ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕХНИЧЕСКИХ ПРОЕКТАХ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

Борощук Дмитрий Владимирович
независимый эксперт

Практическое большинство современных систем безопасности переходит на стандартные сетевые интерфейсы, те самые, которые используются во всех компьютерных сетях. С одной стороны, это замечательно – полная унификация транспортных интерфейсов позволяет расширять вашу систему безопасности без особых дополнительных расходов, создать простой удаленный доступ для охраны и управляющих бизнеса и привнести дополнительные возможности по интеграции различных ранее локальных систем. С другой же стороны – инженеры технических систем безопасности совершенно не готовы к подобному переходу, потому что создание единого транспортного интерфейса по протоколам TCP/IP требует знаний, которые присущи сетевым инженерам, и, увы, осознание того, что это стало частью современной действительности, присуще далеко не всем. Да и инженеры систем безопасности просто не понимают, как сделать систему, которая бы не только фиксировала уже произошедшее преступление, но и могла на каком-то этапе предотвращать его.

СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ НЕБОЛЬШОГО ОБЪЕКТА

Рассмотрим реализацию системы видеонаблюдения для офисного центра, магазина, или складского помещения: пара десятков видеокамер развешаны по всей территории объекта. Они подсоединены через неуправляемые свичи, направленные, в свою очередь, к единому роутеру, в который, помимо всего, подключаются еще и компьютеры пользователей для доступа в Интернет и все сотрудники и гости данного заведения через Wi-Fi модуль этого же роутера, чтобы получить доступ к так ими любимым социальным сеточкам. На посту охраны стоит видеорегистратор с монитором, и охрана с разной долей успешности туда смотрит.

Обычно в проекте все выглядит близко к идеальному: оборудование подключено, настроено, чтобы производилась запись и манипуляции с ней, и физически установлено там, где была техническая возможность, и там, где указал заказчик. В реальности дела обстоят совсем не так в 80% случаев, которые я наблюдал за 16 лет своей профессиональной деятельности.

Все ли правильно сделано? Есть ли слабые места у вашей системы? Сможет ли вся эта система быть в итоге полезна в реальной жизни? Давайте рассмотрим на примерах:

Видеокамеры установлены там, где это было удобно, для фиксирования единственного места, без учета следующих ситуационных особенностей.

- Предполагаемые пути прихода и отхода гипотетического нарушителя (для понимания его траектории движения при совершении преступления). Это достаточно важно – проследить его путь и продолжить наблюдения через камеры ваших соседей или проследить за тем, в какой транспорт он пересядет.
- Камеры на входе четко должны фиксировать лицо входящего на охраняемую территорию для возможной дальнейшей идентификации. Но, как правило, конечный пользователь, как и проектировщик, надеются, что одна из обзорных камер выполнит эту функцию.
- Видеокамеры установлены в таком месте, что направление угла обзора может изменить нарушитель, например, направив ее в другую сторону при помощи шеста или палки. И хорошо, если этот момент будет замечен охраной, но, как правило, это обнаруживается уже постфактум.

Видеокамеры в системе устанавливаются без фиксированного IP-адреса, и пароль на доступ к ним остается стандартным или заменяется весьма простым. Это позволяет нарушителю манипулировать видеопотоками и с легкостью заменить картинку с установленной камеры на свою.

Оборудование сетевой инфраструктуры находится в открытом доступе, а чаще всего просто лежит за потолком.

Это возможность подключиться к вашей внутренней локальной сети потенциальному нарушителю.

Присоединенные через беспроводной доступ устройства имеют прямой выход в вашу сеть. Это так же, как и прямое физическое подключение, чревато тем, что любой, даже случайно подключенный пользователь, обладающий начальными навыками работы с сетевым окружением, может вывести вашу систему безопасности из строя.

Охрана и администрация работают с видеоархивом под одними и теми же правами доступа. Что позволяет простому охраннику иметь доступ к удалению и модификации информации.

Открытое физическое расположение видеорегистратора сразу же привлекает свое внимание и, как правило, уничтожается нарушителем в первую очередь.

Никакого резервного питания для всех компонентов системы. Любой сбой электричества сведет на нет все возможности системы безопасности. Даже самой совершенной.

И еще многое другое, но давайте сегодня остановимся на основах создания условий для информационной безопасности. «Как же этого избежать?» – спросит пытливый читатель. А все достаточно просто – для начала давайте определим принципы построения системы.

Принципы создания условий для информационной безопасности

Разумная достаточность (STAND ALONE или платформенное решение). Выберите наиболее простой набор оборудования, подходящий для решения именно той задачи, над которой вы работаете.

Оптимизация в составе оборудования (минимизация элементов системы). Чем меньше технических элементов в вашей системе, тем меньше количество векторов атак на нее.

Создание закрытой самостоятельной экосистемы (локализация всех элементов). Пусть сеть, предназначенная для систем наблюдения и обеспечения безопасности, будет отделена от общей. Хотя бы логически, при помощи технологии VLAN. Но лучше полностью разделить их на физическом уровне.

Резервированное питание для всех компонентов системы. Классно, когда у вас стоит источник бесперебойного питания, способный продержать в рабочем состоянии оборудование хотя бы минут 40. И помните, что все элементы системы должны иметь такую возможность.

Разделение DVR/NVR/сервер оборудования и АРМ. Рабочее место охранника должно быть максимально отделено от оборудования, на котором хранится запись.

Оборудование сетевого сегмента. Рекомендуется использование оборудования одного производителя – для лучшей интеграции, минимизации технологических сбоев вследствие несовместимости или частичной совместимости компонентов.

Упрощение элементов пользовательского интерфейса. К сожалению, конечные пользователи не всегда технически подкованы, их действия даже без злого умысла могут нанести ущерб вашему техническому решению.

Разделение прав доступа. У каждого человека, который использует вашу систему, должен быть определенный уровень доступа со своими привилегиями. Будет очень неприятно, когда только что взятый на работу охранник сможет спокойно удалить архив записей или получить доступ к информации о всех передвижениях сотрудников внутри охраняемого периметра.

Физическая защита оборудования. Все компоненты технической системы безопасности должны быть установлены в запирающихся коммутационных ящиках. Если в корпусе какого-либо из устройств расположен тампер-датчик вскрытия корпуса, задействуйте его и выведите в отдельный раздел охранной сигнализации. Если есть возможность, изолируйте кабели, задействованные в системе безопасности, от остальной кабельной инфраструктуры.

Рекомендации по подбору оборудования

DVR или NVR. Интегрированные решения с встроенными Ethernet PoE (Power on Ethernet) для подключения и питания видеокамер. Эта рекомендация применима исключительно для маленьких систем начального уровня. Если вы проектируете что-то большее, присмотритесь к чему-нибудь посерьезнее, чем простой NVR.

Маршрутизатор или сетевой экран. Раздача PoE питания на портах (Passive PoE), встроенный Firewall и NAT (правила фильтрации по ip/mac/url), поддержка туннельных протоколов (PPTP/PPoE/IPsec/SSTP/L2TP/IP2IP/EoIP), встроенный VPN сервер.

Беспроводные мосты для удаленного оборудования (если вдруг используете) должны поддерживать многодиапазонность 900 МГц/1800 МГц/2,4 ГГц/5 ГГц, встроенный контроль состояния радиоэфира и иметь поддержку туннельных протоколов (PPTP/PPoE/IPsec/SSTP/L2TP/IP2IP/EoIP).

СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ КРУПНОГО ОБЪЕКТА

Если система безопасности несколько больше системы для небольшого офиса, имеет выход в Интернет или же в общую сеть компании, то имеет смысл установить на границе вашей сети безопасности и внешним миром межсетевой экран, он же аппаратный файрвол.

Технические требования к межсетевому экрану:

- идентификация и контроль приложений по любому порту;
- идентификация и контроль попыток обхода защиты;
- управление неизвестным трафиком;
- сканирование с целью выявления вирусов и вредоносных программ во всех приложениях, по всем портам;
- обеспечение одинакового уровня визуализации и контроля приложений для всех пользователей и устройств;
- упрощение, а не усложнение системы безопасности сети благодаря добавлению функции контроля приложений;
- обеспечение той же пропускной способности и производительности при полностью включенной системе безопасности приложений.

Необходимые программные компоненты в составе межсетевого экрана:

- управление HotSpot (гостевыми точками доступа);
- управление полосой пропускания;
- интерфейсы VLAN;
- VPN (IPSec, SSL, L2TP over IPSec);
- SSL/HTTPS inspections;
- журнал событий и мониторинга;
- настраиваемые зоны;
- система обнаружения вторжений (IntrusionDetection and Prevention).

ЗАЩИТА СЕТЕВОЙ ИНФРАСТРУКТУРЫ БЕЗОПАСНОСТИ

Система видеонаблюдения сформирована, пришло время создавать защиту сетевой инфраструктуры безопасности. Без «лишней воды» постараюсь по пунктам описать основные действия:

1. Идентифицируем пользователя.
   Определяем границы его полномочий.
2. Используем аутентификацию устройств в сети.
3. Создаем отдельные сети VLAN.
4. Включаем фильтрацию IP-адресов на устройствах.
5. Используем VPN для подключения удаленных устройств.
6. Включаем HTTPS, SSL/TLC.
7. Отключаем камеры от сторонних встроенных сервисов.
8. Отключаем DHCP.
   Принцип «Белого списка».
9. Закрываем неиспользуемые порты.
10. Изменяем стандартные порты.
11. Используем аутентификацию устройств в сети.
12. Производим контроль активности сетевого окружения.

СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ В МЕНЯЮЩЕМСЯ МИРЕ

Согласитесь, все достаточно просто – вы создали вроде бы защищенную систему и работать она должна хорошо, но так было бы в идеальном мире, а мы живем при постоянно изменяющихся условиях, и чтобы ваша система продолжала быть эффективной, периодически проверяйте ее и задавайте себе следующие вопросы.

Установили ли вы, кто и как будет использовать систему? Необходимо конкретизировать роли администратора, оператора и наблюдателя.

Известно ли вам, что происходит с хранящимся в архиве материалом? Как долго предполагается хранить видеоматериалы, и кто будет иметь доступ к записям?

Проверена ли физическая безопасность инсталляции? Кабели и сетевое оборудование необходимо тщательно защитить!

Осуществляется ли процедура проверки безопасности системы через определенные промежутки времени? Удостоверьтесь в том, что предусмотренные вами алгоритмы действуют и система работает исправно.

Актуальны ли предпринятые меры информационной безопасности в текущий момент?

Надеюсь, в итоге у вас все получится.

ЗАКОНОДАТЕЛЬСТВО. СТАНДАРТЫ. ПРОВЕРКИ: ЧЕК-ЛИСТЫ

НОВОСТИ

■ **В России впервые утвержден стандарт по тестированию систем оповещения и тушения.** Российские организации будут обязаны ежеквартально тестировать пожарную сигнализацию и дважды в год: работоспособность автоматических систем тушения и противодымной защиты. Такие меры предусматривает уже утвержденный ГОСТ. Росстандарт утвердил ГОСТ «Организация проведения проверки работоспособности систем и установок противопожарной защиты зданий и сооружений». Национальный стандарт вступит в силу 1 мая. За проведение инспекции отвечает собственник объекта, он может привлекать специалистов организации или сторонних экспертов. ГОСТ предусматривает и внеплановые проверки «по мере необходимости». Результаты проверки оформляются в форме акта. Если были обнаружены неисправности, «руководитель обязан принять меры к их устранению».

■ **«Пожарные» чек-листы расширяют сферу применения.** МЧС России представило проект проекта приказа МЧС России «Об утверждении форм проверочных листов, используемых должностными лицами федерального государственного пожарного надзора МЧС России при проведении плановых проверок по контролю за соблюдением требований пожарной безопасности». Сейчас пожарные инспекторы используют чек-листы только при проверках ограниченного ряда объектов – МКД, торговли и общепита, если они относятся к классам умеренного риска функциональной пожарной опасности Ф1.3, Ф3.1 и Ф3.2. Согласно же проекту, чек-листы будут применяться также при проверках:

- детских садов, домов престарелых и инвалидов, больниц, интернатов;
- гостиниц;
- учреждений культуры и спорта;
- вокзалов;
- поликлиник;
- религиозных объектов;
- школ, техникумов, вузов;
- различных контор и офисов, а также производственных зданий и складов;
- садовых и дачных товариществ.