БЕЛЫЕ ХАКЕРЫ AXIS COMMUNICATIONS

«Мир изменился… Многое из того, что было, ушло. Мир никогда не будет прежним».

Братство кольца

Более 20 лет назад, в 1996 году Axis Communications выпустила первое в мире сетевое устройство в видеонаблюдении – сетевую камеру Axis Net Eye 200. В том еще полностью «аналоговом» мире видеонаблюдения очень многим было непонятно, зачем все это нужно и как верить в будущее таких изделий.

Не все, что подключается к глобальной сети, имеет достаточный уровень защищенности, делая работу хакера еще проще и «дешевле». Axis Communications представляет инструмент защиты систем видеонаблюдения – программный комплекс **AXIS Device Manager**.

Причины незащищенности могут быть самые разные: во многих случаях это происходит из-за пренебрежения базовыми методами защиты системным интегратором или конечным потребителем, в других же – наличие уязвимостей в самих устройствах, которые затем становятся известны публично. Поиском таких уязвимостей могут заниматься не только сами злоумышленники-хакеры (black hat hackers), но, в том числе, и специалисты по информационной и кибербезопасности, целью которых является получение знаний и применение их для повышения защищенности устройств. Таких «этичных» исследователей называют белыми хакерами (white hat hackers).

Иногда обнаружить уязвимость бывает достаточно сложно, и весь процесс тянет на научную работу. А иногда все настолько просто, что похоже это не иначе как на невнимание со стороны производителей устройств к таким же базовым вещам или их грубое нарушение.

«Здоровая» киберсреда складывается из трех важных составляющих: используемые технологии, процессы и пользователи. Разработанная Axis Communications программа включает три уровня обеспечения защиты.

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ

Процесс усиления защиты или так называемый «харденинг» состоит из опубликованного документа AXIS Hardening Guide, покрывающего интересы и потребности предприятий разного масштаба с конкретными шагами и рекомендациями по усилению защиты.

Кроме того, «харденинг» включает программные инструменты для эффективного управления. Один из них – AXIS Device Manager – инструмент для управления локальными устройствами. В мире, где угрозы безопасности становятся все более распространенными, AXIS Device Manager – это инструмент для активной защиты устройств и сетей. Программное обеспечение подходит для управления сетевыми камерами Axis, блоков доступа и аудиоустройств. Помимо управления пользователями, обновления встроенного ПО и мониторинга работоспособности, последние версии включают и управление сертификатами 802.1x. Статистика загрузки скачиваний данного ПО – более 6000 раз ежемесячно.

Программное обеспечение предлагает широкий спектр функций управления устройствами, в том числе:

- Автоматически назначать IP-адреса.
- Установка, настройка, замена или обновление отдельного устройства.
- Копирование конфигураций между тысячами устройств.
- Подключение к нескольким серверам/системам.
- Точки восстановления и заводские настройки по умолчанию.
- Обновление прошивки устройства.
- Управление и обновление учетных записей пользователей и паролей.
- Установка и восстановление сертификатов HTTPS и IEEE 802.1x.

Новый диспетчер устройств AXIS обеспечивает более высокий уровень безопасности, позволяя централизованное управление учетными записями, паролями и сертификатами. ПО позволяет установщикам и системным администраторам легко управлять и внедрять более важные функции управления безопасностью.

«Если вы имеете доступ ко всем устройствам в своей сети, установите их эффективно, адаптируйте и защитите, это избавит вас от траты огромного количества времени и усилий. AXIS Device Manager является посредником для доступа ко всем устройствам Axis на любом этапе их жизненного цикла, что позволяет им вносить необходимые изменения в свои настройки», – прокомментировал Ола Леннартсон, глобальный менеджер по продуктам Axis Communications для системного управления. «В быстром темпе текущего мира каждое статическое устройство или сеть не только устарели, но потенциально более восприимчивы к различным киберугрозам. Поэтому для наших клиентов важно убедиться, что они могут использовать инструмент, который позволяет им легко, быстро и надежно управлять всеми устройствами в своей сети. Этот инструмент является диспетчером устройств AXIS».

УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ

В первую очередь, включает в себя более чем 30-летний опыт использования лучших практик в обеспечении безопасности сетевых устройств. Одна из таких практик – это комплексное исследование программного кода перед выпуском продукта на рынок. К данному разделу относится и процесс выявления и скорого устранения слабых мест во встроенном ПО, а также открытое взаимодействие со всеми участниками канала продаж в случае обнаружения уязвимостей. Своевременность и открытость производителя могут сыграть решающую роль в снижении рисков на объектах конечных потребителей.

ОБУЧЕНИЕ И СОТРУДНИЧЕСТВО

Ключевой элемент в кибербезопасности – это знания, понимание проблем, рисков и возможного ущерба. Способность трезво оценить и предпринять соответствующие меры. Axis Communications старается делиться знаниями и накопленным опытом настолько, насколько это возможно, подчеркивая актуальность проблемы, привлекая к ней большее внимание и интерес, повышать «зрелость» рынка, подготавливая к возможной встрече с новыми угрозами. Компания Axis меняет мир, делая его лучше и защищеннее.

ООО «АКСИС КОММУНИКЕЙШНС»
125284, Москва, Ленинградский пр., д. 31 А, стр. 1, этаж 16
тел./факс: (495) 940-6682
www.axis.com