КИБЕРБЕЗОПАСНОСТЬ В IP-СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ: ЗАЩИТА ОТ МНИМЫХ УГРОЗ ИЛИ НЕОБХОДИМОСТЬ?

Рост популярности использования сетевых технологий в системах видеонаблюдения делает особенно актуальными вопросы обеспечения их безопасности. Практика доказывает, что зачастую сами IP-камеры и сетевые видеорегистраторы (NVR) нуждаются в защите. Проведенные исследования показали, что многие IP-камеры и NVR, представленные на современном рынке, имеют уязвимости, позволя злоумышленнику не только просматривать видео, но и использовать устройства для осуществления сетевых атак на другие компьютеры в Интернете. Выяснилось, что та легкость, с которой злоумышленники в кино перехватывают видеопотоки и подменяют видеоизображение, транслируемое от камер, не является красивой режиссерской выдумкой. Некорректно настроенные IP-устройства могут свести на нет все меры по обеспечению безопасности дома или офиса, поэтому важно понимать возможные угрозы кибербезопасности и методы противодействия им.

В мире установлены и используются миллионы IP-камер. К проблемам с кибербезопасностью в IP-системах видеонаблюдения привели две основные причины. Во-первых, системы видеонаблюдения исторически строились на базе закрытых сетей – об этом говорит аббревиатура CCTV, обозначающая именно системы замкнутого телевидения. Для несанкционированного доступа к видеоизображению в закрытой сети требуется получить физический доступ к кабелю, по которому передается сигнал от камеры, поэтому одной из задач любой системы безопасности является контроль своих собственных каналов связи. Поскольку предполагалось, что сигнал передается по физически защищенному каналу связи от камеры на видеорегистратор, большинство производителей этих устройств не использовали аутентификацию при подключении пользователей и шифрование передаваемого трафика. Во-вторых, системы телевизионного наблюдения исторически представляли собой инфраструктуру, где получателем видеоизображения являлся локальный охранник, реагирующий на события. С развитием Интернета, мобильных устройств и распространением IP-камер формат использования последних изменился: люди стали устанавливать камеры к себе домой или в подъезд с доступом через мобильное приложение, IP-камеры появились на улицах городов, передавая потоки видео через сетевую инфраструктуру телекоммуникационных провайдеров. Потребовался онлайн-доступ к видеоизображениям через небезопасный канал связи – публичный Интернет, но, как мы уже отметили, подключаемые к нему IP-камеры не имели эффективных методов защиты от несанкционированного доступа (либо эти технологии были выключены по умолчанию или в связи с недостаточной квалификацией установщиков). Люди массово выставили в Интернет устройства, способные генерировать десятки мегабит трафика, причем значительная часть этих устройств использовала пароль для подключения по умолчанию и имела открытые порты для удаленного администрирования.

Практически все функциональные возможности современных IP-камер реализуются в рамках концепции «система-на-кристалле» (SoC), поэтому при всем кажущемся разнообразии IP-камер, представленных на современном рынке, их внутреннее устройство практически идентично. Внутри почти у всех камер используется операционная система Linux, доступ к которой у многих производителей осуществляется через открытые порты стандартных сетевых протоколов, таких как Telnet и SSH. Стоит отметить, что лишь после возникновения скандала с вредоносным ПО и ботнетом Mirai ведущие производители IP-камер закрыли небезопасные порты на своих устройствах. Основным методом компрометации IP-камер со стороны данного вредоносного ПО являлся подбор паролей по стандартной библиотеке. Таким образом, если к IP-камере разрешен доступ через протокол SSH и в ней установлен стандартный пароль (например, admin), устройство заражалось вредоносным ПО и становилось частью ботнета Mirai. В этой связи актуальным будет анализ методов обеспечения кибербезопасности IP-камер и NVR.

Рассмотрим данные методы на примере оборудования компании Honeywell:

- Все IP-камеры серии equIP имеют аппаратную поддержку инфраструктуры открытых ключей (PKI) для обеспечения информационной безопасности. IP-камеры используют спецификацию Trusted Platform Module (TPM) со специализированным криптопроцессором. Каждая микросхема TPM уникальна для специфического устройства.
- При первом входе в веб-интерфейс камеры и NVR требуется изменить пароль администратора, используемый по умолчанию. Устройства контролируют ввод, не допуская применения простых паролей. Учетная запись блокируется после ввода определенного количества неправильных паролей.
- Получение видеопотока от IP-камеры по сети возможно только с дайджест-аутентификацией ONVIF. Данная функция исключает передачу пароля по сети в открытом виде.
- Обновление прошивки камеры и NVR возможно только с использованием файлов, подписанных электронной

цифровой подписью. Это защищает устройства от установки прошивки, содержащей вредоносный программный код.

- «Небезопасные» сетевые порты и протоколы в IP-камерах и NVR отключены. К ним относятся Telnet, SSH, UPnP и возможность подключения к камере с использованием технологии P2P.
- Возможна проверка подлинности в сети с использованием протокола 802.1x.
- По умолчанию используется безопасное соединение через HTTPS.

Использование безопасного соединения через HTTPS имеет свои основания. В большинстве случаев обмен данными между браузером (через который пользователь просматривает видео с камеры или настраивает устройство) и IP-камерой, NVR или видеосервером происходит по протоколу HTTP. Этот протокол устанавливает правила обмена информацией и служит транспортом для передачи данных – с его помощью браузер загружает страницу с информацией на компьютер или смартфон. Загружаемые данные должны пройти через одну или несколько сетей, каждая из которых может быть потенциально использована для прослушивания трафика или вмешательства в установленное соединение. Это особенно актуально при просмотре страниц через общедоступную сеть Интернет и незащищенные сети WiFi. Для установления безопасного соединения используется протокол HTTPS с поддержкой шифрования. В электронных платежных системах и в системах, обрабатывающих персональные данные пользователей, защита информации исключительно важна, поэтому в них используется только HTTPS. До недавнего времени производители IP-камер и устройств с веб-интерфейсом не использовали HTTPS по умолчанию, однако ситуация стала меняться после того, как по всему миру были взломаны тысячи IP-устройств, подключенных к Интернету. Все современные браузеры поддерживают HTTPS, и его не нужно специально настраивать. Защиту данных в HTTPS обеспечивает криптографический протокол SSL/TLS. По сути, этот протокол является дополнением для HTTP, обеспечивая шифрование данных и делая их недоступными для просмотра посторонними. Протокол SSL/TLS хорош тем, что позволяет двум незнакомым между собой участникам сети установить защищенное соединение через незащищенный канал связи. Как же его можно реализовать, ведь соединение может все время прослушиваться злоумышленником? Для понимания принципа работы воспользуемся следующей абстракцией. Предположим, что вы хотите отправить какую-то ценную вещь другому человеку. Вы кладете ее в прочный чемодан и отправляете его по почте. Чтобы курьер (или кто-либо другой) не украл ее, вы запираете чемодан на замок. Курьер доставляет чемодан, но ваш адресат не может его открыть – у него нет ключа. Тогда он вешает на чемодан свой замок и отправляет обратно вам. Вы получаете чемодан с двумя замками, снимаете свой (теперь это можно сделать) и отправляете снова. Адресат получает, наконец, чемодан, на котором висит только его собственный замок, открывает его и достает вещь. Оказывается, эта хитрая процедура с многократной пересылкой чемодана была нужна, чтобы иметь возможность обмениваться с собеседником зашифрованными сообщениями. В чемодане вы отправили ему ключ шифрования, и теперь он известен вам обоим. Вы можете открыто обмениваться зашифрованными сообщениями, не опасаясь, что их кто-то перехватит – их невозможно расшифровать без знания ключа. Почему нельзя было переслать чемодан отдельно, а ключ от замка отдельно? Потому что в таком случае не было гарантии, что ключ не перехватят и чемодан не откроет кто-то другой.

На аналогичном принципе основана работа протокола SSL/TLS. При установке безопасного соединения через HTTPS ваш браузер и IP-устройство выбирают общий секретный ключ (не передавая его в открытом виде за счет использования вышеописанного «чемодана с замками»), а затем обмениваются информацией, шифруя ее с помощью этого ключа. Секретный ключ генерируется заново для каждого сеанса связи между браузером и IP-устройством. Получим ли мы идеально безопасную систему? К сожалению, нет – для полной надежности не хватает гарантии того, что ваш собеседник является тем, за кого себя выдает. В соединение между браузером и IP-устройством может вклиниться третий участник, расшифровывая все сообщения. Избежать этой ситуации помогает цифровой сертификат – электронный документ, который используется для идентификации IP-устройства или сервера. Пользователю, находящемуся на стороне браузера, сертификат не нужен, но он требуется любому IP-устройству, с которым необходимо установить безопасное соединение. Сертификат подтверждает «подлинность» IP-устройства, на котором он установлен. Выдачей сертификатов занимаются удостоверяющие центры, но самозаверенный сертификат можете выдать вы сами, убедившись в том, что это устройство принадлежит вам или вашей организации. Проверка подлинности сертификата – первое, что делает браузер при установлении безопасного HTTPS-соединения. Обмен информацией с IP-устройством начнется только в том случае, если эта проверка прошла успешно. Если вернуться к аналогии с чемоданом и замками, то цифровой сертификат позволяет убедиться в том, что замок вашего собеседника на чемодане принадлежит именно ему.

Можно с уверенностью сказать, что проблема обеспечения безопасности IP-систем видеонаблюдения – это сложная и многогранная задача, проиллюстрированная лишь частично в координатах «чемодан-получатель», решить которую по силам только тем компаниям, которые смогут доказать пользователям защищенность своих решений и отсутствие рисков для их безопасности.

Honeywell

THE POWER OF **CONNECTED**

АО «ХОНЕВЕЛЛ»
121059, Москва, ул. Киевская, д. 7
тел.: (495) 797-9371, (495) 796-9800
191123, Санкт-Петербург,
ул. Шпалерная, д. 36
тел.: (812) 329-5722
e-mail: securityrussia@honeywell.com
www.security.honeywell.com/ru