ТЕХНИЧЕСКИЙ ОБЗОР

Видеоданные как доказательство

Обеспечение целостности видеоданных с помощью AXIS Camera Station

Июль 2021

AXIS COMMUNICATIONS

Содержание

1 Краткая информация

Для доказательств требуются высококачественные, заслуживающие доверия и неизмененные видеозаписи. Рекомендуемые методики работы с видеоданными, используемыми в качестве доказательств, с помощью AXIS Camera Station:

- Правильно проектируйте, конфигурируйте и проверяйте вашу систему, чтобы получить изображение, записи и защиту необходимого уровня
- Выполняйте регулярное обслуживание
- Работа с доказательствами по установленным процедурам

2 Введение

Видео, записанное с помощью системы видеонаблюдения, практически идеально подходит для использования в качестве доказательства в суде. События, снятые "на пленку", невозможно отрицать – но так ли это? Да, суд, вероятно, примет к рассмотрению видеозаписи, если они хорошего качества, вызывают доверие и не подвергались изменениям.

Но бывают случаи, когда ценность видео как доказательства снижается в результате непредумышленных действий. Например, видеозаписи с разрывами по времени, на которых люди или автомобили неожиданно исчезают или "прыгают" с места на место, могут быть признаны не заслуживающими доверия и не подходящими в качестве доказательств. Видеозапись может быть поставлена под вопрос, если она содержит недостоверные метаданные, например, отметки времени или MAC-адрес камеры. Любое подозрение, что видео могло быть изменено, удалено или модифицировано, снижает доверие к источнику видео.

В частности, здесь описывается роль ПО для управления видео (VMS) AXIS Camera Station в цепочке формирования доказательств, а также роль владельца видео. В частности, здесь описывается роль

ПО для управления видео (VMS) AXIS Camera Station в цепочке формирования доказательств, а также роль владельца видео.

Figure 1. Правильно развернутое и поддерживаемое видеонаблюдение, установленное в ключевых точках, может стать источником ценных доказательств

3 Рекомендованные методики работы с видеоданными, используемыми в качестве доказательств

Компаниям и организациям, использующим видеонаблюдение, необходимы процессы и процедуры, определяющие правила обращения с видеоданными и их хранения. Чтобы в полной готовности встретить ситуацию, когда какая-либо из ваших камер зафиксирует инцидент, вам необходимо позаботиться о том, чтобы видео не было перезаписано, изменено или украдено. Должна быть возможность безопасно экспортировать видеозапись в безопасное хранилище и передать его органам правопорядка.

Но получение высококачественного видео для использования в качестве доказательства - это процесс, который начинается с целенаправленного проектирования вашей системы видеонаблюдения. Также очень важно поддерживать актуальность программного обеспечения и прошивок вашей системы и следить за всеми отклонениями. В этой главе рассказывается о том, какие шаги включает в себя этот процесс и как их можно выполнять с помощью AXIS Camera Station и соответствующего инструментария AXIS Camera Station Integrator Suite.

Если видеозаписи вашей системы видеонаблюдения получены с соблюдением этих принципов проектирования и обслуживания системы и управления инцидентами, они будут соответствовать

действующим требованиям в области кибербезопасности и, с большой вероятностью, будут представлять ценность в качестве доказательств, если возникнет такая необходимость.

Figure 2. ПО AXIS Camera Station облегчает настройку системы видеонаблюдения, ее повседневную эксплуатацию и стратегическое управление ею

3.1 Правильно проектируйте систему

Проектирование системы видеонаблюдения требует тщательности. Вам необходимо выбрать оборудование, соответствующее вашим потребностям, и настроить его так, чтобы оно давало изображение требуемого качества, записывало его так, как нужно вам, и было надежно защищено. AXIS Site Designer существенно облегчает решение этих задач.

3.1.1 Надлежащее качество изображения

Качество изображения зависит от конкретной камеры и ее размещения. Разрешение изображения, точнее говоря, плотность пикселей в зоне наблюдения, можно рассчитать, зная модель камеры, объектив, угол и расстояние от камеры до сцены. Чтобы достичь адекватной плотности пикселей для распознавания лиц в зоне наблюдения, может потребоваться установить больше камер или использовать камеры с более высоким разрешением. Проанализируйте зону обзора, требования к освещению и другие параметры для конкретных камер на вашем объекте. Такой анализ можно удобно выполнить в AXIS Site Designer.

3.1.2 Надлежащее качество записи

Для записи видео необходимо использовать высокоэффективные проверенные аппаратные средства с резервированием. Для повышения надежности системы AXIS Camera Station поддерживает переключение в случае сбоя на локальную запись с сохранением данных на установленную в камере

SD-карту. В случае использования средств аналитики с VMD (видеодетектором движения) проследите, чтобы записи были достаточно длительными, чтобы охватывать весь инцидент. Неоптимальная настройка записи по детектору движения может приводить к перерывам и фрагментации записей. Во многих случаях предпочтительным вариантом является непрерывная запись, но для нее требуется значительно больше ресурсов хранения и нужна постоянно доступная пропускная способность.

3.1.3 Надлежащая безопасность

Вам необходимо принять все необходимые меры для физической защиты системы от несанкционированного доступа. Все аппаратные компоненты, включая камеры, сетевое оборудование и кабели, серверы, устройства хранения, блоки питания и кабели, должны быть надежно защищены. Примеры возможных мер безопасности: размещение серверной в зоне с ограниченным доступом, замки на шкафах с серверами, установка серверов в закрытой стойке, отключение физических портов на сервере, скрытая прокладка сетевых кабелей.

Позаботьтесь о том, чтобы система имела все необходимые средства кибербезопасности для минимизации рисков злоупотребления данными, вмешательства в данные и атак злоумышленников. Т.н. "укрепление" системы можно частично обеспечить программными и техническими средствами, которые позволяют достичь соответствия системы действующим стандартам безопасности. Однако укрепление безопасности также требует, чтобы владелец системы придерживался подхода, ориентированного на безопасность, и активно работал над его внедрением в организации. Например, все пользователи системы должны понимать важность использования надежных, не поддающихся угадыванию паролей, и заботиться о том, чтобы они не были раскрыты. Необходимо минимизировать права доступа пользователей и предоставленные им разрешения, например, придерживаясь принципа наименьших возможных привилегий учетных записей. На владельце системы лежит ответственность за обучение персонала лучшим методикам в области кибербезопасности и их успешное внедрение. Авторизованный интегратор может выполнить укрепление системы, но некоторые меры кибербезопасности могут быть эффективны только при активном содействии людей, использующих систему.

Один из важных путей повышения общей кибербезопасности - защита видео при передаче путем шифрования. При передаче данных между клиентом и сервером AXIS Camera Station применяет шифрование AES для видео, звука и метаданных, и TLS 1.2 для других данных. AXIS Camera Station можно настроить так, чтобы также шифровать по протоколу HTTPS потоки данных между всеми камерами и сервером. Другие рекомендованные методики защиты программного обеспечения включают в себя отключение всех неиспользуемых служб, фильтрацию по IP/MAC-адресам, внедрение IEEE 802.1X, применение контроля SNMP, установку точной даты и времени с доверенного NTP сервера (чтобы гарантировать точность отметок времени в метаданных вашего видео), использование исключительно Axis Secure Remote Access для удаленных подключений (вместо перенаправления портов или использования удаленного рабочего стола). Подробные рекомендации и меры по укреплению кибербезопасности приведены в руководстве Axis по укреплению кибербезопасности.

3.1.4 Конфигурируйте и проверяйте систему

Ключевые составляющие системы можно сконфигурировать еще на этапе проектирования с помощью AXIS Site Designer, выбрав конкретные модели камер, разрешения и времена хранения. После того как система спроектирована и установлена, конфигурации, заданные в AXIS Site Designer, можно автоматически импортировать в AXIS Camera Station, где параметры можно дополнительно настроить и откорректировать в случае необходимости.

После завершения установки систему можно проверить с помощью инструмента AXIS Installation Verifier, входящего в состав AXIS Camera Station Integrator Suite. Этот инструмент проверяет систему в обычном и в ночном режиме, удостоверяясь, что пропускной способности достаточно для работы в

ночном режиме, когда из-за большего уровня шума нагрузка на каналы передачи возрастает. После этого AXIS Installation Verifier выполняет нагрузочное тестирование, постепенно увеличивая объем генерируемых в системе данных до тех пор, пока не обнаружится первое узкое место. Это позволяет понять запас прочности системы и определить, требуются ли какие-то улучшения.

3.2 Выполняйте регулярное обслуживание

Работающую систему необходимо постоянно контролировать и обновлять.

Следите за тем, чтобы оборудование и программное обеспечение функционировали должным образом. Следите за качеством видео, очищайте объективы камер по установленному графику, следите за тем, чтобы в работу камер не было физического вмешательства и чтобы зона и направление обзора камер оставались неизменными. Регулярно проверяйте журналы системы, поскольку в них отражается информация о входе пользователей, подключениях и проблемах с устройствами. AXIS Camera Station позволяет направлять уведомления о различных отклонениях и фиксировать их в журналах системы. Сохраняйте журналы на нестираемых носителях, особенно после серьезных инцидентов. Axis также предоставляет в рамках пакета Integrator Suite возможность онлайнового мониторинга, позволяющую вам контролировать все установленное оборудование и получать информацию о состоянии системы для удобства планового обслуживания и ремонта.

Как аппаратные, так и программные компоненты (операционную систему и VMS) необходимо регулярно обновлять. Применение свежих версий программного обеспечения и прошивок, содержащих актуальные обновления системы безопасности и исправления ошибок, способствует защищенности вашей системы. В идеальном случае VMS находит все обновления программного обеспечения и прошивок автоматически и либо предлагает установить обновления, либо выполняет обновление в автоматическом режиме. Все загружаемое программное обеспечение должно исходить из доверенных источников.

3.3 Работа с доказательствами по установленным процедурам

Если вы применили надлежащие принципы проектирования и обслуживания своей системы видеонаблюдения, ПО AXIS Camera Station позволит вам предоставить вам надежные доказательства любых инцидентов, зафиксированных вашими камерами. Затем вам понадобятся процедуры, определяющие дальнейший порядок действий.

Следуйте рекомендациям правоохранительных органов. Если произошло серьезное преступление, ответственная правоохранительная структура имеет право решать, как должны быть защищены доказательства, и вам необходимо следовать ее инструкциям.

В других случаях главная часть процесса - безопасно экспортировать доказательства. Это означает, что вам необходимо представить их за пределами вашей системы в неизмененном виде, с сохранением той достоверности, которую они имеют внутри системы.

Экспорт должен осуществлять специально назначенный оператор, предпочтительно в присутствии свидетеля. Оператор может быть внешним специалистом, приглашенным специально для осуществления и документирования достоверного экспорта материалов. Привлечение независимой третьей стороны для экспорта позволяет минимизировать риск того, что владельца видео заподозрят в подделке доказательств. Экспортированное оператором видео должно полностью включать в себя инцидент и при этом содержать достаточно информации о предшествующих и последующих событиях.

Выбранные видеофрагменты могут быть записаны на неперезаписываемый носитель, например, диск CD-R, DVD-R или Blu-Ray (-R), который затем можно передать в правоохранительные органы. В качестве альтернативы видеофрагменты можно экспортировать в виде архивных файлов с шифрованием и защитой паролем. Файлы могут быть подписаны цифровой подписью, захешированной с паролем пользователя. Чтобы подтвердить совпадение хеша файла и указанного хеша, необходимо ввести подпись в AXIS File Player. Если хеши совпадают, данные в файле не изменены.

Axis также предлагает инструмент AXIS Camera Station Incident Report, предоставляющий оператору расширенные возможности экспорта. Этот инструмент должен быть настроен заранее администратором, который задает такие данные, как теги инцидентов и место экспорта. После этого инструмент позволяет автоматизировать процесс экспорта, организуя видео по инцидентам и используя теги как имена папок. Экспорт может производиться на локальный ресурс, например, сетевой накопитель (NAS), или на удаленный, доступный по протоколу SMB, например, в облачное хранилище. Отчет включает в себя видеофайлы, стоп-кадры в формате .jpg (создаются в AXIS Camera Station вручную оператором при подготовке отчета), закладки в формате .txt и всю информацию, собранную в отчете, в формате .PDF.

4 Ресурсы по кибербезопасности

Компания Axis применяет в процессе проектирования, разработки и тестирования своего оборудования подходы, направленные на укрепление кибербезопасности, чтобы исключить вероятность недоработок, которые могут быть использованы для атаки. Мы придерживаемся оптимальных методик в области кибербезопасности, в частности, в отношении управления уязвимостями, требований по безопасной передаче и хранению данных, шифрования. Мы стремимся упростить и удешевить для вас применение надлежащих мер контроля в области безопасности, а наше оборудование поддерживает шифрование и управление безопасностью.

Компания Axis как производитель и поставщик систем прилагает все усилия к тому, чтобы предоставлять полные и безопасные системы и решения. В то же время на вас как на пользователе лежит большая ответственность по применению оптимальных методик в области безопасности на своей стороне. Axis предоставляет в помощь вам ряд инструментов, руководств и учебных пособий. На сайте www.axis.com/cybersecurity вы найдете документы по укреплению безопасности, информацию об управлении безопасностью, публикации о кибербезопасности и многое другое.

О компании Axis Communications

Компания Axis вносит весомый вклад в формирование более разумного и безопасного мира, разрабатывая решения, которые повышают безопасность и эффективность бизнеса. Занимая в отрасли технологий сетевого видео ведущие позиции, компания Axis поставляет решения для видеонаблюдения, контроля доступа, сетевых домофонов и звукового сопровождения. Эффективность наших решений повышается благодаря приложениям интеллектуальной аналитики и высококачественному обучению.

Около 4000 специалистов компании Axis трудятся более чем в 50 странах мира, вместе с нашими партнерами по технологиям и по системной интеграции разрабатывая и внедряя решения задач, стоящих перед клиентами по всему миру. Компания Axis была основана в 1984 году. Штаб-квартира компании находится в городе Лунд, Швеция