AXIS Camera Station 5

Руководство по усилению безопасности системы

Введение

Универсального, надежного средства, которое могло бы сделать любую систему безопасности и объект на 100% защищенным от киберугроз, не существует. Как бы привлекательно это ни звучало, такого средства нет и вряд ли оно появится в ближайшее время. Вместо этого необходимо изучить риск, создаваемый угрозами и уязвимостями, уникальными для каждой организации, и, в случае если риск считается неприемлемым, реализовать меры по его снижению. Четко определенные политики и процедуры обеспечивают последовательное информирование и применение этих мер контроля во всей организации и составляют основу зрелой программы кибербезопасности.

Рекомендуемый подход — работать в соответствии со стандартными структурами управления рисками ИТ-безопасности, такими как ISO 27001, NIST CSF и т. п. Хотя эта задача может показаться сложной для небольших организаций, определение базового набора политик информационной безопасности и поддерживающих процессов будет намного лучше, чем полное бездействие. Если ваша организация только начинает путь к кибербезопасности и имеет ограниченные ресурсы в своем распоряжении, мы рекомендуем изучить *Критические элементы управления безопасностью Центра интернет-безопасности (CIS), версия 8*. CIS содержит список из 18 мероприятий по контролю безопасности, разбитых на три группы внедрения, который поможет организациям развивать и совершенствовать свою программу кибербезопасности.

Нарушения безопасности происходят во многих организациях, потому что компания не установила четкие политики, правила и процедуры, регулирующие использование и права доступа для собственных сотрудников. Работает ли ваша организация с политиками и процессами управления видеонаблюдением? Если нет, пора начать их определять.

Цель

Этот документ описывает ряд политик и процедур кибербезопасности, которые могут быть полезны для обеспечения безопасного развертывания и обслуживания систем AXIS Camera Station 5. Хотя они не привязаны напрямую к какой-либо структуре кибербезопасности, мы в основном опираемся на элементы управления безопасностью CIS Security Controls v8, уделяя особое внимание следующим мероприятиям по контролю:

- *Контроль 1: Инвентаризация и контроль корпоративных активов*
- *Контроль 2: Инвентаризация и контроль программных активов*
- *Контроль 3: Защита данных*
- *Контроль 4: Безопасная настройка корпоративных активов и программного обеспечения*
- *Контроль 5: Управление учетными записями*
- *Контроль 6: Управление контролем доступа*
- *Контроль 7: Непрерывное управление уязвимостями*
- *Контроль 10: Защита от вредоносных программ*

Наши рекомендации направлены на то, чтобы помочь установщикам, интеграторам и конечным пользователям снизить общие риски при развертывании систем и управлении системами AXIS Camera Station 5.

Предварительные требования

Предполагается ознакомление с рекомендациями и процедурами, определенными и описанными в *Руководстве по усилению сетевой безопасности AXIS OS*, а также их соблюдение. Кроме того, в этом документе упоминается несколько распространенных ролей пользователей, взаимодействующих с видеосистемой. Сопоставьте эти роли пользователей с вашими собственными классификациями пользователей и ролей. Пользователь может иметь несколько ролей в зависимости от организации.

Определенные роли:

- **Установщик системы**: устанавливает, настраивает, ремонтирует, обновляет и переводит системы на более раннюю версию

Введение

- **Сетевой администратор**: обслуживает сетевую инфраструктуру, подключение конечных узлов, сетевые серверы и ресурсы, а также обеспечивает защиту сети
- **Администратор видеосистемы**: определяет и управляет видеосистемой для обеспечения ее использования, надлежащей производительности и прав пользователей
- **Специалист по обслуживанию видеосистемы**: контролирует, настраивает и устраняет неполадки компонентов для обеспечения производительности системы от имени администратора видеосистемы
- **Пользователи**: лица, использующие клиентское приложение AXIS Camera Station 5 для доступа к живому и записанному видео и, как правило, отвечающие за физическую защиту организации.

Политики безопасности системы

Физическая безопасность

Политика физической защиты

Серверы, устройства, сетевое оборудование и кабели являются физическими объектами, которые могут быть подвергнуты вмешательству, саботажу или украдены. Хост, на котором работает серверное ПО AXIS Camera Station 5 и важное сетевое оборудование (маршрутизаторы, коммутаторы и т. д.) должны быть размещены в среде с физическими и логическими ограничениями доступа. Камеры и прочие подключенные устройства должны быть установлены в труднодоступных местах, также следует использовать вандалозащищенные модели или корпуса. Следует уделить внимание защите кабелей в стенах или кабель-каналах, так как они связаны с повышенным риском несанкционированного вмешательства и саботажа.

Рекомендуемые политики и процедуры
Определите лицо или организационное подразделение, ответственное за визуальный аудит физической защиты серверов VMS, сетевого оборудования, подключенных устройств и кабельной проводки через определенные интервалы времени. Важно поддерживать точный учет всех серверов и устройств, включая их местоположение.

Управление программным обеспечением

Политика в отношении приложений сторонних производителей

Поскольку AXIS Camera Station 5 устанавливается в стандартной среде Windows, может возникнуть соблазн использовать эту среду для программных приложений, не связанных с управлением видео. Установка прочих сторонних приложений открывает возможность внедрения вредоносного ПО в среду, что может привести к простоям системы или предоставить злоумышленнику лазейку для входа в сеть организации.

Рекомендуемые политики и процедуры
Не запускайте на хост-оборудовании ничего, кроме серверного ПО AXIS Camera Station 5 и доверенных сторонних интеграций. Если физическое оборудование должно использоваться для других целей, рекомендуется использовать несколько виртуальных экземпляров сервера и запускать серверное ПО AXIS Camera Station 5 на одной виртуальной машине, а стороннее ПО, не связанное с VMS, на другой виртуальной машине. Информацию о запуске AXIS Camera Station 5 в виртуальной среде можно найти *по этой ссылке*.

Рекомендуется выполнить развертывание антивирусного ПО на всех серверах и компьютерах, которые подключаются к серверу AXIS Camera Station 5. В случае развертывания мобильных устройств это включает установку последних операционных систем и исправлений (т. е. не антивирусного ПО как такового). При антивирусной проверке не сканируйте каталоги и подкаталоги, содержащие базы данных записей. Сканирование этих каталогов на вирусы может повлиять на производительность системы.

Управление учетными записями

Общая политика в отношении учетных записей

Права уровня администратора иногда предоставляются обычным пользователям для удобства. Во многих организациях неясно, кто отвечает за проверку привилегий учетных записей и мониторинг доступа сотрудников к системам.

Рекомендуемые политики и процедуры
Организациям рекомендуется следовать принципу минимальных привилегий при определении системных учетных записей. Это означает, что пользователю должны предоставляться права для доступа только к тем ресурсам и функциям, которые необходимы для выполнения конкретных служебных обязанностей пользователя. Также рекомендуется периодически проверять привилегии учетных записей пользователей системы, чтобы предотвратить «расползание привилегий».

Политика в отношении учетных записей администратора AXIS Camera Station 5

Распространенной ошибкой при развертывании AXIS Camera Station 5 в среде Windows является определение единственной учетной записи администратора для хоста Windows. Со временем пароль может распространиться внутри организации, что

повлечет за собой риск получения несанкционированными лицами привилегий администратора в среде Windows. Это может привести к установке на этот сервер множества нежелательных пользовательских приложений или вредоносного ПО.

Рекомендуемые политики и процедуры
На машине Windows, на которой размещен сервер AXIS Camera Station 5, должна быть как минимум одна учетная запись с правами администратора и одна учетная запись с правами пользователя. Ни одна из этих учетных записей не должна совпадать со стандартной учетной записью администратора Windows. Стандартная учетная запись администратора должна быть отключена после создания учетных записей с правами администратора и пользователя. После развертывания пароль учетной записи администратора должен быть известен и использоваться только **сетевыми администраторами**. Учетная запись с правами пользователя должна использоваться **администратором видеосистемы** если/когда ему нужно войти на сервер AXIS Camera Station 5. Следует отметить, что даже если две вышеуказанные роли выполняются одним и тем же лицом, наличие отдельных учетных записей сетевого администратора и администратора видеосистемы по-прежнему рекомендуется в целях аудита. Для поддержки других ролей, определенных ранее, следует создать дополнительные учетные записи пользователей без привилегий для каждого отдельного **пользователя**, который будет входить в систему.

Если хост, на котором работает AXIS Camera Station 5, размещен в среде домена Active Directory Windows, учетные записи администратора и пользователя могут быть созданы в контексте домена, или для аутентификации на хосте AXIS Camera Station 5 может использоваться существующая доменная учетная запись сотрудника. Это может упростить управление учетными записями, избавив от необходимости создавать и поддерживать дополнительные учетные записи. Это также открывает возможность управления групповыми политиками для применения заданной сложности паролей, развертывания сертификатов и других функций безопасности, доступных в доменных средах.

Политика в отношении учетных записей пользователей AXIS Camera Station 5

Учетные записи пользователей назначаются определенным ролям в AXIS Camera Station 5, что, в свою очередь, определяет конкретные права каждого пользователя в системе, например, к каким видам и к каким видео они имеют привилегированный доступ. Если несколько человек используют одну учетную запись пользователя, возрастает риск передачи пароля другим лицам в организации. Общий доступ к учетным записям также сделает практически невозможным аудит того, кто получал доступ к какой камере/видео и в какое время.

Рекомендуемые политики и процедуры

По возможности используйте Microsoft Active Directory для простого управления пользователями и группами. Кроме того, перед настройкой системы рекомендуем убедиться, что соответствующие группы безопасности определены для всех ролей пользователей.

Active Directory также предоставит:

- Политику паролей, требующую от пользователей регулярной смены пароля
- Защиту от перебора, чтобы учетная запись Windows AD блокировалась после нескольких неудачных попыток аутентификации, в соответствии с политикой паролей организации
- Разрешения на основе ролей, чтобы средства управления доступом могли применяться в масштабах домена

Если необходимо использовать локальные учетные записи Windows, рекомендуется создать уникальную учетную запись для каждого пользователя системы и предоставить им доступ только к тем объектам системы, которые необходимы для выполнения соответствующих обязанностей. Использование групп для пользователей может упростить назначение разрешений, если есть несколько пользователей с одинаковыми разрешениями.

Политика в отношении учетных записей устройств

Учетные записи в устройствах Axis в основном являются компьютерными/клиентскими учетными записями. **Пользователям** никогда не должен быть разрешен прямой доступ к устройству. Единственным клиентом, который должен обращаться к устройствам во время нормальной работы, является сервер AXIS Camera Station 5. Общая стратегия заключается в наличии одинакового пароля для всех устройств. Это создает дополнительные риски, но также может упростить управление паролями, поэтому необходимо оценить собственную толерантность к риску. AXIS Camera Station 5 поддерживает назначение уникальных паролей для каждого устройства через свой интерфейс управления.

Распространенной ошибкой является добавление устройств в AXIS Camera Station 5 с одной учетной записью, которая используется несколькими ролями. В какой-то момент, когда **Специалист по обслуживанию видеосистемы** должен использовать браузер для настройки какого-либо элемента, пароль главной учетной записи устройства (root) раскрывается. В

течение нескольких месяцев большинство людей в организации будут знать пароль для всех устройств и иметь права администратора в системе.

Рекомендуемые политики и процедуры
На устройстве должно быть по меньшей мере две учетные записи администратора: уникальная, созданная для администраторов устройств, и учетная запись root по умолчанию для добавления устройств на сервер AXIS Camera Station 5. Временный доступ, например, когда **Специалист по обслуживанию видеосистемы** получает доступ к устройству с помощью веб-браузера, должен осуществляться с использованием временных учетных записей.

Приложение AXIS Device Manager должно использоваться в качестве основного инструмента для управления учетными записями и паролями устройств. Версия AXIS Device Manager встроена непосредственно в AXIS Camera Station 5 и доступна на вкладке «Управление». Пароль root устройства должен использоваться только AXIS Device Manager и AXIS Camera Station 5, он должен быть известен только тем, кто использует AXIS Device Manager или AXIS Camera Station 5 в качестве инструмента управления устройствами.

Используйте AXIS Camera Station 5 для предоставления временной учетной записи, когда кому-то в роли специалиста по обслуживанию требуется доступ к устройствам через веб-браузер для устранения неполадок или технического обслуживания. Выберите устройство(а) и создайте новую учетную запись, желательно с правами оператора, которую может использовать специалист по обслуживанию. После завершения задачи удалите временную учетную запись.

Обслуживание системы

Политика исправлений хоста Windows AXIS Camera Station 5

Сервер и клиенты AXIS Camera Station 5 работают в среде Windows. Важно, чтобы эти системы поддерживались в актуальном состоянии, чтобы системы, на которых размещено программное обеспечение AXIS Camera Station 5, не имели открытых уязвимостей, которые могут быть использованы для получения несанкционированного доступа к системе управления видео.

Рекомендуемые политики и процедуры
Для всех систем AXIS Camera Station 5, работающих на NVR Axis или пользовательском оборудовании, рекомендуется отключить автоматическое обновление. Обновления Windows в прошлом вызывали нестабильность базовой ОС Windows, поэтому рекомендуется тестировать доступные обновления на отдельных машинах, чтобы обеспечить стабильность системы, прежде чем распространять их на все хост-системы, на которых работает AXIS Camera Station 5. Однако необходимо найти баланс между безопасностью и стабильностью, поскольку оставление системы Windows без исправлений на длительное время влечет за собой риски для всей среды. Исходя из уровня подверженности системы клиента внешним угрозам, временные рамки для обеспечения получения системами последних обновлений должны быть изложены в политике исправлений.

Политика обновления программного обеспечения AXIS Camera Station 5

Использование последнего выпуска программного обеспечения для AXIS Camera Station 5 в большинстве случаев гарантирует применение обновлений для защиты от всех недавно обнаруженных уязвимостей. Чем дольше система работает без актуальных обновлений, тем выше вероятность того, что изъяны в защите будут использованы злоумышленниками и что система будет взломана.

Рекомендуемые политики и процедуры
Важно определить политику исправлений с регулярными оценками развернутых версий программного обеспечения, чтобы гарантировать актуальность AXIS Camera Station 5. Политика исправлений также должна определять, кто несет ответственность за управление работой, связанной с обновлением как серверного, так и клиентского программного обеспечения. Для AXIS Camera Station 5 самый последний выпуск можно найти на сайте *www.axis.com*. AXIS Camera Station 5 требует последних библиотек .NET, поэтому необходимо согласовать политику исправлений Windows с политикой AXIS Camera Station 5.

Политика обновления прошивки устройств

Своевременно обновляя версии встроенного ПО в устройствах, можно сократить наиболее распространенные риски, так как последние версии встроенного ПО будут включать обновления для всех известных уязвимостей, которыми могут воспользоваться хакеры. Axis предоставляет выпуск прошивки устройства с долгосрочной поддержкой (LTS), который включает исправления безопасности и устранение ошибок, при этом добавление функций ограничено для обеспечения стабильности платформы в долгосрочной перспективе. Для получения дополнительной информации о стратегии Axis в отношении разработки прошивки см. документ *Управление встроенным ПО Axis*.

Рекомендуемые политики и процедуры
Для аппаратных устройств политика должна предусматривать постоянное поддержание прошивки в актуальном состоянии. Процессы могут использовать встроенную функцию обновления прошивки в AXIS Camera Station 5 или AXIS Device Manager Extend для определения наличия новых версий прошивки для устройств Axis. Необходимо запланировать время, обычно в нерабочие часы, для развертывания всех обновлений прошивки для всех камер. AXIS Camera Station 5/ AXIS Device Manager Extend также может проверить, были ли приняты обновления прошивки. Если в системе содержатся интеграции, на которые может повлиять обновление, рассмотрите возможность стандартизации на версии прошивки LTS.

Сетевая безопасность

Политика удаленного доступа

Устройства и службы, доступные из Интернета, увеличивают риск того, что внешние злоумышленники будут исследовать или использовать известные уязвимости. Камеры, доступные из Интернета, например, небольшими организациями, которым требуется удаленный доступ к видео, могут стать легкой добычей для злоумышленников, если используются слабые пароли или обнаруживается новая критическая уязвимость. Удаленный доступ к среде Windows должен быть строго контролируемым, по возможности его следует избегать. Хотя среда Windows может иметь подключение к Интернету для удобства обновления систем, использование служб удаленного рабочего стола, таких как Windows Remote Desktop, TeamViewer и AnyDesk, создает пути для получения доступа к вашей системе при отсутствии должного управления.

Рекомендуемые политики и процедуры
Никогда не предоставляйте IP-адрес/порт камеры таким образом, чтобы к ней можно было получить доступ напрямую из Интернета. Если требуется удаленный доступ к видео, используйте Axis Secure Remote Access. AXIS Camera Station 5 использует облачный сервер удаленного доступа для обеспечения зашифрованного удаленного доступа к системе через клиент AXIS Camera Station 5 или мобильное приложение AXIS Camera Station. Помимо ответственности за управление подключениями для удаленных и мобильных пользователей, сервер удаленного доступа играет важную роль в защите целостности при использовании удаленными пользователями. Дополнительную информацию об Axis Secure Remote Access можно найти *по этой ссылке*. Axis поставляет официальные фирменные мобильные приложения как для Android, так и для Apple iOS. Мобильное приложение AXIS Camera Station следует загружать только из официальных источников: Google Play Store и Apple App Store соответственно.

Что касается удаленного доступа к среде Windows, не рекомендуется предоставлять такой доступ к системе, работающей под управлением AXIS Camera Station 5. Однако, если это необходимо, следует проявлять особую осторожность, чтобы убедиться, что выбранное приложение удаленного рабочего стола является безопасным, и доступ предоставляется только тем лицам, которым он необходим. Рекомендуется внедрять дополнительные уровни контроля, такие как многофакторная аутентификация (MFA). Настоятельно рекомендуется вести журналы и последующий аудит попыток удаленного подключения для отслеживания того, кто и в какое время получает удаленный доступ к среде Windows.

Политика ограничения доступа к локальной сети

Сокращение доступа к локальной сети может помочь снизить многие распространенные угрозы за счет уменьшения поверхности атаки. Существует много способов сократить доступ к сети, включая физическую сегментацию сети (отдельное сетевое оборудование и кабели), логическую сегментацию сети с помощью виртуальных локальных сетей (VLAN) и фильтрацию IP-адресов. Камеры Axis поддерживают фильтр IP (таблицы IP), чтобы устройство реагировало только на запросы соединения, поступающие с явно разрешенных IP-адресов.

Рекомендуемые политики и процедуры
NVR AXIS Camera Station S22 — это аппаратные серверы с двумя сетевыми портами. Один из портов создает сегментированную сеть для камер, а другой подключается к основной сети (домену) для обслуживания клиентов системы управления видео. Сервер работает как мост и межсетевой экран для сети камер, предотвращая прямой доступ клиентов к камерам. Это снижает вероятность угроз со стороны злоумышленников в основной сети.

Если сервер AXIS Camera Station 5 и камеры размещены в основной сети, рекомендуется настроить IP-фильтр камеры, ограничив доступ только серверами, на которых размещены AXIS Camera Station 5, AXIS Device Manager и дополнительными служебными клиентами.

Политика сетевого шифрования

Сетевой трафик, передаваемый по небезопасным сетям, обязательно должен быть зашифрован. Интернет попадает под классификацию небезопасной сети. Локальная сеть также может быть классифицирована как небезопасная, и поэтому

сетевой трафик также должен быть зашифрован. Политика, применяемая к видеопотоку в сети, зависит от того, как классифицируется видео и какова вероятность того, что злоумышленники получат сетевой доступ к видеосистеме. Рекомендуется исходить из предположения, что сеть уже подверглась взлому. У крупных организаций обычно есть политика, определяющая классификацию сети.

Рекомендуемые политики и процедуры

Трафик между видеоклиентом и сервером AXIS Camera Station 5 должен использовать шифрование. Трафик между сервером AXIS Camera Station 5 и камерами должен быть зашифрован в зависимости от инфраструктуры. Камеры Axis поставляются с самозаверяющим сертификатом и HTTPS, включенным по умолчанию. Если есть риск сетевого спуфинга, например, когда вредоносный компьютер пытается выдать себя за камеру, следует использовать инфраструктуру открытых ключей (PKI) с сертификатами, подписанными ЦС. AXIS Camera Station 5 имеет встроенный локальный центр сертификации (CA), который может экономично управлять подписанием и распространением серверных сертификатов для устройств Axis.

Версии TLS

Мы рекомендуем отключить TLS версий 1.1 и 1.0. Установщик AXIS Camera Station предлагает помощь во время установки или обновления.

Шифры HTTPS

AXIS Camera Station 5 поддерживает и использует наборы шифров TLS для безопасного шифрования соединений HTTPS. Конкретный набор шифров зависит от клиента, подключающегося к AXIS Camera Station 5, или контактируемой службы, и AXIS Camera Station 5 согласует его в соответствии с протоколом TLS. Мы рекомендуем настроить Windows таким образом, чтобы не использовать наборы шифров TLS 1.2, перечисленные *в RFC 7540*. Возможность отключения набора шифров зависит от устройств и камер, используемых совместно с AXIS Camera Station 5. Если для устройства или для камеры нужен определенный набор шифров, деактивировать набор слабых шифров невозможно.

Управление данными

Классификация видео

Живое и записанное видео должно быть классифицировано. Видео может быть классифицировано как общедоступное, частное, ограниченное, также могут использоваться любые другие классы, определенные политиками организации. Во многих случаях видео регулируется законами и региональными нормами, а также внутренними ИТ-политиками, поэтому владелец системы несет ответственность за ознакомление с законами и правилами, применимыми к их видеоданным.

Рекомендуемые политики и процедуры
Классифицируйте живое видео, записанное видео и аудио в соответствии с действующими в организации политиками классификации данных. Настройте привилегии доступа пользователей и усиление защиты системы в соответствии с конфиденциальностью видео и аудиоданных. Если аудио не требуется, его можно отключить на уровне устройства.

Дополнительные средства контроля безопасности

В зависимости от уровня зрелости и толерантности к риску вашей организации мы рекомендуем реализовать несколько дополнительных средств контроля безопасности из CIS Controls v8, чтобы помочь снизить риски кибербезопасности в повседневной работе.

Дополнительные элементы управления CIS:

Контроль 8: Управление журналами аудита
Собирайте, создавайте оповещения, просматривайте и сохраняйте журналы аудита событий, которые могут помочь обнаружить, понять или восстановить систему после атаки.

Контроль 14: Внедрение программы обучения осведомленности о безопасности и навыкам
Получите представление о навыках и поведении ваших сотрудников. Обучайте персонал выявлять различные формы атак.

Контроль 17: Реагирование на инциденты и управление инцидентами
Используйте письменные планы реагирования на инциденты с четко определенными фазами обработки/управления инцидентами и ролями персонала, а также с указанием, как сообщать о нарушениях безопасности соответствующим органам и третьим сторонам.

Руководство по усилению безопасности системы
AXIS Camera Station 5

Версия M3.2
Дата: 2024
Номер по каталогу T10179095