезопасности. В 2015 Hikvision открыла «Лабораторию сетевой и информационной безопасности», которая включена в систему кибербезопасности Hikvision. Совместно с лабораторией сетевой и информационной безопасности и отделом информационной безопасности, был сформирован комитет по обеспечению безопасности продуктов. Компания также создала лабораторию тестирования безопасности и систему сетевой безопасности, которая ориентирована на организацию, процедуры и, в особенности, на проекты безопасности сети. Данная лаборатория создана для улучшения общих стандартов кибербезопасности продуктов и систем компании.

Однако за кибербезопасность продукта отвечает не только производитель. Все, кто участвуют в жизненном цикле проекта, включая пользователей, системных интеграторов, операторов, проектировщиков и других поставщиков услуг, также ответственны за использование передовых средств защиты кибербезопасности и сталкиваются с теми же проблемами, что и производитель. Технологии - составляют лишь 30 процентов от решения данных проблем, остальные 70 – управление. Все заинтересованные стороны должны работать сообща, чтобы бороться с возможными препятствиями в области кибербезопасности.

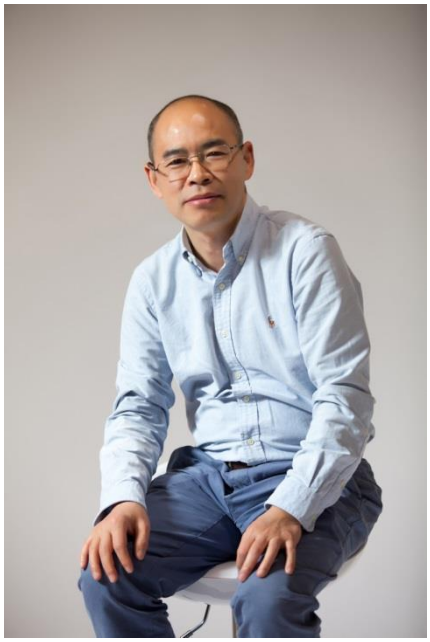
Сейчас, когда индустрия видеонаблюдения отчаянно нуждается в объединении сил для решения проблем, с которыми мы все сталкиваемся, мы отмечаем рост внимания и обеспокоенности общественности и средств массовой информации к вопросу безопасности интернета

вещей. Мы осознаем свою ответственность и миссию в данном вопросе. Hikvision отстаивает такие принципы и ценности компании, как направленность на успех клиента, ценностно-ориентированность, честность и практичность, стремление к совершенству. Hikvision в первую очередь уделяет внимание сетевой и информационной безопасности своих клиентов в отношении прибыли компании.

Угроза кибербезопасности всегда будет существовать, поэтому мы не должны терять бдительность и продолжать работать над улучшением безопасности продуктов.

Ху Ян Чжун, Президент

Hangzhou Hikvision Digital Technology Co., Ltd.



2. Предисловие

За последние пять лет мы стали свидетелями развития оцифровки в индустрии видеонаблюдения и стремительного развития самой отрасли. За эти пять лет мы увидели, как индустрия умного видеонаблюдения вплотную занялась изучением и поиском путей внедрения интернета вещей, и мы рады тому, что именно данная отрасль возглавила разработку, изучение и внедрение технологии IoT.

Безусловно, развитие индустрии умного видеонаблюдения должно отвечать тенденциям в области оцифровки, сетевых и умных технологий. Однако кибербезопасность совершенно новая область для индустрии видеонаблюдения. Открытость сетей связала системы безопасности, которые ранее были независимыми и полностью изолированными, и обеспечила поток и обмен данными, что значительно упростило и улучшило жизнь общества. Это привело к еще более инновационным возможностям, позволило индустрии интернета вещей расти и вывело развитие цивилизации на новый уровень.

Во время перехода индустрии видеонаблюдения от «аналогового», «изолированного» и «накопленных данных» к «цифровому», «сетевому» и «умному» мы оценили преимущества, которые цифровая и сетевая революция привнесли в отрасль. Но мы также стали свидетелями медленного распространения различных видов преднамеренных кибератак из интернета. Кроме того, поскольку современные системы безопасности основаны на «бесшовном» переключении с оригинальных систем безопасности, некоторые из особенностей отрасли могут содержать возможные дефекты при размещении в сетевой среде.

Hikvision - один из лидирующих поставщиков продуктов видеонаблюдения на мировом рынке для более чем 155 стран и регионов. Как компания такого масштаба, Hikvision относится к этим проблемам со всей серьезностью. Наша компания прекрасно понимает с технической точки зрения, как поддерживать и улучшать здоровье, благополучие и безопасность населения.

Кибербезопасность — это проблема не определенной страны или компании. Все заинтересованные стороны, правительства и компании должны понимать, что проблема кибербезопасности — это проблема, с которой сталкиваются все в мире и для решения этой проблемы требуется международное сотрудничество, поиск методов предотвращения угроз и применение лучших практик обеспечения кибербезопасности. В связи с резким ростом «кибератак в Америке» [1], вредоносных программ, как «EternalBlue» и многих других, очевидно, что мы вступили в новую

[1] https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

эру в борьбе с киберпреступностью. Для эффективного решения проблем безопасности, заинтересованные стороны должны сформировать механизмы доверия и сотрудничества.

Hikvision берет на себя следующие обязательства: поддерживать и придерживаться международно признанных стандартов кибербезопасности и лучших практик; поддерживать научные исследования по расширению возможностей защиты сети; совершенствовать и использовать открытые методы защиты, чтобы пользователи могли оценить возможности кибербезопасности Hikvision.

Мы и впредь будем прислушиваться к нашим клиентам для совершенствования и улучшения процедур, технологий и методов обеспечения кибербезопасности.

3. Угрозы безопасности в интернете вещей

Угрозы безопасности в интернете вещей можно классифицировать следующим образом: угрозы уровня восприятия, угрозы сетевого уровня и угрозы прикладного уровня.

Уровень восприятия

- Кража устройства или его повреждение:

  Оборудование интернета вещей, которое не имеет физической защиты и установлено в отдаленных местах, может быть украдено или повреждено.

- Вмешательство в работу или подделка устройства:

  Уличные терминалы и прочие установки могут подвергаться нападениям, вмешательствам и подделке.

- Атака известных уязвимостей:

  К таким известным уязвимостям относятся ОС или программное обеспечение с истекшей лицензией, и неисправленные уязвимости. Огромное количество устройств IoT указывают на наличие проблем процесса обновления и обслуживания.

- Специальные механизмы атак и обхода процедур проверки личности пользователя:

  Использование слабых паролей или паролей по умолчанию в среде интернета вещей.

- Кража конфиденциальной информации:

  Конфиденциальная информация в форме обычного текста, который хранится непосредственно в самом устройстве, легко доступна для чтения и вмешательства.

- Устройства дистанционного управления:

  Наличие тестовых и отладочных портов в прошивке, делает ее уязвимой для удаленного доступа злоумышленников, если не приняты надлежащие меры безопасности.

  Порт отладки не имеет ограничений на выполнение кода, а значит злоумышленники могут полностью управлять устройством через этот порт.

- Кража персональных данных:

  Утечка персональных данных при сборе, передаче или обработке данных в интернете вещей.

Сетевой уровень

- Внедрение в сеть через беспроводной доступ:

  К недостаткам беспроводных протоколов относится отсутствие надежной аутентификации, что может привести к несанкционированному доступу к персональным данным.

- Атака незашифрованного сетевого потока:

  Незашифрованный поток может быть перехвачен, скопирован или искажен нежелательным посредником. Злоумышленники также могут получить доступ к конфиденциальной информации, если во время связи с устройствами, облачными и мобильными терминалами, команды управления и собранные данные не зашифрованы.

- Кибератаки и вторжения из интернета:

  Проблемы безопасности, с которыми сталкиваются IP-системы: атаки и вторжения из интернета.

- DoS-атаки:

  DDoS-атаки, вызванные вирусами.

Прикладной уровень

- Трудности в управлении процессом обновления и безопасности различных устройств, управляемых на прикладном уровне.
- Угрозы нарушения конфиденциальности и безопасности, вызванные несанкционированным доступом.
- Отсутствие обновления и/или проверки конфигураций безопасности.

Рассмотрев множество скрытых угроз безопасности в интернете вещей, включая аппаратные средства, программное обеспечение и среду, а также сложности вычислительных возможностей, Hikvision создала видеоцентрированное решение для интернета вещей с абсолютно новой многофункциональной системой безопасности, которая сможет обеспечить защиту конечных устройств, данных, приложений, систем и сети, с соблюдением требований безопасности.

Программное обеспечение, аппаратные и облачные сервисы тесно связаны в платформе интернета вещей Hikvision. Они работают вместе, чтобы обеспечить самый безопасный опыт использования для пользователей. Многие функции безопасности включены по умолчанию, а основные функции безопасности, такие как активация и шифрование устройства, не могут быть изменены для предотвращения их случайного отключения пользователем.

4. Сетевая и информационная безопасность в отрасли видеонаблюдения

Индустрия видеонаблюдения прошла долгий путь от аналогового до цифрового видеонаблюдения. В аналоговую эру системы видеонаблюдения функционировали в частных сетях, поэтому отрасль была ориентирована на стоимость продукта, производительность и простоту использования. Кибербезопасность систем в то время не была основным направлением, но по мере того, как индустрия видеонаблюдения стремительно развивала сетевое подключение, она переходила от аналоговой эры к цифровой, что позволило перенести лучшие методы информационной безопасности в эру цифровых технологий. Ранее производители индустрии видеонаблюдения, как правило, включали поддержку по умолчанию для всех протоколов, чтобы обеспечить более удобное использование своего продукта с устройствами сторонних производителей. Также был активирован автоматический выбор протокола на сервере. Несмотря на то, что данные настройки делают продукт гораздо более удобным для клиента, они не соответствуют рекомендациям по обеспечению безопасности информации.

В последние годы индустрия видеонаблюдения сталкивается с проблемами кибербезопасности, вызванными развитием продуктов и отрасли. Хотя некоторые могут утверждать иное, наличие этих проблем не означает, что вся индустрия уязвима. Более того, отрасль в настоящее время предпринимает совместные усилия для решения потенциальных угроз безопасности и внедряет эффективные контрмеры.

Объективно говоря, проблемы кибербезопасности относятся не только к индустрии видеонаблюдения, а являются проблемами, с которыми сталкивается общество в целом. Рассматривая всю ИТ область, проблемы кибербезопасности существуют во всех областях, и найден следующий консенсус:

Распространенность уязвимостей системы безопасности

Не существует ИТ-системы или продукта без уязвимостей. На самом деле уязвимость систем безопасности весьма распространенное явление. В каждом продукте миллионы строк кода и, если хотя бы один параметр или строки установлены неверно, это может привести к уязвимости высокого уровня риска в системе. На сегодняшний день автоматические или ручные методы не способны выявить все возможные проблемы кибербезопасности. Поэтому решение проблем безопасности продукта очень актуально.

Безопасность всей системы

Безопасность одной точки не может гарантировать безопасность всей системы. Вся система должна быть надежно защищена. Для обеспечения безопасности систем видеонаблюдения все внешние, внутренние, сетевые, охранные устройства и платформа должны работать сообща и дополнять друг друга. Кибератака любого связанного устройства приведет к уязвимости, которая может отразиться на всей системе.

Стороннее программное обеспечение с открытым исходным кодом

В настоящее время используется множество стороннего программного обеспечения с открытым исходным кодом в различных типах систем. Такое открытое, общее и бесплатное программное обеспечение превалирует среди разработчиков. Оно также является важным компонентом в цепи поставок программного обеспечения. Но поскольку компании пользуются преимуществами программного обеспечения с открытым исходным кодом, такие продукты также несут огромные риски для безопасности. За последние годы в программном обеспечении с открытым исходным кодом часто наблюдаются уязвимости высокого уровня риска, например, Struts2, OpenSSL и прочие. Многие из этих компонентов используются в нижних слоях информационных систем и имеют очень широкую область применения. Таким образом, уязвимости наносят ущерб не только конкретным продуктам, но и целым отраслям промышленности.

Безопасность в динамическом балансе

«Абсолютной» безопасности не существует. Безопасность может быть только относительной. Наступательные и оборонительные стратегии - игра с нулевой суммой. Механизмы и методы, которые сегодня считаются безопасными, уже завтра

могут перестать быть таковыми. Продукты, которые сегодня считаются безопасными, могут быть взломаны. Это означает, что у безопасности нет предела. Каждый продукт будет иметь проблемы с информационной безопасностью в течение своего жизненного цикла; вопрос только в том, возникнут ли эти проблемы и когда.

➢ **Управление безопасностью продуктов**

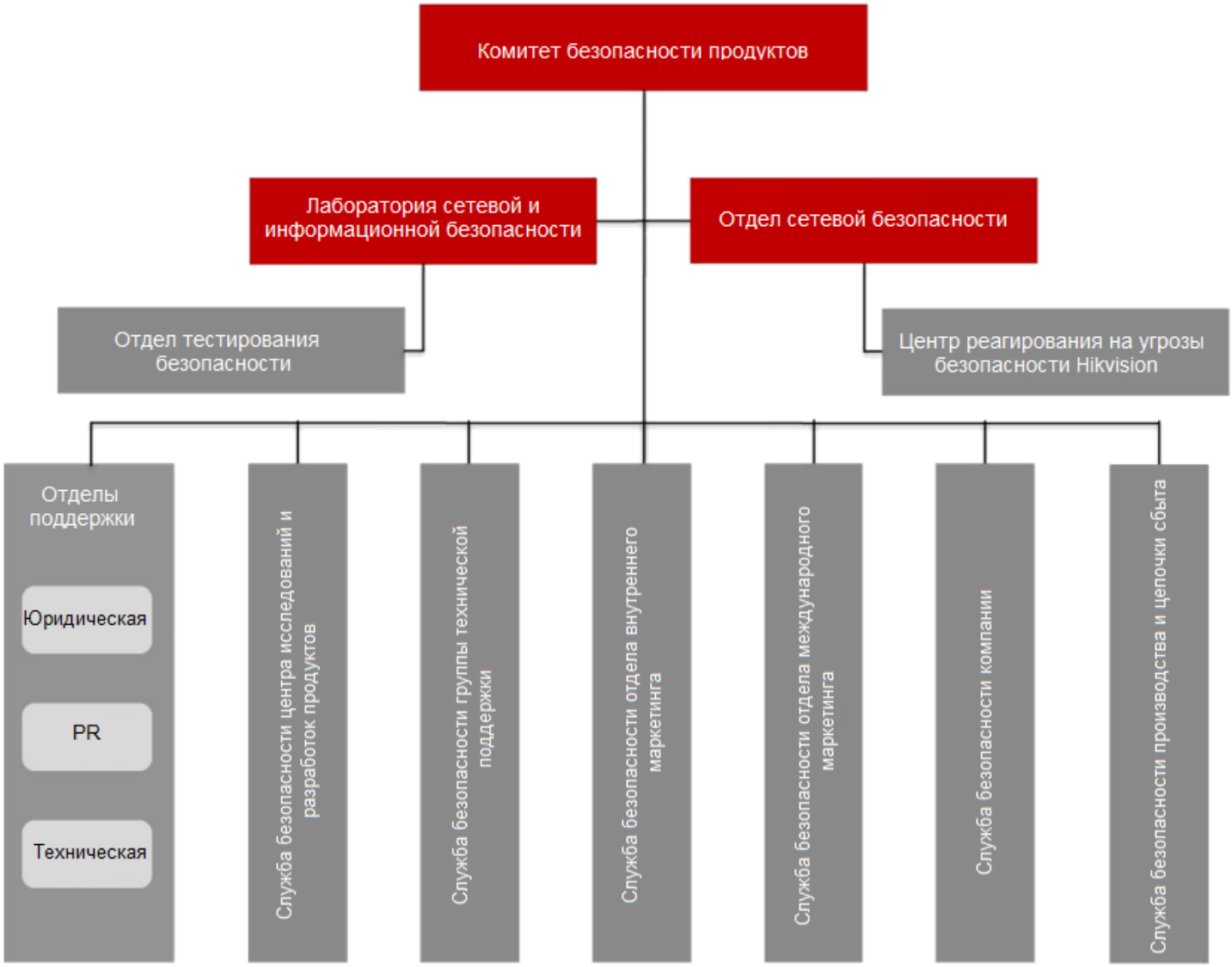
Важнейшим элементом системной безопасности является управление безопасностью. Даже если системы более безопасны, если пользователь не может управлять ими или работать с ними определенным образом, это не обеспечивает полную безопасность системы. В настоящее время некоторые проблемы безопасности в индустрии видеонаблюдения в основном возникают по причине «ненадлежащего» использования и неэффективного управления безопасностью. Многие устройства кибербезопасности по-прежнему имеют «слабые» пароли, а в некоторых системах безопасности не установлены брандмауэры или другое оборудование для обеспечения безопасности. Пользователям также необходимо обращать внимание на предупреждения по безопасности от производителей, обновлять прошивку до последней версии и устанавливать исправления для системы безопасности как можно скорее. В конечном счете, все устройства, подключенные к интернету, должны поддерживать установку исправлений, которая информирует пользователей о необходимости установки Patch-файлов.

5. Жизненный цикл продукта

Этот раздел включает семь аспектов, которые описывают работу Hikvision по созданию жизненного цикла продукта.

5.1 Организация

Для включения деятельности по обеспечению безопасности продуктов в процессы разработки, сбытовую цепочку, маркетинг и продажи, доставку, техническое обслуживание и другие процессы, сначала необходимо создать организационную структуру, которая сможет гарантировать ее реализацию и возложить четкие обязанности на каждую из групп. Ниже приводится структура Hikvision:



Комитет безопасности продуктов

Комитет безопасности продуктов отвечает за стратегическое планирование и разработку политики для сетевой и информационной безопасности компании. Относительно сетевой информационной безопасности, при возникновении вопросов или проблем, комитет имеет право принимать решения и вносить необходимые коррективы. Ху Ян Чжун, президент Hikvision выступает в качестве председателя. Комитет безопасности продуктов создал специализированный департамент сетевой безопасности, который занимается разработкой стратегий, политики, процедур и стандартов сетевой и информационной безопасности, а также ежедневно управляет распределением ресурсов.

Отдел сетевой безопасности

Мы создали отдел сетевой безопасности, который работает совместно с отделом исследований и разработок и другими отделами Hikvision, для составления планов обеспечения безопасности, которые смогут защитить от атак и улучшить защиту системы. Будучи постоянным элементом комитета безопасности продуктов, отдел сетевой безопасности отвечает за реализацию стратегий по обеспечению безопасности продуктов, установку базового уровня их безопасности, внедрение оценки безопасности, внешнее сотрудничество, исследование технических стандартов, продвижение исследований и разработок, участие в обзоре основных событий и предоставление рекомендаций руководителям компании. Данный отдел также отвечает за соответствие стратегии безопасности продуктов компании с отраслевыми требованиями, создание спецификаций исследований и разработок, внедрение элементов безопасности в процесс исследований и разработок, и обеспечение их применения в различных продуктовых линейках.

Лаборатория сетевой и информационной безопасности

Лаборатория сетевой и информационной безопасности исследует и внедряет технологии, связанные с безопасностью интернета вещей. В основном она занимается информированием о IoT, обеспечением безопасности компонентов и продуктов видеонаблюдения, проведением испытаний на возможность проникновения в систему, обеспечением защиты IoT и других областей. Данная лаборатория занимается исследованием передовых технологий безопасности IoT и совершенствует их.

HSRC: Центр реагирования на угрозы безопасности Hikvision

Центр реагирования на угрозы безопасности Hikvision собирает, обрабатывает и выявляет уязвимости продуктов или решений Hikvision. Наша компания дорожит своей безопасностью и всегда стремится обеспечить безопасность своих пользователей. Мы также надеемся использовать данный центр в качестве платформы для расширения сотрудничества и обмена опытом внутри отрасли.

Отделы управления безопасностью продуктовых линеек

Каждая линейка продуктов Hikvision имеет собственный отдел управления безопасностью, который работает совместно с отделом сетевой безопасности над установкой базового уровня безопасности и соответствующими техническими стандартами продуктов, а также отвечает за реализацию таких процессов, как планирование, исследование и разработка, а также тестирование требований безопасности к линейке продуктов.

Отдел тестирования безопасности

Отдел тестирования безопасности выполняет тестирование безопасности продуктов для всех линеек Hikvision. Данный отдел отвечает за проверку политики безопасности продуктов компании и эффективность использования базовых уровней безопасности. Он также отвечает за обеспечение безопасности выпущенных продуктов и предотвращение различных типов угроз безопасности, которые могут возникнуть в процессе исследований и разработок.

Отделы поддержки

Данные отделы отвечают за исполнение соответствующего внутреннего контроля, законов и правил, продвижение бренда, аудит и PR-поддержку по вопросам, связанным с безопасностью продукта.

5.2 Процедуры и стандарты

Компания Hikvision разработала набор базовых уровней безопасности продуктов, на основе национальных и международных законов и нормативных документов, отраслевых стандартов, требований безопасности клиентов, стороннего анализа, отраслевой деятельности, опыта и конкретных требований к безопасности. Данный набор включает спецификации и стандарты для базовых уровней безопасности различных продуктов, безопасное кодирование, безопасное использование паролей, управление ключами безопасности, безопасное управление сеансом, сертификацию безопасности, тестирование безопасности, управление случаями нарушения безопасности и другое. Эти спецификации и стандарты охватывают все аспекты безопасности продукта.

Общие положения для обеспечения безопасности продукта

Общие положения для обеспечения безопасности продуктов — это план по обеспечению безопасности продуктов компании, который включает политику безопасности, цели, организацию, управление, процедуры и действия. Общие положения — это также общая концепция и проект обеспечения безопасности продуктов компании, который служит основой для всех документов более низкого уровня.

Документы по процедуре обеспечения безопасности продукта

Обеспечение безопасности продуктов входит в число основных процедур компании, а процедуры управления безопасностью разрабатываются в соответствии с требованиями. Например, процедуры реагирования на угрозы безопасности продукта разработаны в соответствии с особенностями оценки безопасности продукта и с порогом его чувствительности. Технические требования и шаблоны для базовых уровней безопасности продукта разработаны в соответствии с руководящими принципами изложенных требований безопасности продукта. Для каждой линейки продуктов предусмотрены особые базовые уровни безопасности продуктов, сбытовых цепочек и услуг. Также разработаны рекомендации по базовым уровням безопасности, сформулированы требования к тестированию безопасности продукта и шаблоны тестирования.

Базовые уровни безопасности

Продукты компании включают не только продукты собственной разработки, но и продукты сторонних производителей. Поскольку стандарты безопасности для различных продуктов и систем отличаются, для соответствия всем стандартам безопасности компании требуется проверка и дополнительная защита безопасности поставляемого продукта, чтобы оно соответствовало базовому уровню безопасности и все угрозы были устранены. Базовые уровни безопасности разработаны в соответствии с научно-исследовательской работой, закупкой продуктов сторонних производителей, работой и обслуживанием системы, усилением безопасности, управлением и тестированием безопасности. Перед массовым выпуском новых продуктов необходимо провести проверку безопасности. Только после выполнения всех требований, процесс массового производства будет запущен.

5.3 Процесс исследований и разработок в области безопасности HSDLC

Мы включили широкий спектр мероприятий по обеспечению безопасности в процесс исследований и разработок, включая проектирование, разработку и тестирование безопасности, сочетая широкие исследовательские и опытно-конструкторские разработки

Hikvision и лучшие методы обеспечения безопасности отрасли, такие как OpenSAMM, BSIMM, CSDL, MSDL и обратную связь с клиентами. Мы обеспечиваем эффективное осуществление мероприятий по обеспечению безопасности и предоставляем более безопасные продукты и решения для наших клиентов.

Определение концепции

На этапе теоретической проработки, в анализе требований безопасности продукта есть два важных момента:

Во-первых, базовый уровень безопасности продукта должен быть в списке обязательных требований. Он используется для выполнения основных требований по реализации целей безопасности или контроля рисков на допустимом уровне. Цели безопасности формируются на основе международных или национальных законов и правил, требований заказчика, промышленных стандартов и др., их цель - обеспечить соблюдение стандартов безопасности, защитить соединения и информацию пользователей от несанкционированного доступа, усилить контроль доступа к системе/защиту конфиденциальных данных и повысить защитную возможность системы.

Во-вторых, в будущем необходимо будет провести анализ угроз для этих продуктов в сценарии приложения, чтобы определить другие целевые требования безопасности. Анализ угроз используется для поиска источника, типа и точки атаки. Это выполняется, чтобы облегчить нам оценку рисков и обеспечить включение соответствующих мер в список требований к продукту.

Этап проектирования

На этапе проектирования, когда дизайн продукта становится более точным, угрозы, выявленные на этапе теоретической проработки, должны быть дополнительно

проанализированы и доработаны. На данном этапе осуществляется проектирование архитектуры безопасности продукта и оборудования обеспечения безопасности. Hikvision опирается на спецификации обеспечения безопасности OWASP и другие передовые отраслевые практики для разработки собственных спецификаций проектирования кибербезопасности.

Этап разработки

На этапе разработки выполняются кросс-обзоры в соответствии с защищенными спецификациями кодирования. Инструмент автоматического сканирования кодов Static Analysis Coverity используется для быстрого и точного сканирования дефектов в очень сложном коде. Это снижает риск возникновения проблем с защитой кода.

Этап проверки

Чтобы гарантировать безопасность продуктов Hikvision и предотвратить возникновение различных проблем безопасности на этапе исследований и разработок, мы проводим тесты безопасности на каждом этапе данного процесса:

- Во время тестирования безопасности продукта, Hikvision проводит тестирование безопасности протокола, используя специальные инструменты, как Defensics от Codenomicon и Peach Fuzzer, чтобы обеспечить безопасность сетевого протокола, устойчивость к угрозам и проверку надежности для всех продуктов, а также для поиска неизвестных уязвимостей;
- На этапе тестирования безопасности системы используются специальные инструменты сканирования уязвимостей, как Nessus Professional и NSFOCUS Система удаленной оценки защищенности (RSAS) для отслеживания CVE2 информации об уязвимостях. Это позволяет обнаруживать слабые места системы, включая уязвимости, проблемы конфигурации и уязвимости системы приложений;
- Основное антивирусное программное обеспечение, такое как Symantec или Avira, используется до выпуска продукта для обнаружения известных вирусов, троянских программ, бэкдоров и другого вредоносного программного обеспечения;
- Компания также регулярно приглашает известные охранные компании и публичные испытательные платформы для проведения испытаний на возможность проникновения в систему. Необходимость проведения как можно большего количества испытаний на возможность проникновения обусловлена желанием минимизировать бизнес-риски и держать угрозы безопасности под контролем.

[2] CVE: Самая авторитетная база данных уязвимостей в мире: общие уязвимости и риски http://cve.mitre.org

Управления конфигурацией

Управление конфигурацией является важной задачей, гарантирующей целостность, согласованность и отслеживаемость продукта. Управление конфигурацией содержит множество процессов, включая стратегию и планирование, идентификацию элементов конфигурации, управление изменениями элементов конфигурации, отслеживание состояния конфигурации, отчетность о конфигурации, аудит конфигурации, управление сборкой, управление выпуском, стороннее программное обеспечение и управление компонентами с открытым исходным кодом, а также управление репозиториями и многое другое. Управление конфигурацией обеспечивает целостность доставки продуктов Hikvision, включая стороннее программное обеспечение и компоненты с открытым исходным кодом в продукте. Процесс управления конфигурацией Hikvision является неотъемлемой частью всего процесса разработки продуктов. Вышеупомянутые действия по управлению конфигурацией проводятся на каждом этапе процесса разработки для обеспечения отслеживаемости продуктов. Они являются ключевыми элементами, обеспечивающими безопасность.

Спецификации управления сборкой проекта

Спецификации управления сборкой включают в себя управление ресурсами, а также управление и оптимизацию процесса. Распределение обязанностей важная составляющая управления конфигурацией. Выполняемые действия, роли и обязанности должны быть четко определены в спецификациях в процессе сборки проекта. В процесс разработки должны быть интегрированы различные этапы разработки продукта и указан жизненный цикл.

Центр сбора и компиляции

Для обеспечения точного воспроизведения процесса сборки, Hikvision создала центр сборки, где все аппаратные средства, инструменты сборки, стороннее программное обеспечение, источники данных и операционные системы отвечают строгим стандартам и требованиям. Центр сборки является интегрированным решением для создания и сборки продукта и предоставляет облачный сервис для поддержки деятельности по созданию программного обеспечения во время процесса разработки.

Стандартизация процесса сборки обеспечивается за счет централизованного управления инструментами, стандартизации сценариев сборки, сборки в один клик, автоматической установки среды сборки, полностью автоматизированного процесса сборки, загрузки исходного кода, упаковки, статического анализа кода, автоматического модульного

тестирования и тестирования системы. Это гарантирует воспроизводимость, отслеживаемость и восстановление процесса сборки.

Центр сборки также выполняет две дополнительные функции: Проверка наличия вирусов и цифровую подпись. Центр проверки наличия вирусов одновременно запускает восемь антивирусных программ и интегрируется в процесс тестирования. В целях безопасности центр цифровой подписи использует исходный код, скомпилированный с ключом из базы данных ключей. Hikvision выдает разрешения и подписывает документы на выполнение необходимых действий для отслеживания всего процесса.

Управление компонентами

Продукты Hikvision собственного производства управляются через компонентную систему. В компонентной системе есть две концепции интеграции: CCI (непрерывная интеграция компонентов) и PCI (непрерывная интеграция продуктов). Инженеры непрерывной интеграции используют разные точки входа для создания CCI и PCI, внедрения компонентов, доставки и автоматической интеграции.

Управление инструментальным и сторонним компонентом

Hikvision закупает множество сторонних программ и программ с открытым исходным кодом по всему мира. Сторонние компоненты остаются сложной задачей для всех компаний. Вот почему Hikvision серьезно относится к следующим вопросам:

- Надежность исходного кода или источника компонента
- Известные уязвимости, которые все еще существуют
- Авторизованный контроль соответствия
- Обработка новых уязвимостей
- Жизненные циклы сторонних компонентов
- Включение сторонних компонентов в жизненный цикл продукта Hikvision

Hikvision нужно не только учитывать сторонние компоненты, но и гарантировать, что соответствующие компоненты, необходимые для скомпилированных исходных кодов или для сторонних компонентов, управляются надлежащим образом. Hikvision разработала «Спецификации управления сторонними компонентами и исходными кодами», чтобы

гарантировать, что стороннее программное обеспечение соответствует нашим требованиям и может эффективно управляться.

Подготовка сотрудников

Сотрудники являются фронтом защиты любой компании, поскольку они имеют доступ к потенциально конфиденциальной информации. Поэтому необходима обязательная подготовка по вопросам сетевой и информационной безопасности, чтобы сотрудники могли защитить интересы клиентов и предотвратить проблемы контроля доступа, проблемы безопасности связи и проблемы защиты конфиденциальных данных. Для управления сотрудниками, Hikvision разработала «Стандарты службы технической поддержки» в соответствии с ISO27001 и другими стандартами. Эти спецификации включают кодексы поведения, личную безопасность, защиту информации и прочее.

Hikvision строго управляет доступом сотрудников к сети. Сотрудники подписывают письменные обязательства, в которых подробно прописаны их роли, обязанности и юридические риски. Наши сотрудники обязаны пройти обучение по обеспечению кибербезопасности и сдать соответствующие тесты.

Экстренное реагирование

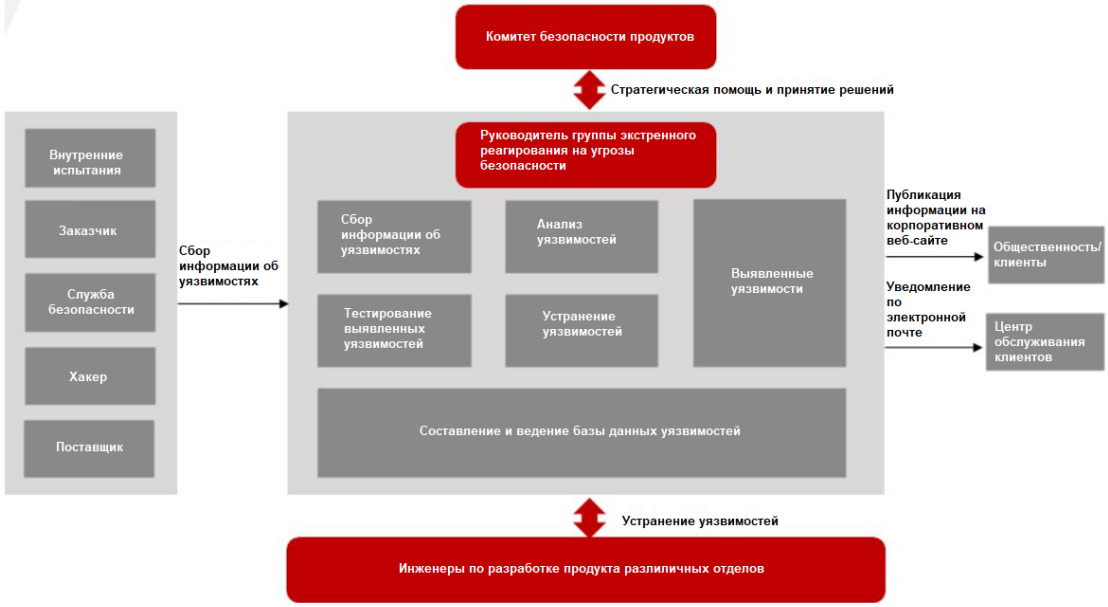
Hikvision создала «Центр экстренного реагирования на угрозы безопасности» (SRC), который отвечает за принятие, обработку, выявление и решение проблем уязвимости, связанных с безопасностью продуктов и решений Hikvision. В его обязанности входят:

- Реагирование и принятие мер по устранению случаев нарушений безопасности, заявленных клиентами;
- Реагирование и принятие мер по вопросам обеспечения безопасности, заявленных промышленными ассоциациями;
- Разработка стратегии управления случаями нарушения информационной безопасности компании и процедур по урегулированию данных инцидентов;
- Анализ уязвимостей и исправлений, анонсируемых и выпущенных поставщиками системного программного обеспечения и профессиональными компаниями безопасности.

Компания также определяет обязанности каждого отдела и процедуры управления случаями нарушений безопасности продукта для обеспечения качества и эффективности управления. В сферу ответственности центра экстренного реагирования на угрозы безопасности входит обеспечение безопасности продукта во время предпродажных,

торговых и послепродажных процессов, безопасное взаимодействие клиентов с продуктами, сотрудничество с организациями обеспечения безопасности, управление экстренным реагированием на угрозы безопасности, предоставление информации о безопасности, соответствие требованиям информационной безопасности и нормативно-правовое соответствие.

Предусмотрены четкие положения для эффективного урегулирования вопросов безопасности. Например, первоначальное подтверждение случая нарушения безопасности должно быть получено менее чем за 24 часа, а уязвимости высокого уровня риска должны быть исправлены в течение 30 дней.



Управление уязвимостями

Hikvision следует за ISO/IEC 30111, ISO/IEC 29147 и другими спецификациями, чтобы установить порядок обработки и предупреждения об уязвимостях безопасности продукта. Они включают в себя четыре этапа:

- Изучение уязвимостей и сбор данных: Мы получаем информацию об уязвимостях от клиентов, внешней сертификации, инженеров-исследователей проблем безопасности и специализированных веб-сайтов безопасности. Одновременно с этим наши штатные команды постоянно ведут поиск потенциальных угроз безопасности. Мы поощряем политику ответственного раскрытия нахождения подобных угроз, то есть, если внешний агент обнаруживает уязвимость, он должен предоставить производителю достаточное количество времени для обработки и решения проблемы до ее публичного раскрытия.
- Оценка, анализ и проверка уязвимости: При наличии предполагаемых или подтвержденных уязвимостей группа HSRC будет работать с лицом,

ответственным за продукт, для быстрого выполнения практических и связанных с ними оценок рисков.

- Отслеживание и решение: После подтверждения уязвимости, HSRC немедленно отправляет полученную информацию лицу, обнаружившему эту уязвимость, и активно отслеживает процесс и обратную связь. Они также изучают данную уязвимость, чтобы гарантировать устранение проблемы для всех соответствующих версий и моделей продукта.

Hikvision стремится защищать конфиденциальность клиентов и информации об уязвимостях на каждом этапе процесса. Если информация о наличии уязвимости попадет в руки злоумышленников, это чревато серьезными последствиями. Все стороны должны защищать конфиденциальность этой информации.

Группа экстренного реагирования на угрозы безопасности Hikvision активно участвует в отраслевой и общественной деятельности и установила долгосрочные отношения с CERT, платформами раскрытия уязвимостей, клиентскими SRC и другими поставщиками, инженерами-исследователями проблем безопасности и сторонними координационными организациями.

5.4 Безопасность сбытовых цепочек

Чтобы снизить риски и обеспечить целостность аппаратного и программного обеспечения, Hikvision применяет меры по борьбе с несанкционированным вмешательством, внедрением и заменой на ключевых этапах производства продукта, например, программирование/калибровка, загрузка программного обеспечения и производственные испытания. Это помогает предотвратить несанкционированную замену оборудования, вмешательство или внедрение программного обеспечения, вирусы и другие риски. Система управления данными продуктами принимает программное обеспечение, необходимое для устройства. Перед установкой программного обеспечения в устройства проводится несколько проверок целостности.
Сеть, используемая в цепочке сбыта для записи и загрузки программного обеспечения, сборки и тестирования, должна быть изолирована от ИТ-системы офиса компании и интернета.

Hikvision использует автоматическое тестирование для снижения рисков и угроз безопасности, вызванных человеческим фактором.

Hikvision внедрила безопасный и строгий процесс технического обслуживания для обеспечения высокого качества продуктов. Данные всего процесса записываются в

производственную систему и систему штрихового кодирования Hikvision. Для обеспечения отслеживаемости продукции ведется детальный учет и журнал исследований и разработок, закупок, производства (программирование, загрузка программного обеспечения, сборка, тестирование и др.), складских и логистических процессов.

5.5 Соответствие требованиям безопасности

Международная правовая среда постоянно развивается, а требования, касающиеся контроля за рынком, постоянно ужесточаются. В частности, в области законодательства о кибербезопасности многие страны и регионы в последние годы приняли соответствующие законы и положения, например, ЕС (Общие положения о защите данных). Обеспечение безопасности стало серьезной проблемой для поставщиков интернета вещей. Hikvision стремится создать эффективные системы безопасности внутреннего контроля, которые следуют и соответствуют требованиям различных отраслей, областей и стран, а также завершают свою собственную основу соответствия в своих системных процессах и контрольных мероприятиях.

В Hikvision работает команда юристов для изучения, выявления и отслеживания законов и положений, применимых к компании. В то же время, Hikvision активно устанавливает долгосрочное сотрудничество с опытными и престижными юридическими фирмами как внутри страны, так и за рубежом. Мы создали специальную группу для интеграции применимых законов и правил в деятельность Hikvision, выявления и контроля юридических рисков, связанных с разработкой, производством, поставкой и обслуживанием продукции, а также для предоставления консультаций и поддержки по вопросам соответствия. По мере принятия новых законов и положений, мы проводим специальное обучение для повышения информированности о соблюдении требований законодательства для новых сотрудников, менеджеров среднего и высокого уровня, а также руководящих сотрудников для обеспечения кибербезопасности.

Как отмечается в «Заявлении о создании системы обеспечения кибербезопасности для продуктов видеонаблюдения», Hikvision стремится улучшить и обеспечить полную безопасность системы видеонаблюдения. В дополнение к соблюдению применимых государственных и местных правил безопасности, а также ссылаясь на передовой опыт в отрасли, компания создала полную, устойчивую и надежную систему безопасности, которая включает в себя политику компании, организацию, процесс, технологию и спецификации.

Hikvision поддерживает основные международные стандарты и активно участвует в их разработке. Уже к концу 2016 года Hikvision присоединилась к десяткам отечественных и

международных организаций по промышленным стандартам, таким как TC260[3], TC100[4], CSA[5] и ONVIF[6]. Hikvision участвовала в разработке промышленных стандартов безопасности, которые открывают ключевые технологии безопасности для работы с другими отраслевыми экспертами и национальными организациями по стандартизации над улучшением стандартов обеспечения безопасности интернета вещей.

Hikvision также сотрудничает с независимыми сторонними организациями по оценке для проведения честных оценок безопасности и сертификации.

3 http://www.tc260.org.cn/
4 http://www.tc100.org.cn/
5 Федерация информационной облачной безопасности: https://cloudsecurityalliance.org/
6 Открытый форум по интерфейсу сетевого видео: https://www.onvif.org/

ISO/IEC 9001

ISO/IEC 9001: На данный момент эта система 2008 года одна из лучших систем контроля качества в мире. Данная система охватывает продукты или услуги компании и включает руководящие принципы и спецификации. Обеспечение соответствия продуктов и услуг компании всей структуре управления качеством имеет основополагающее значение для ее роста и развития.

ISO/IEC 27001

ISO/IEC 27001: Система управления информационной безопасностью 2013 года является самым авторитетным, строгим и широко распространенным стандартом сертификации систем для обеспечения информационной безопасности в мире. Прохождение данной сертификации означает, что компания уже создала научно обоснованную систему управления информационной безопасностью. Вместе с единой стратегией развития компании и управлением информационной безопасностью гарантируется, что риски информационной безопасности находятся под контролем и в случае угрозы будут приняты соответствующие меры. Ezviz Cloud - первый поставщик облачных услуг для домашнего использования в Китае, получивший сертификат ISO/IEC 27001:2013. Используя эти меры управления информационной безопасностью и механизмы защиты информационных активов, а также следуя модели на основе цикла PDCA, мы намерены обеспечивать информационную безопасность и предоставлять надежные информационные услуги и соответствующие гарантии безопасности.

Сертификация зрелости программного обеспечения CMMI5

Интегрированная модель зрелости процессов программного обеспечения (CMMI) — это система управления процессами на уровне предприятия, используемая ведущими мировыми компаниями. Она признана авторитетным стандартом оценки продуктов и услуг предприятий, а также служит методом улучшения процессов, который может помочь компаниям достичь коммерческих целей, обеспечить качество, гарантировать поставки и повысить уровень удовлетворенности клиентов. Существует пять уровней зрелости, которые компании указывают в спецификациях программного обеспечения CMMI. 5 уровень является высшим уровнем.

Ступенчатая защита информационной безопасности

Сертификация ступенчатой защиты информационной безопасности — это базовая система, используемая для защиты информационной безопасности в Китае. Она служит основой для защиты достижений в области информирования и поддержания национальной информационной безопасности. Для оценки уровней защиты безопасности информационных систем используется пятибалльная шкала оценок с максимальной оценкой пять.

Данная шкала основана на значимости системы с точки зрения национальной безопасности, национальной экономики и общества в целом; она также учитывает потенциальный вред национальной безопасности, социальному порядку, общественному благосостоянию и потенциальную степень ущерба юридическим правам и интересам граждан, юридических лиц или других организаций. 5 уровень является высшим уровнем безопасности.

В соответствии с установленными положениями в «Административных мерах по обеспечению ступенчатой защиты информационной безопасности», внутренние информационные системы EZVIZ Cloud и Hikvision прошли 3 уровень обеспечения защиты информационной безопасности и соответствуют техническим гарантиям и требованиям управления национальными стандартами информационной безопасности. Они также создали собственные долгосрочные механизмы, гарантирующие продолжение работы в области безопасности в будущем.

Аудит SOC

Отчеты по системному и организационному управлению (SOC) предоставляются профессиональными сторонними бухгалтерскими фирмами в соответствии с установленными стандартами, выпущенными департаментом внутреннего контроля американского института дипломированных общественных бухгалтеров (AICPA).

Отчет SOC 2 ссылается на аудиторские стандарты AICPA раздела AT-C 105, 205 и раздела TSP 100 2017 в SSAE № 18 и представляет собой отчет, который фокусируется на проектах контроля безопасности, доступности и конфиденциальности для систем облачных сервисов.

Отчет SOC 2: Пользовательские облачные организации, независимые аудиторы, контролирующие организации, акционеры компании и другие заинтересованные стороны могут использовать отчет SOC 2, чтобы оценить механизмы внутреннего

управления поставщика облачных решений (включая безопасность, доступность, целостность процесса, конфиденциальность и др.).

EZVIZ Cloud проходит аудит SOC2 в отношении безопасности данных третьих сторон.

5.6 Управление персоналом

Hikvision стремится создать общекорпоративную культуру знаний и информированности о безопасности. Для этого проводятся мероприятия по информированию и просвещению в области кибербезопасности, и начата образовательная деятельность и обучение на основе различных знаний в области кибербезопасности и навыков, требуемых различными службами. Hikvision также планирует проведение тренингов по кибербезопасности, ориентированных на индустрию видеонаблюдения. Hikvision будет публиковать периодические издания, посвященные вопросам кибербезопасности на своей внутренней платформе, а также будет использовать специализированные плакаты, брошюры и другие методы распространения информации о кибербезопасности.

Hikvision выделила ключевые должности в отношении кибербезопасности для каждой области обслуживания и для обеспечения безопасности продуктов.

Следующие требования применяются к руководящим сотрудникам:

- Прежде чем сотрудник вступит в должность, он должен пройти соответствующую проверку, подтверждающую наличие необходимого опыт и знаний, которые отвечают потребностям клиентов.
- Сотрудник должен пройти квалификационную подготовку, которая повысит уровень информированности и улучшит соответствующие навыки. Изучается поведение и действия руководящих сотрудников, чтобы выяснить, имели ли место какие-либо нарушения.
- Когда сотрудник покидает свою должность, сотрудники отдела кадров и безопасности удаляют или изменяют его разрешения и учетные записи в соответствии с рассмотрением ухода с ранее занимаемой должности. При необходимости активы сотрудника также будут удалены. Рассмотрение ухода с ранее занимаемой должности также относится к переводам и увольнениям.

Чтобы улучшить технические знания наших сотрудников для эффективного выполнения ими своих обязанностей, Hikvision разработала специализированный план усовершенствования систем биобезопасности и базовый курс обучения, который улучшит возможности сотрудников в области обеспечения кибербезопасности.

Компания стремится улучшить знания и навыки сотрудников в отношении кибербезопасности и поощряет самообучение. Запустив широкий спектр специализированных тренингов, которые следуют практическим рекомендациям, Hikvision надеется улучшить знания в области кибербезопасности и навыки руководящих сотрудников. Например, Hikvision проводит семинары, форумы и тематические исследования, посвященные кибербезопасности.

Наши сотрудники обязаны взять на себя техническую и юридическую ответственность за результаты своих действий. Наши сотрудники знают, что случаи нарушения кибербезопасности могут существенно повлиять на клиентов, компанию и другой персонал, поэтому Hikvision привлекает сотрудников к ответственности за свои действия и результаты своих действий, будь то намеренные или нет.

5.7 Обмен и сотрудничество

- Компания EY из Великобритании была приглашена оценить общую практику информационной безопасности Hikvision и помочь улучшить систему кибербезопасности компании;

- Отдел безопасности Cisco был приглашен для тестирования системы управления безопасностью исследований и разработок компании, чтобы обеспечить соответствие системы безопасности исследований и разработок Hikvision компаниям мирового класса;

- Hikvision расширила обмен и сотрудничество с отечественными и международными охранными компаниями, такими как Synopsys и IBM, для повышения безопасности
продуктов компании.

- Hikvision пригласила известные отечественные и международные группы тестирования безопасности для проведения испытаний на возможность проникновения в систему продуктов компании. Минимизация рисков гарантирует их нахождение под нашим контролем;

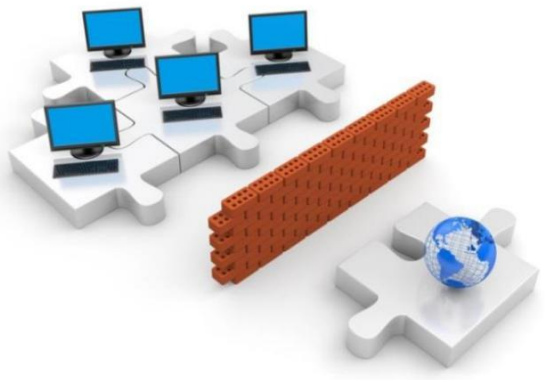
- Hikvision пригласила EY из Великобритании для оценки SOC2 и сертификации продукции компании, чтобы обеспечить безопасность и конфиденциальность облачных продуктов;

- Hikvision пригласила известных отечественных и международных экспертов в области обеспечения безопасности, для проведения занятий для сотрудников отдела исследований и разработок Hikvision, чтобы улучшить стандарты безопасности;

- Ежегодно лаборатория сетевой и информационной безопасности проводит семинары с клиентами по обеспечению безопасности продуктов. Цель данных семинаров - обмен знаниями о правилах реагирования в случае нарушения безопасности и требованиях безопасности, информирование клиентов о новых тактиках в области обеспечения безопасности и лучшее изучение требований клиентов;

- Компания также запустила «Программу вознаграждения белых хакеров», чтобы побудить отечественных и международных белых хакеров протестировать информационную безопасность Hikvision, и сообщить об ошибках безопасности, если такие имеются, чтобы Hikvision могла продолжать улучшать безопасность продукта.

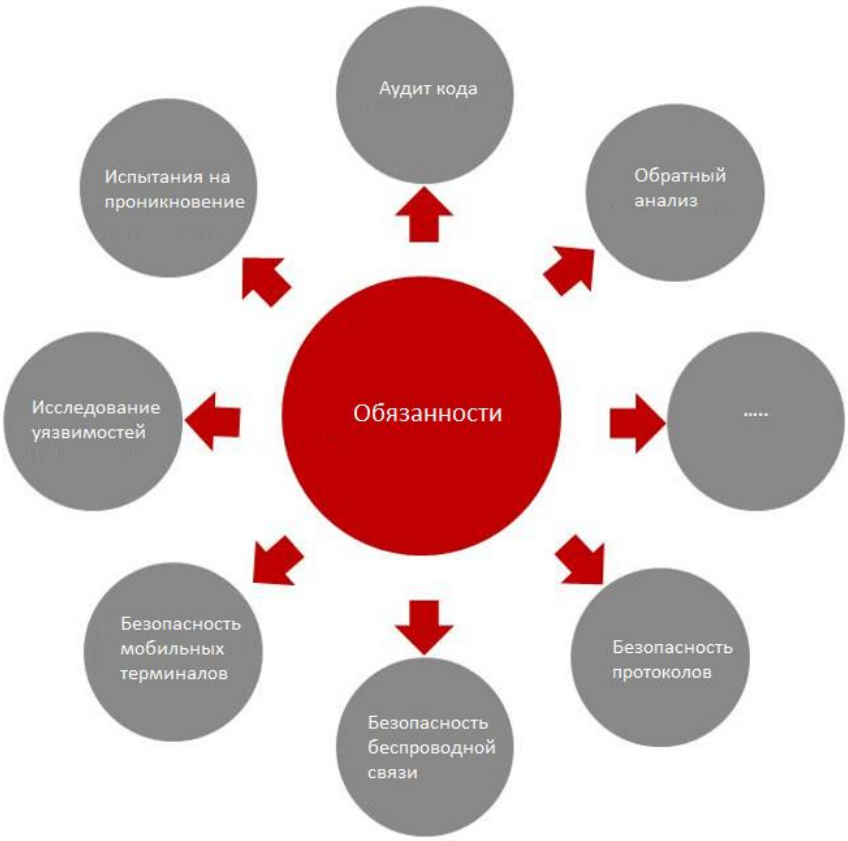
Hikvision также занимается внешним обменом и сотрудничеством и принимает отзывы от заинтересованных сторон. Hikvision применяет передовые технологии и опыт управления от других лидеров индустрии видеонаблюдения и постоянно улучшает возможности информационной безопасности компании.



6. Исследование безопасности продукта

6.1 Уязвимость при эксплуатации

Лаборатория сетевой и информационной безопасности специализируется на исследованиях и практиках в области безопасности интернета вещей, включая проведение испытаний на проникновение, аудит кода, обратный анализ, исследование уязвимостей, безопасность мобильных терминалов, безопасность протоколов и безопасность беспроводной связи. Ее цель - обнаружить и исправить проблемы безопасности до того, как их обнаружат хакеры.



Обязанности:

Обнаружение уязвимости встроенного устройства: Объединение опыта Hikvision со встроенной безопасностью устройства и использованием обратного инжиниринга прошивки, отладки последовательного порта, статического анализа и других методов для обнаружения уязвимостей.

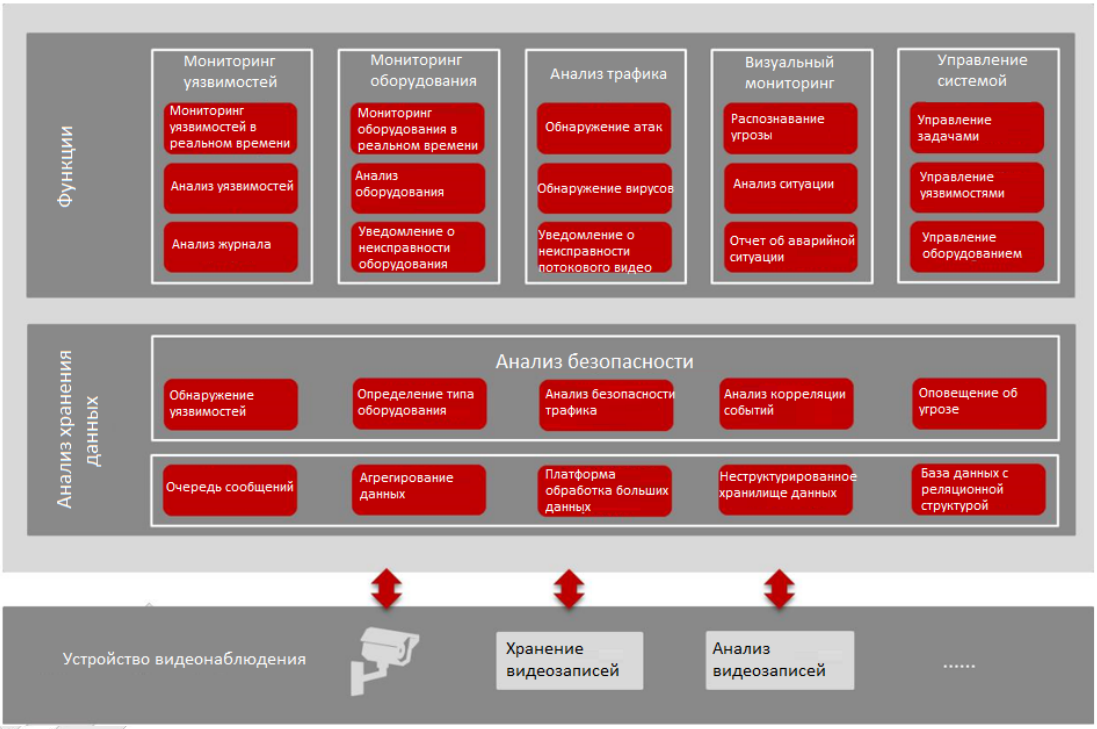
Обнаружение уязвимости протокола: Интеграция как коммерческих, так и собственных инструментов тестирования для обнаружения уязвимости в основных протоколах безопасности.

Исследование безопасности беспроводной сети: Группа специалистов с беспроводной средой тестирования безопасности для аппаратного обеспечения может имитировать несанкционированное извлечение информации, атаки с повторным навязыванием сообщения, спуфинг-атаки и перехват сеанса.

Веб-безопасность: Для проведения испытаний на возможность проникновения в систему используются инструменты системного интегратора, инструменты веб-тестирования собственной разработки, поисковые роботы и пассивные прокси-технологии. Эти инструменты позволяют обнаружить внедрение SQL, XSS межсайтовый скриптинг, утечку конфиденциальной информации и прочие проблемы веб-безопасности.

6.2 Осведомленность об угрозах безопасности

Огромная сетевая система интернета вещей, сформированная устройствами, сетью, платформами и приложениями, требует многоуровневой защиты и облачных, интеллектуальных возможностей анализа безопасности больших данных. Реализация проекта умной ситуационной осведомленности, визуализации и обеспечения безопасности всех сетей станет новой тенденцией интернета вещей. Безопасность ситуационной осведомленности относится к получению, пониманию и отображению важных элементов безопасности, которые могут привести к изменениям состояния системы в крупномасштабных системных средах.



Оценка уязвимости

Оценка уязвимости указывает возможность системы ситуационной осведомленности о безопасности эффективно обнаруживать угрозы безопасности. Система ситуационной осведомленности безопасности Hikvision включает в себя основную базу данных уязвимостей и может обнаруживать известные уязвимости. Кроме того, у Hikvision есть команда исследователей уязвимостей, которые постоянно отслеживают объявления о безопасности других известных организаций и производителей и постоянно анализируют, выявляют и проверяют различные типы новых уязвимостей. Благодаря постоянной работе профессиональной команды исследователей уязвимостей Hikvision, угрозы безопасности выявляются своевременно и меры по их устранению принимаются незамедлительно.

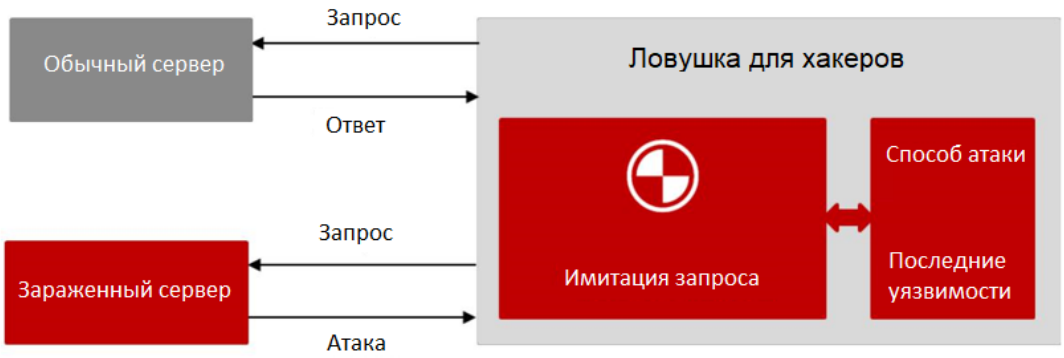
Кроме того, видеосистема ситуационной осведомленности о безопасности Hikvision может также обнаруживать угрозы безопасности и выполнять корреляционный анализ информации об активах. Установив модель анализа больших данных для динамического анализа накопленных данных и данных в реальном времени, можно точно и эффективно определить статус безопасности и направление развития всей сети. Затем можно обеспечить разумное усиление безопасности в сетевых ресурсах видеонаблюдения для обеспечения безопасности системы наблюдения.

Визуализация безопасности

Визуализация может напрямую помочь в отображении характеристик данных и облегчить для читателя их интерпретацию. Поэтому для анализа больших данных (глубокой проверки пакетов, анализа трафика) требуется дисплей.

Когда система атакуется, требуется быстрая идентификация источника и канала атаки, а также быстрое принятие ответных мер. Эффективные ответные меры должны быть предприняты до того, как данная атака нанесет дополнительный урон. После нападения необходимо быстро принять меры для предотвращения повторения подобных атак.

6.3 Система-ловушка для хакеров



Ловушка для хакеров - это, по сути, механизм для обмана нападающих. Используются подставные хосты, сетевые службы или информация, чтобы заманить злоумышленников. Затем поведение атакующего фиксируется и анализируется, чтобы можно было идентифицировать его инструменты, методы и намерения.

Ловушки для хакеров можно классифицировать как высоко-взаимодействующие или низко-взаимодействующие в зависимости от принципа их реализации. Высоко-взаимодействующие обычно реализуются с использованием реальной операционной системы или программного приложения. Низко-взаимодействующие имитируют ответы протокола обычного сервера.

Операционная система высоко-взаимодействующей ловушки способна обнаружить различные типы методов вторжения, такие как использование уязвимостей и слабые пароли. Также можно выявить образцы атаки. Низко-взаимодействующие ловушки могут захватывать поведение атаки, такое как сканирование сети и взлом пароля. В настоящее время Hikvision в основном использует высоко-взаимодействующие ловушки, такие как Conpot, Mirai, Struts2 и другие.

7. Обязательства в отношении обеспечения безопасности

Hikvision стремится использовать передовые технологии обеспечения конфиденциальности и безопасности для защиты личной информации клиентов и защиты пользовательских данных.

Hikvision использует интегрированную инфраструктуру безопасности для всей экосистемы видеонаблюдения интернета вещей. Hikvision также имеет профессиональную команду обеспечения безопасности, отвечающую за поддержку всех продуктов Hikvision. Эта команда обеспечивает проверку безопасности и тестирование выпущенных и разрабатываемых продуктов. Команда обеспечения безопасности также проводит тренинги и активно отслеживает новые проблемы безопасности и отчеты об угрозах. Чтобы узнать, как сообщить о проблемах Hikvision и как подписаться на рассылку уведомлений об обеспечении безопасности, пройдите: http://overseas.hikvision.com/en/about_437.html.

Hikvision

Cybersecurity White Paper

See Far, Go Further

HIKVISION

Hikvision Digital Technology Co., Ltd.

No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China